Entwicklung eines Kriterienkatalogs zur Identifikation von Schwachstellen in der Sicherungskultur für Informationstechnologie (IT)

GRS - 713

Gesellschaft für Anlagen-
und Reaktorsicherheit
(GRS) gGmbH

Entwicklung eines Kriterienkatalogs zur Identifikation von Schwachstellen in der Sicherungskultur für Informationstechnologie (IT)

Clemens Heitsch
Birte Ulrich
Manuela Jopen
Christian Lambertus
Patrick Gebhardt

März 2023

Anmerkung:

Das diesem Bericht zugrunde liegende Forschungsvorhaben wurde mit Mitteln des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) unter dem Förderkennzeichen 4720R01660 durchgeführt.

Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei der GRS.

Der Bericht gibt die Auffassung und Meinung der GRS wieder und muss nicht mit der Meinung des BMUV übereinstimmen.

GRS - 713
ISBN 978-3-910548-04-6

Deskriptoren
Informationssicherheit, Informationssicherheitskultur, IT-Sicherheit, Sicherungskultur

Kurzfassung

Die Bedeutung der Sicherungskultur für die Wirksamkeit von Sicherungsmaßnahmen wird seit einigen Jahren verstärkt diskutiert und wurde u. a. auch im Rahmen der deutschen IPPAS-Mission als ein wichtiges Werkzeug zur Sicherstellung des erforderlichen Schutzes vor Störmaßnahmen oder sonstigen Einwirkungen Dritter identifiziert. IT-Systeme werden in deutschen kerntechnischen Anlagen verstärkt eingesetzt. In den letzten Jahren gab es außerdem einige Angriffe mit Schadsoftware auf IT-Systeme und industrielle Steuerungssysteme von kritischen Infrastrukturen im In- und Ausland. Hierzu zählen zum Beispiel die IT-Angriffe durch Stuxnet, Crashoverride/Industryer (auf das ukrainische Stromnetz) und Triton/TriSIS (auf ein sicherheitstechnisches System in einer petrochemischen Anlage in Saudi-Arabien). Vor diesem Hintergrund sind die Erstellung und Umsetzung von IT-Sicherheitskonzepten und eine hohe Sicherungskultur auch für die Informationstechnologie entscheidende Einflussfaktoren, die sich auf das Sicherungs- und Sicherheitsniveau von kerntechnischen Anlagen und Einrichtungen auswirken. Neben gezielten Angriffen auf IT-Systeme und industrielle Steuerungsanlagen besteht zudem das Risiko, dass Schadsoftware unbeabsichtigt und unentdeckt durch Mitarbeiter der Organisation eingebracht wird.

In diesem Vorhaben wurde die Fragestellung der Umsetzung von bewährten Vorgehensweisen zur Schaffung einer hohen Sicherungskultur im Hinblick auf die Informationssicherheit vertieft untersucht, wobei auch die Schnittstelle zur Sicherheitskultur betrachtet wurde. Hierfür wurde zunächst der Stand von Wissenschaft und Technik zu nationalen und internationalen Anforderungen an und Merkmalen von Sicherungskultur ermittelt. Aspekte sowie relevante Anforderungen und Merkmale, die die Informationssicherheitskultur betreffen, wurden herausgearbeitet. Basierend darauf wurde eine Liste von Kriterien, anhand derer Verbesserungspotential in der Informationssicherheitskultur aufgedeckt werden können, erarbeitet. Abschließend wurde ein Fragebogen entwickelt, der z. B. im Rahmen von Selbsteinschätzungen oder Audits zur Überprüfung der Informationssicherheitskultur genutzt werden kann. Zusammen mit den in diesem Vorhaben erarbeiteten Kriterien einer guten Informationssicherheitskultur wurden die Aspekte der Sicherheits- und der Sicherungskultur vergleichend dargestellt. Dieser Vergleich zeigt, dass einige Kriterien in allen Kulturfacetten zum Tragen kommen, jedoch oft unterschiedliche Formulierungen verwendet werden. Auch werden in manchen Kulturfacetten Aspekte adressiert, die in den anderen Kulturfacetten ebenfalls zur Anwendung kommen könnten, dort, jedoch nicht adressiert werden.

Abstract

The importance of the security culture for the effectiveness of security measures has been increasingly discussed for several years and was also identified, among other things, within the framework of the German IPPAS mission as an important tool for ensuring the necessary protection against disruptive measures or other third-party interference. IT systems are increasingly being used in German nuclear facilities. In recent years, there have also been several attacks with malware on IT systems and industrial control systems of critical infrastructures in Germany and abroad. These include, for example, the IT attacks by Stuxnet, Crashoverride/Industryer (on the Ukrainian power grid) and Triton/TriSIS (on a safety-related system in a petrochemical plant in Saudi Arabia). Against this background, the creation and implementation of IT security concepts and a high security culture also for information technology are decisive influencing factors that have an impact on the security and safety level of nuclear facilities and installations. In addition to targeted attacks on IT systems and industrial control systems, there is also the risk of malware being introduced unintentionally and undetected by employees of the organisation.

In this project, the question of implementing best practices to create a high security culture with regard to information security was examined in depth, also considering the interface with the safety culture. For this purpose, the state of the art in science and technology regarding national and international requirements and characteristics of security culture was first determined. Aspects as well as relevant requirements and characteristics concerning information security culture were elaborated. Based on this, a list of criteria was developed that can be used to identify potential for improvement in the information security culture. Finally, a questionnaire was developed that can be used, for example, in the context of self-assessments or audits to check the information security culture.

Together with the criteria for a good information security culture developed in this project, the aspects of the security and safety culture were compared. This comparison shows that some criteria are used in all culture facets, but often different formulations are used. Also, aspects are addressed in some culture facets that could also be applied in the other culture facets but are not addressed there.

Inhaltsverzeichnis

1 Einleitung

Die Bedeutung der Sicherungskultur für die Wirksamkeit von Sicherungsmaßnahmen wird seit einigen Jahren verstärkt diskutiert und wurde u. a. auch im Rahmen der deutschen IPPAS-Mission als ein wichtiges Werkzeug zur Sicherstellung des erforderlichen Schutzes vor Störmaßnahmen oder sonstigen Einwirkungen Dritter identifiziert. Im Fokus der Empfehlungen, die die IAEA der Bundesrepublik im Rahmen der IPPAS-Mission im Jahr 2017 ausgesprochen hat, stand auch die Förderung von Aktivitäten zur nuklearen Sicherungskultur. Mit den Arbeiten in diesem Vorhaben hat die GRS ihre Kompetenz in den Bereichen Sicherheits- sowie Sicherungskultur und der Informationssicherheit erweitert.

Vor dem Hintergrund des verstärkten Einsatzes von IT-Systemen in deutschen kerntechnischen Anlagen sowie den Erfahrungen aus Angriffen mit Schadsoftware auf IT-Systeme und industrielle Steuerungssysteme von kritischen Infrastrukturen[1] im In- und Ausland sind die Erstellung und Umsetzung von IT-Sicherheitskonzepten und eine hohe Sicherungskultur auch für die Informationstechnologie entscheidende Einflussfaktoren, die sich auf das Sicherungs- und Sicherheitsniveau von kerntechnischen Anlagen und Einrichtungen auswirken. Neben gezielten Angriffen auf IT-Systeme und industrielle Steuerungsanlagen besteht zudem das Risiko, dass Schadsoftware unbeabsichtigt und unentdeckt durch Mitarbeiter der Organisation eingebracht wird.

Zur Sicherstellung des erforderlichen Schutzes vor Störmaßnahmen oder sonstigen Einwirkungen Dritter ist das Zusammenwirken personeller, organisatorischer, technischer und baulicher Faktoren notwendig. Sicherungskultur setzt insbesondere bei den personellen und organisatorischen Faktoren an und umfasst unterschiedliche organisatorische Ebenen (Einzelpersonen, Management, ganze Organisation) sowie die Ebene des Staates, der die lenkende und führende Aufgabe besitzt, Organisationen dabei zu unterstützen, effektive Methoden und Werkzeuge für eine positive Sicherungskultur einzuführen.

[1] Die GRS verfasste zu der Thematik des Angriffs mit Schadsoftware auf IT-Systeme und industrielle Steuerungssysteme von kritischen Infrastrukturen die WLN 2021/01, zu Malware auf speicherprogrammierbaren Steuerungen unter SIMATIC WinCC und SIMATIC PCST die WLN 2010/07 und zu Schadsoftwarefunde im Kernkraftwerk Gundremmingen, Block B die WLN 2016/08.

Sowohl die Sicherungs- als auch die Sicherheitskultur sind durch eine, für die Gewährleistung der Sicherheit der Anlage erforderliche, sicherheitsgerichtete Grundhaltung, Verantwortung und Handlungsweise aller Mitarbeiter bestimmt. Hierzu zählen auch die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter bezüglich Informationssicherheit. Die Vernetzung dieser Faktoren mit dem Ziel eines sicherheitsgerichteten Handelns ist Grundlage für eine hohe Sicherheits- und Sicherungskultur auch im Bereich der Informationssicherheit.

In diesem Vorhaben wurde die Fragestellung der Umsetzung von bewährten Vorgehensweisen („good practices“) zur Schaffung einer hohen Sicherungskultur im Hinblick auf die Informationssicherheit vertieft untersucht, wobei auch die Schnittstelle zur Sicherheitskultur betrachtet wurde. Hierfür wurde zunächst der Stand von Wissenschaft und Technik zu nationalen und internationalen Anforderungen an und Merkmalen von Sicherungskultur ermittelt. Aspekte, die die Sicherungskultur hinsichtlich Informationssicherheit betreffen, sowie relevante Anforderungen und Merkmale, die auch für die Informationssicherheit von Bedeutung sind, wurden herausgearbeitet.

In einem nächsten Schritt wurden anhand der ermittelten Erkenntnisse Kriterien, die für die „good practices“ im Rahmen der Sicherungskultur hinsichtlich Informationssicherheit berücksichtigt werden sollten, erarbeitet. Ziel war die Entwicklung einer Liste von Kriterien, anhand derer Verbesserungspotential in der Sicherungskultur hinsichtlich Informationssicherheit aufgedeckt werden können.

Anhand dieser Kriterienliste wurde schließlich ein Fragebogen entwickelt, der alle Fragen enthält, die z. B. im Rahmen von Selbsteinschätzungen oder Audits zur Überprüfung der Sicherungskultur hinsichtlich Informationssicherheit von Interesse sind.

2 Stand von Wissenschaft und Technik

Zu den Grundprinzipien des Verhaltenskodex für die Sicherheit und Sicherung radioaktiver Strahlenquellen der IAEA /IAE 04/ zählt u. a., dass jeder Staat zum Schutz des Einzelnen, der Gesellschaft und der Umwelt geeignete Maßnahmen ergreifen sollte, um die Förderung der Sicherheits- und der Sicherungskultur zu gewährleisten.

Nach /IAE 06/ sollen alle Organisationen, die an der Umsetzung des physischen Schutzes beteiligt sind, der Sicherheitskultur, ihrer Entwicklung und Aufrechterhaltung den gebührenden Vorrang einräumen, um ihre wirksame Umsetzung in der gesamten Organisation sicherzustellen.

Nachfolgend wird zunächst auf die verschiedenen Definitionen der Sicherheitskultur, Sicherungskultur und der Informationssicherheit eingegangen und dargelegt, welche Definition im Rahmen dieses Vorhabens verwendet wurde. Anschließend werden die im Rahmen dieses Vorhabens erarbeiteten Erkenntnisse zur Sicherheits-, Sicherungs- und Informationssicherheitskultur mit Fokus auf das Thema dieses Vorhabens zusammengefasst.

2.1 Definition der Begriffe Sicherheitskultur, Sicherungskultur, Informationssicherheit

In diesem Abschnitt werden für die zentralen Begriffe Sicherheitskultur, Sicherungskultur und Informationssicherheit, die innerhalb dieses Berichtes verwendet werden, die gängigen Definitionen aus dem nationalen und internationalen Kontext aufgeführt und, wo notwendig, voneinander abgegrenzt. Insbesondere die Verwendung und Abgrenzung der Begriffe Sicherheit und Sicherung in der Nuklearbranche, sowie der Verwendung des Begriffes Informationssicherheit, der in der Nuklearbranche in den Bereich der Sicherung fällt, kann in diesem Zusammenhang oft zu Verwirrungen führen. Von daher ist es notwendig die Begriffe so zu definieren, wie sie innerhalb des Berichtes zu verstehen sind.

2.1.1 Sicherheitskultur

Der Begriff Sicherheitskultur, wird in diesem Bericht so verstanden, wie er im internationalen nuklearen Kontext durch die IAEA (safety culture) und im nationalen Kontext

innerhalb des nuklearen Regelwerks verwendet wird. Die Definitionen sind nachfolgend aufgeführt.

Definition nach IAEA Glossary 2022 /IAE 22/:

- Die Gesamtheit der Eigenschaften und Einstellungen von Organisationen und Einzelpersonen, die dafür sorgen, dass Schutz- und Sicherheitsfragen die ihrer Bedeutung entsprechende Aufmerksamkeit erhalten.

Definition nach IAEA Safety Fundamentals No. SF-1 /IAE 06b/:

- Eine Sicherheitskultur, die die Einstellungen und das Verhalten aller betroffenen Organisationen und Personen in Bezug auf die Sicherheit bestimmt, muss in das Managementsystem integriert werden. Die Sicherheitskultur umfasst:
  - Individuelles und kollektives Engagement für die Sicherheit seitens der Führung, des Managements und des Personals auf allen Ebenen;
  - Verantwortlichkeit von Organisationen und Einzelpersonen auf allen Ebenen für die Sicherheit;
  - Maßnahmen zur Förderung einer hinterfragenden und lernenden Haltung und zur Selbstgefälligkeit in Bezug auf die Sicherheit zu verhindern

Definition nach IAEA Safety Series No. 75 INSAG-4 /IAE 91/:

- *Sicherheitskultur ist die Zusammenstellung aller Merkmale und Einstellungen in Organisationen und von Einzelpersonen, die sicherstellt, dass Themen der nuklearen Sicherheit die oberste Priorität erhalten, die sie aufgrund ihrer Signifikanz verdienen.*

Definition gemäß den Sicherheitsanforderungen an Kernkraftwerke (SiAnf) /BMU 15/ und KTA 1402 /KTA 17/:

- *Die Sicherheitskultur ist durch eine, für die Gewährleistung der Sicherheit der Anlage erforderliche, sicherheitsgerichtete Grundhaltung, Verantwortung und Handlungsweise aller Mitarbeiter bestimmt. Sicherheitskultur umfasst dazu die Gesamtheit der Eigenschaften und Verhaltensweisen innerhalb eines Unternehmens und beim Einzelnen, die dazu dienen, dass die nukleare Sicherheit als eine übergeordnete Priorität die Aufmerksamkeit erhält, die sie aufgrund ihrer Bedeutung erfordert. Sicherheitskultur betrifft sowohl die Organisation als auch die Einzelpersonen.*

Wesentlich an den Definitionen ist, dass Sicherheitskultur alle Einstellungen und Verhaltensweisen sowohl von der Organisation als auch von Einzelpersonen umfasst, die relevant für die nukleare Sicherheit sind.

Innerhalb des IT-Grundschutz Kompendiums des Bundesamts für Sicherheit in der Informationstechnik (BSI) /BSI 22/, welches auch eine wichtige Informationsquelle für diesen Bericht darstellt, wird der Begriff Sicherheitskultur ebenfalls verwendet. Die Verwendung weicht jedoch von den oben aufgeführten Definitionen der nuklearen Sicherheitskultur ab. Zur Vollständigkeit und zur Diskussion der Abgrenzung der unterschiedlich verwendeten Begriffe ist die Definition aus /BSI 22/ im Folgenden aufgeführt.

Definition im IT-Grundschutz Kompendium des BSI /BSI 22/:

- ***Sicherheitskultur:*** *Der Begriff Sicherheitskultur umfasst die sicherheitsbezogenen Einstellungen, Werte und grundlegenden Überzeugungen einer Institution und aller ihrer Mitarbeiter. Zur Sicherheitskultur gehört auch, wie offen der Umgang mit Fragen zur Informationssicherheit in der Institution gelebt wird. So ist für die effektive und effiziente Behandlung von Sicherheitsvorfällen eine vertrauensvolle und offene Kommunikationskultur wichtig, damit Sicherheitsvorfälle auch umgehend weitergemeldet und lösungsorientiert angegangen werden.*

    - *Wie ist der Umgang in der Behörde oder dem Unternehmen mit geschäftsrelevanten Informationen und mit Risiken generell? Ist die Institution eher risiko-orientiert oder eher risikovermeidend? Werden Informationen eher freizügig oder nur restriktiv weitergegeben?*

    - *Wie sind die Anforderungen an Genauigkeit und Präzision? Sind kleinere Fehler beispielsweise in Texten tragbar, weil diese ohnehin noch mehrere Abstimmprozesse durchlaufen müssen? Kann ein Eingabefehler bereits zu folgenschweren Schäden führen?*

    - *Wie sind die Ansprüche an Verfügbarkeit? Gibt es eine Vielzahl enger Termine? Können Bearbeitungszeiten für Anfragen und Geschäftsprozesse flexibel festgelegt werden? Sind kleinere Terminüberschreitungen oder -änderungen im Allgemeinen tragbar oder führen sie zu harten Konsequenzen?*

    Stark beeinflusst wird die Sicherheitskultur einer Institution davon, in welcher Branche diese tätig ist. In Hochsicherheitsbereichen wird naturgemäß weniger offen mit Informationen umgegangen als in Forschungseinrichtungen.

Aus Sicht der GRS kann die oben aufgeführte Definition im Kontext der Nuklearbranche als eine Kultur der Informationssicherheit bezeichnet werden und fällt damit eher in den Bereich der nuklearen Sicherungskultur.

2.1.2 Sicherungskultur

Der Begriff Sicherungskultur, wird in diesem Bericht so verstanden, wie er im internationalen nuklearen Kontext durch die IAEA (security culture) verwendet wird. Die Definition der Sicherungskultur der IAEA orientiert sich stark an der IAEA-Definition der Sicherheitskultur. Ebenso werden auch viele Konzepte zur Sicherheitskultur sinngemäß auf die Sicherungskultur übertragen. Die Definition ist nachfolgend aufgeführt.

Definition der nuklearen Sicherungskultur aus IAEA Nuclear Security Series No. 7 /IAE 08/:

- *Die Zusammenstellung von Merkmalen, Einstellungen und Verhaltensweisen von Einzelpersonen, Organisationen und Institutionen, die als Mittel zur Unterstützung und Verbesserung der nuklearen Sicherung dient.*

2.1.3 Schnittstelle zwischen Sicherheit und Sicherung

Die nachfolgenden Definitionen aus IAEA INSAG-24 „The Interface between Safety and Security at Nuclear Power Plants“ /IAE 10/ zeigen die unterschiedlichen Ziele auf, die durch die nukleare Sicherheit bzw. Sicherung verfolgt werden.

- **(Nuclear) safety:**

  Das Erreichen von ordnungsgemäßen Betriebsbedingungen, die Verhütung von Unfällen oder die Milderung von Unfallfolgen, was zum Schutz der Arbeiter, der Öffentlichkeit und der Umwelt vor ungebührlichen Strahlengefahren führt.

- **(Nuclear) security:**

  Die Verhinderung und Aufdeckung von und Reaktion auf Diebstahl, Sabotage, unbefugten Zugang, illegale Weitergabe oder andere böswillige Handlungen im Zusammenhang mit Kernmaterial, anderen radioaktiven Substanzen oder den damit verbundenen Einrichtungen.

Einen ähnlichen Vergleich der Definition findet man in /WIN 16a/:

- **Nukleare Sicherheit**

  befasst sich mit der Schaffung und Anwendung eines hervorragenden Managements, der Auslegung und des Betriebs von Anlagen zum Schutz von Menschen und Umwelt vor Unfällen, Anlagenstörungen und menschlichem Versagen.

- **Nukleare Sicherung**

  befasst sich mit allen Aktivitäten oder Systemen, die zum Schutz von Kernmaterial und hochradioaktivem Material vor unbefugtem Zugang, Diebstahl, Abzweigung oder Sabotage beitragen, einschließlich u. a. Bewachung, physischer Schutz, Anlagenauslegung, Personalüberprüfung, IT-Sicherheit, technische Maßnahmen usw.

2.1.4 IT-Sicherheit und Informationssicherheit

Für die IT-Sicherheit bestehen sowohl national als auch international verschiedene Begrifflichkeiten und Definitionen, die im Folgenden zunächst dargestellt werden.

2.1.4.1 BSI

Das BSI-Kompendium enthält keine Definition der IT-Sicherheit oder der IT. Der Begriff „Informationstechnik“ wird im Leitfaden zur Basisabsicherung nach IT-Grundschutz /BSI 17/ mit dem gleichen Wortlaut wie in der Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungskategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT) definiert.

- ***Informationstechnik (IT)*** *umfasst alle technischen Mittel, die der Verarbeitung oder Übertragung von Informationen dienen. Zur Verarbeitung von Informationen gehören Erhebung, Erfassung, Nutzung, Speicherung, Übermittlung, programmgesteuerte Verarbeitung, interne Darstellung und die Ausgabe von Informationen*. /BSI 17/

Auch wenn der Begriff Informationstechnik an der ein oder anderen Stelle im BSI-Grundschutzkompendium enthalten ist, findet sich hierfür keine Definition. Stattdessen verwendet das BSI verstärkt den Begriff „Informationssicherheit“, der im IT-Grundschutzkompendium /BSI 22/ wie folgt definiert ist:

- ***Informationssicherheit*** *hat den Schutz von Informationen als Ziel. Dabei können Informationen sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Schutzziele oder auch Grundwerte der Informationssicherheit sind*

Vertraulichkeit, Integrität und Verfügbarkeit. Viele Anwender ziehen in ihre Betrachtungen weitere Grundwerte mit ein.

- ***Integrität*** *bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf „Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf „Informationen" angewendet. Der Begriff „Information" wird dabei für Daten verwendet, denen je nach Zusammenhang bestimmte Attribute wie z.B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.*

- ***Vertraulichkeit*** *ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.*

- *Die* ***Verfügbarkeit*** *von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.*

Darüber hinaus werden im BSI-Grundschutzkompendium folgende Begriffe definiert, die mit der IT-Sicherheit in Verbindung gebracht werden können:

- ***Cyber-Sicherheit*** *befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierend Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Häufig wird bei der Betrachtung von Cybersicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt*. /BSI 22/

- ***IT-Systeme*** *sind technische Anlagen, die der Informationsverarbeitung dienen oder eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.*

2.1.4.2 DIN

In DIN EN IEC 62645 /DIN 21/, die Anforderungen an die Cybersicherheit für leittechnische und elektrische Systeme in Kernkraftwerken stellt, wird der Begriff Cybersicherheit anstelle von Informationssicherheit oder IT-Sicherheit verwendet. Er ist wie folgt definiert /DIN 21/:

- *Satz von Tätigkeiten und Maßnahmen, die darauf abzielen Folgendes zu verhindern, zu entdecken und darauf zu reagieren:*
  - *böswillige Veränderungen (Integrität) von Funktionen, die die Ausführung oder Unversehrtheit der durch programmierbare digitale leittechnische Systeme zu erbringenden Dienste beeinträchtigen können (einschließlich Kontrollverlust), was zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnte;*
  - *böswilliges Zurückhalten oder Verhindern von Zugriff auf oder Austausch von Informationen, Daten oder Ressourcen (einschließlich Anzeigeverlust), was die Ausführung der durch leittechnische Systeme zu erbringenden Dienste beeinträchtigen könnte (Verfügbarkeit), was zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnte;*
  - *böswillige Offenlegung von Informationen (Vertraulichkeit), was dazu benutzt werden könnte, böswillige Handlungen vorzunehmen, die zu einem Störfall, einer unsicheren Situation oder Leistungsverminderung der Anlage führen könnten;*

2.1.4.3 IAEA

In IAEA NSS No. 17-T /IAE 11/ werden folgende Begriffe definiert:

- **Computer Security**
  - *A particular aspect of information security that is concerned with computer based systems, networks and digital systems.*
- **Information Security**
  - *The preservation of the confidentiality, integrity and availability of information.*
  - *Confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities or processes*

- *Integrity: The property of protecting the accuracy and completeness of assets.*
- *Availability: The property of being accessible and usable upon demand by an authorized entity.*

- *Note: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.*

2.1.4.4 NIST

Das US-amerikanische National Institute of Standards and Technology (NIST) definiert in NIST-800-30 /NIS 12/ den Begriff **Information Technology** wie folgt

- *Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.*

Das **Information System** wird definiert als

- *A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.*

Der Begriff **Information Security** wird in /NIS 12/ vergleichbar zur Definition der Informationssicherheit des BSI und der IT-Sicherheit der SEWD-Richtlinie definiert:

- *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.*
- *Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*
- *Integrity: Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.*
- *Availability: Ensuring timely and reliable access to and use of information.*

2.1.4.5 Zusammenfassung

Die Darstellung der Definitionen in den vorangegangenen Teilkapiteln zeigt auf, dass in verschiedenen Regelwerken unterschiedliche Begriffe für die IT- oder Informationssicherheit verwendet werden. Oftmals sind die Definitionen jedoch vergleichbar. Im Wesentlichen zeigt sich, dass zwischen Informationen und Informationstechnik oder IT-Systemen unterschieden wird. Im Rahmen dieses Vorhabens wird der Ansatz der SEWD-Richtlinie verfolgt, die in ihrer Definition der IT-Sicherheit sowohl Informationen als auch Informationstechnik adressiert. Da der Begriff „Informationssicherheit" international einheitlicher verwendet wird als der Begriff der IT-Sicherheit, wird auch im Rahmen dieses Vorhabens im weiteren Verlauf der Begriff Informationssicherheit verwendet, der wie folgt definiert ist:

- ***Informationssicherheit*** *hat den Schutz von Informationen und Informationstechnik zum Ziel. Informationen können dabei sowohl auf Papier, in Rechnern oder auch in Köpfen gespeichert sein. Die Grundwerte der Informationssicherheit sind Vertraulichkeit, Integrität und Verfügbarkeit.*

Konsistent dazu wird in diesem Bericht für die zugehörige Kultur der Begriff Informationssicherheitskultur verwendet und nicht mehr der ursprünglich verwendete Begriff „Sicherungskultur für Informationstechnologie".

2.2 Sicherheitskultur

2.2.1 Aufbereitung der Erkenntnisse aus den Aktivitäten der GRS

Die GRS wurde 2011 durch das BfS damit beauftragt, einen Leitfaden zur Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch Genehmigungs- und Aufsichtsbehörden zu entwickeln. Als Grundlage hierfür wurde zunächst der Stand von Wissenschaft und Technik zu Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur erfasst und in einem Bericht (GRS-A-3795) zusammengestellt /GRS 15a/. Der Leitfaden wurde in einem separaten Bericht (GRS-A-3792) veröffentlicht /GRS 15b/. Darüber hinaus wurde in einem Bericht von 2016 (GRS-A-3862) die Erhaltung und Weiterentwicklung der Sicherheitskultur in Kernkraftwerken unter Berücksichtigung der nach dem Unfall von Fukushima geänderten Randbedingungen der Kernenergienutzung in Deutschland diskutiert. Im Folgenden werden die Arbeiten dieser Berichte kurz zusammengefasst.

2.2.1.1 GRS-A-3795: Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur

Im Bericht GRS-A-3795 /GRS 15a/ wird der Stand von Wissenschaft und Technik zum Thema Sicherheitskultur dargestellt. Der Bericht war Teil eines Vorhabens, in dem ein Leitfaden zur Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch die Genehmigungs- und Aufsichtsbehörden entwickelt wurde.

GRS-A-3795 behandelt ausschließlich das Thema der Sicherheitskultur und geht nicht auf die Sicherungskultur ein. Es diente für dieses Vorhaben als Grundlage für das Verständnis der Sicherheitskultur und die hierzu in diesem Vorhaben durchgeführten Arbeiten. Im Folgenden werden die Aspekte aus /GRS 15a/ kurz zusammengefasst, die für dieses Vorhaben von Relevanz waren.

Kap. 4 geht zunächst auf die Definition und die Bedeutung der Sicherheitskultur nach IAEA-Regelwerk und den Sicherheitsanforderungen für Kernkraftwerke /BMU 12/ ein. In diesem Zusammenhang werden weitere Begriffe wie „Handeln“, „Unternehmen“ und „Attitude“ im Sinne von „Einstellung“ oder „Verhaltensweisen“ diskutiert, die im engen Zusammenhang mit dem Begriff der Sicherheitskultur stehen.

In Kap. 4.3 und 4.4 wird festgestellt, dass die IAEA einen engen Bezug zwischen Sicherheitskultur und Sicherheitsmanagement herstellt. Demnach hat zum Managementsystem eine Sicherheitskultur zu gehören, die Einstellungen und Verhaltensweisen in Unternehmen bzw. Institutionen und von Personen bestimmt, soweit diese Einstellungen, Verhaltensweisen, Unternehmen, Institutionen und Personen mit der Sicherheit zu tun haben.

Kap. 4.5 und 4.6 geht auf die Charakteristika und Attribute der Sicherheitskultur nach /IAE 09/ ein und übersetzt sie. Diese Übersetzung wurde im Rahmen dieses Vorhabens verwendet (siehe Anhang A).

Kap. 4.7 diskutiert darauf aufbauend den Zusammenhang zwischen Management, Sicherheitskultur, Handeln und Sicherheit nach Definition der IAEA.

Darüber hinaus werden die Attribute und Charakteristika nach /IAE 09/ im Zusammenhang mit einem gebräuchlichen Modell aus der Zuverlässigkeitsforschung und -bewertung diskutiert. Dieses Modell betrachtet die Ausführung bzw. Unterlassung

erforderlicher Aktionen als Funktion äußerer und innerer Rahmenbedingungen (z.B. Sicherheitspolitik, Organisationsstrukturen, Arbeitsbedingungen etc.) dieser Aktion. In Kap. 4.7 wurden die Charakteristika und Attribute entsprechend dieser Unterscheidung neu kategorisiert.

Die Überlegungen der IAEA zur Sicherheitskultur basieren auf dem Ansatz zur Unternehmenskultur von Edgar Schein. Daher werden seine Arbeiten abschließend in Kap. 5 ausführlich dargestellt und diskutiert.

2.2.1.2 GRS-A-3792: Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch die Genehmigungs- und Aufsichtsbehörden

Der Bericht GRS-A 3792 /GRS 15b/ „Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch die Genehmigungs- und Aufsichtsbehörden“ enthält einen Leitfaden, der bei der bundesweit einheitlichen Erfassung und Beurteilung wesentlicher Aspekte der Sicherheitskultur deutscher Kernkraftwerke beim Restbetrieb, Nachbetrieb und Rückbau unterstützen soll. Dabei konzentriert er sich auf die Aktionen und Vorkehrungen, mit denen Führungskräfte die Sicherheitskultur in ihrem Verantwortungsbereich stärken können (die IAEA führt dies unter dem Aspekt „leadership for safety culture“).

GRS-A 3792 geht nicht auf die Sicherungskultur ein. Es diente als Grundlage für das Verständnis der Sicherheitskultur und die hierzu in diesem Vorhaben durchgeführten Arbeiten. Im Folgenden werden die Aspekte aus GRS-A 3792 kurz zusammengefasst, die für dieses Vorhaben von Relevanz waren.

Die im Rahmen des Vorhabens gewonnenen Erkenntnisse aus der Fachliteratur erlauben es nach /GRS 15b/, die Erfassung und Beurteilung sicherheitskultureller Faktoren auf Aktionen und Vorkehrungen zu konzentrieren, die direkter Beobachtung zugänglich sind und von denen man erwarten kann, dass sie beobachtbare Leistungen durch ihre Wirkung auf die nicht direkt beobachtbare Leistungs- und Einsatzbereitschaft fördern. Aufgrund dieser Wirkung sind die betreffenden Aktionen und Vorkehrungen positiv zu beurteilen. Der Leitfaden in GRS-A 3792 ist Ergebnis einer systematischen Auswahl der wesentlichen Aktionen und Vorkehrungen dieser Art.

Der Leitfaden unterscheidet insgesamt 17 Arten von Aktionen und Vorkehrungen, die in 5 Themengruppen gebündelt sind (siehe **Fehler! Ungültiger Eigenverweis auf Textmarke.**). Zu jeder Gruppe enthält der Leitfaden Aktionspunkte und Fragen, die zur Klärung dieses Themas beitragen können. Diese Aktionspunkte und Fragen führen nach empirisch belegten Erkenntnissen aus der Fachliteratur dazu, die psychologischen Faktoren (Grundannahmen i.S.v. E. Schein) zu stärken, von denen eine zuverlässige Erfüllung von Personalaufgaben im Unternehmen abhängt /GRS 15b/. Die in Tab. 2.1 enthaltenen Themen wurden bei der Entwicklung des Kriterienkatalogs berücksichtigt.

Tab. 2.1 Themen, die im Leitfaden /GRS 15b/ erfasst werden

Gruppe	Art der Aktion/Vorkehrung	Führungskräfte aller Ebenen der Unternehmenshierarchie sollen in ihren jeweiligen Zuständigkeitsbereichen…
Rahmenbedingungen des Handelns schaffen	1. Vorrang der Sicherheit	...den Geführten Politik und Ziele von Unternehmen und Anlage, das Betriebsreglement und ihre Bedeutung für zuverlässiges, auf Sicherheit bezogenes Handeln genau vermitteln. • …unmissverständlich den Vorrang der Sicherheit vor anderen Zielen ausreichend oft und nachdrücklich propagieren
	2. Arbeitsbedingungen	…bestmögliche Bedingungen, zuverlässiges, auf Sicherheit gerichtetes Handeln in Bezug auf Mensch, Organisation und Technik schaffen (u.a. kein Zeitdruck, gute Arbeitsmittel). • …bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben schaffen. • …alle ihre Möglichkeiten nutzen, den erforderlichen Bestand qualifizierten Personals im Unternehmen und auf den Anlagen zu erhalten
	3. Qualifikation	…Kompetenz, Handeln und Leistung der Geführten unvoreingenommen beurteilen und geeignete Weiterentwicklungsmöglichkeiten eröffnen.
Personalführung	4. Klare Vorgaben	…eindeutige Entscheidungen treffen, genaue Anweisungen erteilen und präzise Informationen geben, insbesondere in Bezug auf Sicherheit und Zuverlässigkeit. • …sich bei ihren Entscheidungen, Anweisungen und Auskünften klar und eindeutig ausdrücken.

Gruppe	Art der Aktion/Vorkehrung	Führungskräfte aller Ebenen der Unternehmenshierarchie sollen in ihren jeweiligen Zuständigkeitsbereichen…
	5. Vorbildfunktion	…durch das eigene zuverlässige, auf Sicherheit gerichtete Handeln Vorbild der Geführten sein. • …den Vorrang der Sicherheit bei ihren Entscheidungen und Handlungen eindeutig vorleben.
	6. Nachfragen der Geführten	…Geführte ermutigen und unterstützen, Fragen und Bedenken zu Arbeit, Sicherheit und Zuverlässigkeit unverzüglich und rückhaltlos zu äußern. • …für Rat, Hinweise, Fragen, Bedenken und Kritik anderer offen sein, Klärungsbedürftiges sachlich-wohlwollend klären und Verbesserungsbedürftiges verbessern (auch 7. zugeordnet)
	7. Reaktion auf Nachfragen	…Fragen und Bedenken der Geführten zu Arbeit, Sicherheit und Zuverlässigkeit sachlich, stichhaltig und vor Beginn betroffener Arbeiten klären bzw. ausräumen.
	8. Überwachen	…zuverlässiges, auf Sicherheit gerichtetes Handeln der Geführten auch vor Ort wirksam überwachen und, falls erforderlich, unterstützend oder berichtigend eingreifen. • …vor Ort ausreichend oft präsent sein, um sich aus erster Hand zu informieren und die korrekte Erfüllung von Aufgaben zu unterstützen.
Fehler, Verbesserungen, Vorkehrungen angehen	9. Wachsamkeit der Geführten	…Geführte ermutigen und unterstützen, auf Handlungen, Beinahe-Fehler und Gegebenheiten, die Sicherheit und Zuverlässigkeit zuwiderlaufen, zu achten, wo geboten: berichtigend einzugreifen und ihre Erkenntnisse rückhaltlos, zeitnah und sachlich zu berichten. • …den offenen Bericht über Fehler, Beinahe-Fehler, Fehlermöglichkeiten und Schwachstellen fördern, Ursachen und (reale bzw. mögliche) Folgen unvoreingenommen untersuchen sowie für eigene Fehler und deren Folgen rückhaltlos einstehen. (auch 10. Zugeordnet)
	10. Fehler der Führungskraft	…für eigene Fehler und ihre Folgen eindeutig die Verantwortung zu übernehmen.
	11. Fehlerbehandlung	…Fehler und Verbesserungsbedürftiges zeitnah und unvoreingenommen untersuchen, Ursachen möglichst genau bestimmen und geeignete Vorsorge treffen.

Gruppe	Art der Aktion/Vorkehrung	Führungskräfte aller Ebenen der Unternehmenshierarchie sollen in ihren jeweiligen Zuständigkeitsbereichen…
		• …gewonnene Erkenntnisse für die Entwicklung und Implementierung wirksamer Vorkehrungen und Verbesserungen nutzen (auch 12. + 13. Zugeordnet)
	12. Verbesserungsvorschläge	…Geführte ermutigen und unterstützen, rückhaltlos alle ihre Ideen zu äußern, wie die Sicherheit und die Zuverlässigkeit zu verbessern sind.
	13. Lernende Organisation	…Erkenntnisse aus Äußerungen der Geführten (Fragen, Bedenken, Berichte, Vorschläge, usw.), Betriebserfahrung, eigenen Beobachtungen und anderen Quellen zeitnah für Vorkehrungen nutzen, die Sicherheit und Zuverlässigkeit erhöhen.
Anerkennung und Sanktionierung	14. Anerkennung	…die Leistung der Geführten zeitnah im angemessenen Verhältnis zu real erbrachten Leistungen so anerkennen, dass Sicherheit und Zuverlässigkeit gestärkt werden. • …Leistungen der Mitarbeiter angemessen so anerkennen, dass der Vorrang der Sicherheit vor anderen Zielen unmissverständlich zum Ausdruck kommt.
	15. Sanktionierung	…Handeln, das aus stichhaltigen Gründen zu sanktionieren ist, zeitnah gebührend ahnden.
Sozialverhalten	16. Arbeitsklima	…ein Arbeitsklima mit und zwischen den Geführten fördern, das zuverlässiges, auf Sicherheit gerichtetes Handeln unterstützt. • …zu Ankündigungen und Zusagen stehen, alle im Unternehmen mit Respekt behandeln und auf den respektvollen Umgang ihrer Mitarbeiter mit anderen hinwirken. (auch 17. Zugeordnet)
	17. Verlässlichkeit	…zu Ankündigungen und Zusagen stehen.

2.2.1.3 GRS-A-3862: Erhaltung und Weiterentwicklung der Sicherheitskultur in Kernkraftwerken unter Berücksichtigung der aktuellen Randbedingungen der Kernenergienutzung in Deutschland

Das dem Bericht GRS-A-3862 /GRS 16/ zugrundeliegende Vorhaben hatte das Ziel, herauszuarbeiten, inwieweit eine Sicherheitskultur förderbar ist, welche Möglichkeiten der

Förderung einer Sicherheitskultur bestehen und wie man vor der Implementierung die Wirksamkeit einer beabsichtigten Förderung der Sicherheitskultur beurteilen kann. Dabei waren die Herausforderungen zu berücksichtigen, die sich während der Restlaufzeiten, der Nachbetriebsphase und des Rückbaus der Anlagen für die Sicherheitskultur und ihre Förderung ergeben. In Anhang A von /GRS 16/ werden die Ergebnisse des Vorhabens im Zusammenhang mit den Charakteristika und Attributen nach IAEA GS-G 3.5 /IAE 09/ diskutiert. In diesem Zusammenhang wird in /GRS 16/ beschrieben, wie die Attribute und Charakteristika der Sicherheitskultur nach IAEA GS-G 3.5 /IAE 09/ in die Kategorien Mensch, Technik und Organisation unter Berücksichtigung der Ebenen einer Unternehmenskultur nach Edgar Schein eingeordnet werden können. Die Zuordnung ist in Tab. 2.2 dargestellt.

Tab. 2.2 Struktur der Klassifizierung sicherheitskultureller Faktoren nach /GRS 16/

MTO-System Ebenen	**Mensch**	**Technik**	**Organisation**
Artefakte	Direkt beobachtbares Verhalten	Gebäude, Maschinen, Werkzeuge, usw.	Strukturen und Prozesse in Einklang mit den Regelungen der formalen Organisation
Wertvorstellungen	Verkündete Ziele, Absichten, usw.		Ziele eines Unternehmens, Ziele einer Gruppe, Rechtfertigung des Handelns (auch nachträglich)
Grundannahmen	Handlungsleitende Werte, ebensolches Wissen, etc.		

Im weiteren Verlauf des Berichts /GRS 16/ wird ein möglicher Prozess zur Förderung der Sicherheitskultur sowie ihr Zusammenhang mit dem integrierten Managementsystem beschrieben und diskutiert. Die aus diesem Bericht gewonnenen Erkenntnisse dienten für dieses Vorhaben als Grundlage für das Verständnis der Sicherheitskultur und die hierzu in diesem Vorhaben durchgeführten Arbeiten.

2.2.2 Erkenntnisse aus dem IAEA-Regelwerk

Nachfolgend wird auf folgende IAEA-Dokumente eingegangen und die für dieses Vorhaben relevanten Informationen zusammengefasst:

- IAEA GS-G 3.5 - The management system for nuclear installations, 2009 /IAE 09/
- IAEA TECDOC 1707 - Regulatory Oversight of Safety Culture in Nuclear Installations, 2013 /IAE 13/
- IAEA Working Document: A harmonized Safety Culture Model, 2020 /IAE 20/

2.2.2.1 GS-G 3.5: Managementsystem für kerntechnische Einrichtungen

In IAEA GS-G 3.5 /IAE 09/ werden Empfehlungen und Anleitungen gegeben, die zur Errichtung, Implementierung, Bewertung und kontinuierlichen Verbesserung eines Managementsystems beitragen. Ein solches Managementsystem soll eingesetzt werden, um eine starke Sicherheitskultur zu fördern und zu unterstützen, indem es

- ein gemeinsames Verständnis der Schlüsselaspekte der Sicherheitskultur innerhalb der Organisation gewährleistet,
- Mittel bereitstellt, mit denen die Organisation einzelne Mitarbeiter und Teams bei der sicheren und erfolgreichen Ausführung ihrer Aufgaben unterstützt
- eine lernende und hinterfragende Haltung auf allen Ebenen der Organisation verstärkt und
- Mittel bereitstellt, mit denen die Organisation kontinuierlich versucht, ihre Sicherheitskultur zu entwickeln und zu verbessern.

IAEA GS-G 3.5 nennt Anforderungen, die ein Managementsystem erfüllen sollte. In diesem Zusammenhang wird auch auf die Sicherheitskultur eingegangen, die eng verknüpft ist mit dem Managementsystem. Nach IAEA GS-G 3.5 hat jede Organisation irgendeine Form von Kultur. Sicherheitskultur ist die Art von Organisationskultur, bei der Sicherheit oberste Priorität hat und als wesentlich für den langfristigen Erfolg der Organisation angesehen wird. Die Sicherheitskultur sollte auf einer Reihe von Sicherheitsüberzeugungen und einem Verhaltenskodex basieren, der die richtige Einstellung zur Sicherheit widerspiegelt, und von allen Personen in der Organisation gemeinsam vertreten wird.

IAEA GS-G 3.5 enthält eine Reihe von Charakteristika und Attributen, die für eine gute Sicherheitskultur herangezogen werden können. Sie dienen dabei sowohl der Erreichung eines gemeinsamen Verständnisses darüber, welche Faktoren in Bezug auf die Sicherheitskultur berücksichtigt werden sollten, als auch zur Bewertung von Stärken und Schwächen einer Organisation im Rahmen einer Selbstbewertung oder durch eine externe Überprüfung. Sie sind in Anhang A aufgeführt.

2.2.2.2 TECDOC 1707: Regulatorische Aufsicht über die Sicherheitskultur in kerntechnischen Anlagen

Das technische Dokument IAEA TECDOC 1707 /IAE 13/ beschreibt, dass Unternehmenskultur sowohl physische Manifestationen wie Verhalten, Symbole und Worte als auch nicht sichtbaren Aspekte wie Normen, Werten, Gedanken und Gefühlen umfasst, die von den Menschen der Organisation geteilt werden und die die Art und Weise steuern, wie sie innerhalb und außerhalb der Organisation miteinander interagieren. /IAE 13/ verweist an dieser Stelle auf Edgar Schein, dessen Modell von drei Ebenen ausgeht, die er als Artefakte („Artefacts“), Wertvorstellungen („Espoused Values“) und Grundannahmen („Basic Assumptions“) bezeichnet.

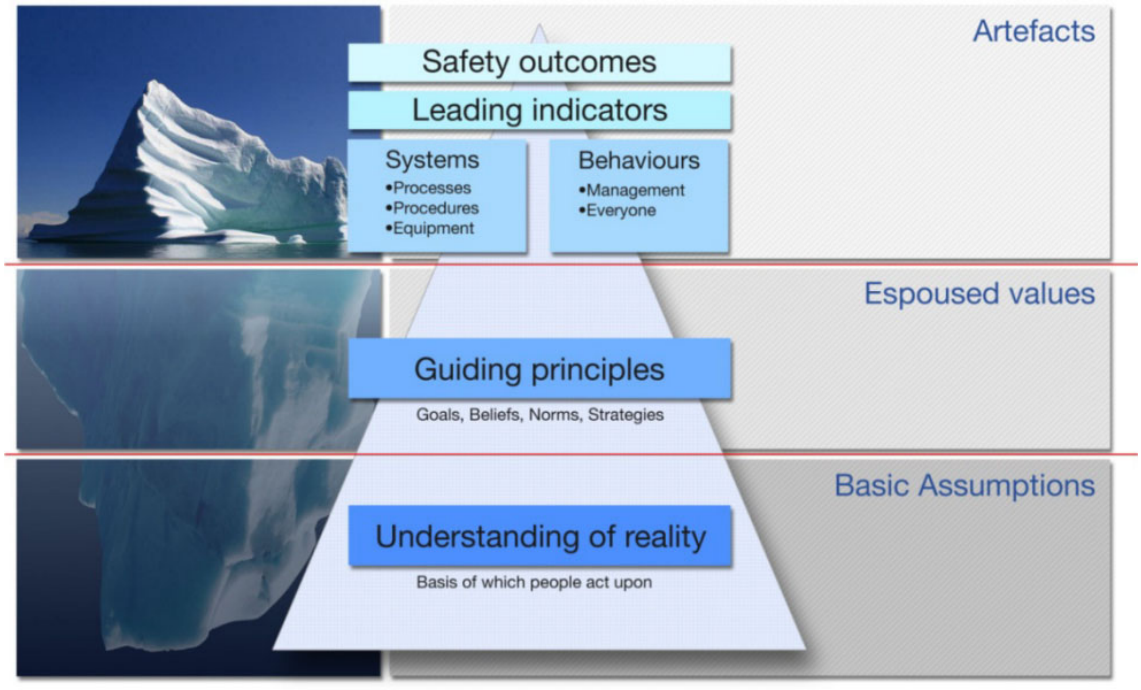

Abb. 2.1 Ebenen des Modells nach Edgar Schein /IAE 13/

Darüber hinaus befasst sich TECDOC 1707 mit der Rolle der regulatorischen Aufsicht im Zusammenhang mit der Sicherheitskultur. Demnach liegt die Verantwortung für die

Sicherheit bei der Person oder Organisation, die für die Einrichtungen und dort ausgeführten Tätigkeiten verantwortlich ist. Daher wird von den Betreibern gefordert, dass sie eine starke Sicherheitskultur in ihrer Organisation fördern. Die Aufgabe der Aufsichtsbehörde ist in diesem Zusammenhang sicherzustellen, dass der Betreiber dieser Verantwortung nachkommt. Sie ergreift entsprechend Maßnahmen, wenn sie feststellt, dass das Sicherheitsmanagementsystem des Betreibers nicht ausreichend wirksam ist oder das Sicherheitsverständnis der Organisation nachlässt. Hierfür beschreibt /IAE 13/ einen Prozess zur Überwachung der Sicherheitskultur.

Der Bericht enthält keine Informationen, die im Verlauf dieses Vorhabens verwendet wurden, diente jedoch als Grundlage für das Verständnis der Sicherheitskultur und die hierzu in diesem Vorhaben durchgeführten Arbeiten.

2.2.2.3 IAEA: Ein harmonisiertes Modell der Sicherheitskultur

Im Arbeitsdokument der IAEA „*A harmonized Safety Culture Model*“ /IAE 20/ werden die verschiedenen Sichtweisen der IAEA sowie von WANO (World Association of Nuclear Operators) und INPO (Institute of Nuclear Power Operations) zur Sicherheitskultur beleuchtet. In dem Dokument werden Merkmale und Attribute beschrieben, die in Organisationen mit einer gesunden Sicherheitskultur vorhanden sind. Viele der Charakteristika und Attribute des Modells nach IAEA und von WANO finden sich in dieser Darstellung wieder. Es werden die in Tab. 2.3 dargestellten Charakteristika und Attribute beschrieben. Sie wurden bei der Erstellung der Kriterien-Matrix mitbetrachtet.

Tab. 2.3 Liste mit Charakteristika und Attributen nach /IAE 20/

Charakteristik	Attribute
Individual Responsibility (Individuelle Verantwortung) Alle Personen sind persönlich für die Sicherheit verantwortlich. Jeder Einzelne fühlt sich verpflichtet, die Standards und Erwartungen zu kennen und rigoros zu erfüllen.	**IR.1 Adherence (Einhaltung)** Einzelpersonen verstehen und akzeptieren die Bedeutung von Standards, Prozessen, Verfahren, Erwartungen und Arbeitsanweisungen. Einzelpersonen auf allen Ebenen der Organisation halten sich an Standards und Erwartungen. **IR.2 Ownership (Eigentum)** Einzelpersonen zeigen in ihrem Verhalten und in ihren Arbeitspraktiken persönliches Engagement für Sicherheit. Sie fördern sicheres Verhalten in allen Situationen und schulen andere bei Bedarf. **IR.3 Collaboration (Zusammenarbeit)**

Charakteristik	Attribute
	Einzelpersonen und Arbeitsgruppen helfen sich gegenseitig beim Erreichen von Zielen, indem sie ihre Aktivitäten innerhalb und über Unternehmensgrenzen hinweg kommunizieren und koordinieren. Der Einzelne versteht und akzeptiert den Wert unterschiedlichen Denkens bei der Optimierung der Sicherheit.
Questioning Attitude (Hinterfragende Haltung) Einzelpersonen bleiben wachsam gegenüber Annahmen, Anomalien, Bedingungen, Verhaltensweisen oder Aktivitäten, die die Sicherheit beeinträchtigen können, und äußern diese Bedenken dann angemessen. Alle Mitarbeiter achten auf Selbstgefälligkeit und vermeiden sie. Sie erkennen an, dass kleinere Probleme Warnzeichen für etwas Bedeutenderes sein können. Einzelpersonen sind sich der Bedingungen bewusst und machen auf potenzielle Schwachstellen aufmerksam und melden diese dann.	**QA.1 Recognize Unique Risks (Einzigartige Risiken erkennen)** Einzelpersonen verstehen die einzigartigen Risiken, die mit Nuklear- und Strahlentechnologie verbunden sind. Sie verstehen, dass die Technologien komplex sind und auf unvorhergesehene Weise mit erheblichen Folgen versagen können. **QA.2 Avoid Complacency (Selbstzufriedenheit vermeiden)** Einzelpersonen erkennen und planen die Möglichkeit von Fehlern, unvorhergesehenen Problemen und unwahrscheinlichen Ereignissen, selbst wenn die Ergebnisse in der Vergangenheit erfolgreich waren. Einzelpersonen erkennen, dass Selbstzufriedenheit oft mit Erfolg einhergeht und bemühen sich ständig, sie bei sich selbst und anderen zu vermeiden. **QA.3 Question Uncertainty (Fragen bei Unsicherheit)** Einzelpersonen stoppen, wenn sie unsicher sind und suchen Rat. Die Situation und die Risiken werden bewertet und gemanagt, bevor fortgefahren wird. **QA.4 Recognize and Question Assumptions (Annahmen erkennen und in Frage stellen)** Personen stellen Annahmen in Frage und sind bereit, unterschiedliche Perspektiven anzubieten, wenn sie glauben, dass etwas nicht richtig ist.
Communication (Kommunikation) Kommunikation unterstützt den Fokus auf Sicherheit. Führungskräfte nutzen formelle und informelle Kommunikation, um häufig die Bedeutung von Sicherheit zu vermitteln. Die Organisation unterhält eine Vielzahl von	**CO.1 Free flow of Information (Freier Informationsfluss)** Einzelpersonen kommunizieren offen und aufrichtig, sowohl nach oben als auch nach unten und im gesamten Unternehmen. Der Informationsfluss nach oben wird als genauso wichtig erachtet wie der Informationsfluss nach unten. **CO.2 Transparency (Transparenz)**

Charakteristik	Attribute
Kommunikationskanälen, einschließlich der direkten Interaktion zwischen Managern und Mitarbeitern. Ein effektiver Dialog wird gefördert. Wirksame Kommunikation zur Unterstützung der Sicherheit ist breit gefächert und umfasst die Kommunikation am Arbeitsplatz, Gründe für Entscheidungen und Erwartungen.	Die Kommunikation mit Aufsichts-, Wirtschaftsprüfungs-, Regulierungsorganisationen und der Öffentlichkeit ist angemessen, professionell und korrekt. **CO.3 Reasons for Decisions (Entscheidungsgründe)** Führungskräfte stellen sicher, dass die Gründe für technische und administrative Entscheidungen den zuständigen Personen rechtzeitig mitgeteilt werden. **CO.4 Expectations (Erwartungen)** Führungskräfte kommunizieren und verstärken häufig die Erwartung, dass Sicherheit gegenüber konkurrierenden Zielen betont wird. **CO.5 Workplace Communication (Kommunikation am Arbeitsplatz)** Kommunikation über Sicherheit ist in alle Arbeitsaktivitäten integriert, damit jeder über die Informationen verfügt, die für ein sicheres und effektives Arbeiten erforderlich sind.
Leader Responsibility (Führungsverantwortung) Führungskräfte zeigen in ihren Entscheidungen und Verhaltensweisen eine Verpflichtung zur Sicherheit. Führungskräfte sind Vorbilder für Sicherheit. Executive und Senior Manager sind die führenden Verfechter der Sicherheit und zeigen ihr Engagement in Wort und Tat. Führungskräfte in der gesamten Organisation setzen ein Beispiel für Sicherheit. Unternehmensrichtlinien betonen die überragende Bedeutung der Sicherheit.	**LR.1 Strategic Alignment (Strategische Ausrichtung)** Führungskräfte etablieren und fördern organisatorische Prioritäten, die Sicherheit über konkurrierende Ziele stellen. Führungskräfte verfolgen einen langfristigen Ansatz für das Geschäft und richten Richtlinien und Maßnahmen aus. Sie betonen, dass ein hohes Maß an Sicherheit erforderlich ist, um ein hohes Produktionsniveau aufrechtzuerhalten. **LR.2 Leader Behaviour (Verhalten von Führungskräften)** Führungskräfte in der gesamten Organisation geben ein Beispiel für Sicherheit. **LR.3 Employee Engagement (Mitarbeiterengagement)** Führungskräfte entwickeln eine abgestimmte und engagierte Belegschaft, die ein positives Umfeld zur Unterstützung der Sicherheit schafft. Führungskräfte suchen die aktive Beteiligung von Einzelpersonen auf allen Ebenen bei der Identifizierung und Lösung von Problemen. Faktoren, die die Arbeitsmotivation und die Arbeitszufriedenheit beeinflussen, werden bei der Entscheidungsfindung berücksichtigt. **LR.4 Resources (Ressourcen)**

Charakteristik	Attribute
	Führungskräfte stellen sicher, dass Personal, Ausrüstung, Verfahren und andere Ressourcen verfügbar und angemessen sind, um die Sicherheit zu gewährleisten. Die Personalpolitik, einschließlich Einstellung, Nachfolgeplanung und Beförderungen, legt großen Wert auf sicherheitsorientiertes Verhalten und Entscheidungen. **LR.5 Field Presence (Präsenz)** Führungskräfte sind häufig in allen Bereichen der Organisation präsent und beobachten die Arbeits- und Materialbedingungen. Sie stellen Fragen, kommunizieren, schulen und stärken Standards und Erwartungen. Führungskräfte hören auf die Bedenken und das Feedback der Belegschaft und handeln entsprechend. **LR.6 Rewards and Sanctions (Belohnungen und Sanktionen)** Führungskräfte stellen sicher, dass Belohnungen und Sanktionen sicherheitsfördernde Einstellungen und Verhaltensweisen fördern. Menschen sind nicht nur für die Ergebnisse verantwortlich, sondern auch dafür, wie sie die Ergebnisse erzielen. **LR.7 Change Management (Änderungsmanagement)** Führungskräfte verwenden einen systematischen Prozess zur Kommunikation und Umsetzung von Veränderungen, damit die Sicherheit nicht gefährdet wird. Die Gründe für die Änderung werden klar kommuniziert. Die Auswirkungen der Änderung auf die Sicherheit werden vor, während und nach der Änderung bewertet. **LR.8 Authorities, Roles and Responsibilities (Autoritäten, Rollen und Verantwortlichkeiten)** Führungskräfte stellen sicher, dass Autoritäten, Rollen und Verantwortlichkeiten klar definiert und verstanden werden.
Decision Making (Entscheidung treffen) Entscheidungen sind systematisch, rigoros, gründlich und umsichtig. Führungskräfte unterstützen konservative Entscheidungen und die Fähigkeit, sich von unvorhergesehenen Umständen schnell zu erholen. Führungskräfte verfolgen den	**DM.1 Systematic Approach (Systematischer Ansatz)** Einzelpersonen verwenden einen konsistenten, systematischen Ansatz, um relevante Faktoren, einschließlich des Risikos, bei der Entscheidungsfindung zu bewerten. Durch einen systemischen Ansatz werden qualitativ hochwertige Informationen aus allen relevanten Quellen gesammelt.

Charakteristik	Attribute
Entscheidungsprozess. Die Verantwortung für die Entscheidungsfindung ist klar.	**DM.2 Conservative Approach (Konservativer Ansatz)** Einzelpersonen treffen umsichtige Entscheidungen anstelle von Entscheidungen, die einfach zulässig sind. Aktionen werden als sicher eingestuft, bevor sie fortfahren, und nicht, bis sie sich als unsicher erwiesen haben. **DM.3 Clear Responsibility (Klare Verantwortung)** Autorität und Verantwortung für Entscheidungen sind spezifisch und klar definiert. **DM.4 Resilience (Resilienz)** Es wird immer eine umsichtige Entscheidungsfindung verwendet, aber im Vorgriff auf unvorhergesehene Situationen, in denen kein Verfahren oder Plan zur Anwendung kommt, entwickeln Organisationen die Fähigkeit zur Anpassung.
Work Environment (Arbeitsumfeld) Vertrauen und Respekt durchdringen die Organisation. In der Organisation wird ein hohes Maß an Vertrauen gepflegt. Unterschiedliche Meinungen werden gefördert, diskutiert und bedacht. Die Mitarbeiter werden über Maßnahmen informiert, die auf ihre Bedenken hin ergriffen wurden.	**WE.1 Respect is evident (Respekt ist offensichtlich)** Alle Personen werden mit Würde, Respekt und Offenheit behandelt und ihre Beiträge werden anerkannt. **WE.2 Opinions are valued (Meinungen werden geschätzt)** Einzelpersonen werden ermutigt, Fragen zu stellen, Bedenken zu äußern und Vorschläge zu machen. Abweichende Meinungen werden erbeten und respektiert. **WE.3 Trust is Cultivated (Vertrauen wird kultiviert)** Vertrauen wird zwischen Einzelpersonen und Arbeitsgruppen in der gesamten Organisation gefördert. Offenheit und Ehrlichkeit werden zwischen Einzelpersonen, zwischen Arbeitsgruppen und in der gesamten Organisation gefördert. **WE.4 Conflicts are resolved (Konflikte werden gelöst)** Konflikte werden mit fairen und transparenten Methoden gelöst. Konflikte werden zeitnah gelöst. **WE.5 Facilities Reflect Respect (Einrichtungen spiegeln Respekt wider)** Hauswirtschaft und materielle Bedingungen spiegeln Respekt gegenüber Mensch und Ausrüstung wider. Die Einrichtungen tragen zu einer produktiven

Charakteristik	Attribute
	Arbeitsumgebung bei und der Haushalt wird aufrechterhalten.
Continuous Learning (Fortlaufendes Lernen) Lernen wird großgeschrieben. Die organisatorische Lernfähigkeit ist gut entwickelt. Die Organisation verwendet eine Vielzahl von Ansätzen, um das Lernen zu stimulieren und die Leistung zu verbessern, einschließlich menschlicher, technischer und organisatorischer Aspekte. Einzelpersonen und Teams sind sehr kompetent und suchen nach Verbesserungsmöglichkeiten.	**CL.1 Constant Examination (Ständige Prüfung)** Die Sicherheit wird regelmäßig durch eine Vielzahl von Techniken überwacht und bewertet, einschließlich unabhängiger und Selbstbewertungen ihrer Programme und Praktiken. Die Sicherheitskultur wird regelmäßig bewertet und weiterentwickelt. **CL.2 Learning from Experience (Aus Erfahrung lernen)** Die Organisation sammelt, evaluiert und setzt relevante interne und externe Erkenntnisse zeitnah und effektiv um. Die gewonnenen Erkenntnisse werden auch mit relevanten Organisationen geteilt. **CL.3 Training (Schulung)** Die Organisation bietet effektive Schulungen und stellt den Wissenstransfer sicher, um eine sachkundige und kompetente Belegschaft zu erhalten. **CL.4 Leadership Development (Führungskräfteentwicklung)** Kompetente Führungskräfte werden durch die Führungskräftetrainings- und Nachfolgemanagementprozesse entwickelt. **CL.5 Benchmarking (Vergleich)** Die Organisation lernt von den Praktiken anderer Organisationen, einschließlich anderer Branchen.
Problem Identification and Resolution (Problemidentifikation und -lösung) Sicherheitsrelevante Probleme werden systematisch identifiziert, umfassend bewertet und entsprechend ihrer Bedeutung zeitnah gelöst. Die Identifizierung und Lösung eines breiten Spektrums von Problemen, einschließlich menschlicher Leistung und organisatorischer Probleme, werden verwendet, um die Sicherheit zu stärken und die Leistung zu verbessern.	**PI.1 Identification (Identifikation)** Es wird eine Methode zum Sammeln von Problemen implementiert. Bei den gesammelten Problemen handelt es sich nicht nur um Hauptprobleme, sondern auch um kleinere Probleme, da sie zu großen Problemen werden können. Einzelpersonen identifizieren Probleme rechtzeitig. Selbstauskunft wird von der Organisation erwartet und geschätzt. **PI.2 Evaluation (Bewertung)** Probleme werden gründlich bewertet, um die zugrunde liegenden Ursachen zu ermitteln und festzustellen, ob das Problem in anderen Bereichen existiert. Probleme werden in einem angemessenen Zeitrahmen bewertet. **PI.3 Resolution (Lösung)**

Charakteristik	Attribute
	Identifizierte Probleme werden entsprechend korrigiert. Die Wirksamkeit der Maßnahmen wird bewertet, um sicherzustellen, dass Probleme angemessen angegangen werden. Wichtige Lektionen werden geteilt. **PI.4 Trending (Trends identifizieren)** Probleme werden analysiert, um mögliche Muster und Trends zu identifizieren. Um eine ganzheitliche Betrachtung von Ursachen und Wirkungen zu erhalten, wird ein breites Spektrum an Informationen ausgewertet.
Raising Concerns (Bedenken äußern) Das Personal kann Sicherheitsbedenken ohne Angst vor Vergeltung, Einschüchterung, Belästigung oder Diskriminierung äußern. Die Organisation erstellt, pflegt und bewertet Richtlinien und Prozesse, die es dem Personal ermöglichen, Bedenken frei zu äußern.	**RC.1 Supportive Policies are implemented (Unterstützende Richtlinien werden implementiert)** Die Organisation legt eine Richtlinie klar fest und setzt sie effektiv um. Die Richtlinie unterstützt die Rechte und Pflichten einer Person, Sicherheitsbedenken zu äußern. Die Organisation duldet keine Belästigung, Einschüchterung, Vergeltung oder Diskriminierung, um Bedenken zu äußern. **RC.2 Confidentiality is possible (Vertraulichkeit ist möglich)** Die Organisation implementiert mindestens eine Methode zum Vorbringen und Lösen von Bedenken, die vertraulich und unabhängig vom Einfluss des Linienmanagements ist. Dem Betroffenen wird zeitnah eine Rückmeldung gegeben.
Work Planning (Arbeitsplanung) Der Prozess der Planung und Kontrolle von Arbeitsaktivitäten wird so umgesetzt, dass die Sicherheit aufrechterhalten wird. Arbeit wird in einem bewussten Prozess verwaltet, in dem Arbeit identifiziert, ausgewählt, geplant, ausgeführt und kritisiert wird. Die gesamte Organisation ist in den Prozess eingebunden und unterstützt ihn umfassend. Alle relevanten Teile der Organisation arbeiten zusammen, um den Prozess der Kontrollarbeit zu unterstützen.	**WP.1 Work Management (Arbeitsmanagement)** Es gibt einen systematischen Ansatz zur Auswahl, Planung, Koordination und Durchführung von Arbeitsaktivitäten, so dass die Sicherheit betont wird. Der Arbeitsprozess berücksichtigt die Identifizierung und das Management relevanter Faktoren, einschließlich des Risikos. **WP.2 Safety Margins (Sicherheitsmargen)** Die Arbeiten werden so geplant und durchgeführt, dass Sicherheitsmargen erhalten bleiben. Sicherheitsmargen werden nur durch einen systematischen und rigorosen Prozess verstanden, sorgfältig gepflegt und geändert. **WP.3 Documentation and Procedures (Dokumentation und Verfahren)** Die Dokumentation, einschließlich der Verfahren, ist vollständig, genau, zugänglich, benutzerfreundlich, verständlich, aktuell. Änderungen werden verfolgt.

2.3 Sicherungskultur

2.3.1 Erkenntnisse aus dem IAEA-Regelwerk

Nachfolgend wird auf folgende IAEA-Dokumente eingegangen und die für dieses Vorhaben relevanten Informationen zusammengefasst:

- IAEA NSS No 7 – Nuclear Security Culture, Implementing Guide /IAE 08/
- IAEA NSS No 28-T – Self-assessment of Nuclear Security Culture in Facilities and Activities /IAE 17/
- IAEA NSS No 38-T – Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material /IAE 21/

2.3.1.1 IAEA NSS No. 7: Sicherungskultur

Der Standard NSS Nr. 7 „*Nuclear Security Culture, Implementing Guide*“ der IAEA /IAE 08/ beinhaltet einen Leitfaden, der die grundlegenden Konzepte und Elemente der nuklearen Sicherungskultur aus Sicht der IAEA erläutert. Darin wird der Begriff der nuklearen Sicherungskultur definiert (siehe Kap. 2.1.2).

Nach IAEA NSS Nr. 7 soll eine angemessene nukleare Sicherungskultur sicherstellen, dass der Umsetzung nuklearer Sicherungsmaßnahmen die ihrer Bedeutung gebotene Aufmerksamkeit geschenkt wird /IAE 08/.

Das wichtigste gemeinsame Ziel von Sicherheits- und Sicherungskultur besteht nach IAEA NSS Nr. 7 darin, das Risiko durch radioaktives Material und zugehörige Einrichtungen zu begrenzen. Dieses Ziel basiert weitgehend auf gemeinsamen Grundsätzen, wie z. B. einer hinterfragenden Haltung, rigorosen und umsichtigen Herangehensweisen sowie einer effektiven Kommunikation /IAE 08/.

Gemäß IAEA NSS Nr. 7 berücksichtigen sowohl die nukleare Sicherheit als auch die nukleare Sicherung das Risiko von unbeabsichtigtem menschlichem Fehlverhalten.

Zusätzlich werden bei der nuklearen Sicherung auch vorsätzliche Handlungen, mit denen Schaden verursacht werden soll, betrachtet. Aus diesem Grund erfordert die Sicherungskultur gegenüber der Sicherheitskultur andere Einstellungen und Verhaltensweisen, wie die Vertraulichkeit von Informationen oder die Bestrebung zur Abschreckung böswilliger Handlungen /IAE 08/.

Während bei der Sicherheitskultur alle Personen aufgefordert sind, Informationen im Sinne der Transparenz und des Dialogs offen auszutauschen, erfordert die Sicherungskultur, dass Einzelpersonen auf Bedrohungen und Vorfälle sofort reagieren und dabei die Kommunikation auf jene autorisierten Personen beschränken, die in Kenntnis gesetzt werden müssen. In diesem Sinne weist IAEA NSS Nr. 7 darauf hin, dass Sicherheits- und Sicherungskultur gemeinsam gefördert werden müssen /IAE 08/.

In Kap. 3 beschreibt IAEA NSS Nr. 7 die Rollen und Zuständigkeiten der Personen und Institutionen, die für eine gute Sicherungskultur verantwortlich sind. Hierzu zählen der Staat, verschiedene Organisationen sowie ihre Manager, das Personal, die Öffentlichkeit und die internationale Community /IAE 08/.

In Kap. 4 von IAEA NSS Nr. 7 werden die Charakteristika und Indikatoren der nuklearen Sicherungskultur beschrieben. Eine im Rahmen dieses Vorhabens verwendete Übersetzung dieser Charakteristika und Attribute ist in Anhang A zu finden.

2.3.1.2 IAEA NSS No. 28-T: Selbstbewertung der Sicherungskultur

Im Standard NSS Nr. 28-T /IAE 17/ der IAEA wird eine Methodik beschrieben, die Betreiber von Kernkraftwerken und ihre Aufsichtsbehörden dabei unterstützen sollen, ihre nukleare Sicherungskultur selbst zu beurteilen und Möglichkeiten zu ihrer Stärkung zu ermitteln. Die Methodik baut auf dem Modell der Sicherungskultur in IAEA NSS Nr. 7 /IAE 08/ auf und erweitert es um weitere Indikatoren, die in Anhang A dargestellt sind.

Darüber hinaus werden Selbstbewertungsmethoden beschrieben. Dabei werden die Indikatoren der aktuellen Sicherungskultur des Unternehmens mit den in IAEA NSS Nr. 28-T aufgeführten Indikatoren verglichen, die ein Referenzniveau für eine optimale Sicherungskultur bilden /IAE 17/.

Die Selbsteinschätzung ist ein schrittweiser Prozess. Anfangs kann es sich nach IAEA NSS Nr. 28-T auf eine Überprüfung der Indikatoren durch das Management auf der

Grundlage verfügbarer Beobachtungen, Dokumentenprüfungen und anderer Quellen beschränken, um einen Einblick in den Zustand der nuklearen Sicherungskultur zu erhalten. Wenn die Entscheidung getroffen wird, eine Selbstbewertung mit einem breiteren Umfang einzuleiten, kann es sinnvoll sein, sich auf die Kernmerkmale zu konzentrieren, die für die Ergebnisse der jüngsten Risikobewertungen, die Schlussfolgerungen der zuständigen Behörden und andere Quellen relevant sind. Die Analyse vergangener Sicherungsvorfälle und die Ermittlung ihrer Ursachen können auch dabei helfen, gefährdete Merkmale der Sicherungskultur auszuwählen. Eine Selbstbewertung mit eingeschränktem Anwendungsbereich schließt eine Selbstbewertung mit einem breiteren Anwendungsbereich nicht aus, wenn dies später als notwendig erachtet wird /IAE 17/.

Da das ultimative Ziel der Entwicklung einer Sicherungskultur darin besteht, persönliche Verhaltensqualitäten wie Professionalität, persönliche Verantwortlichkeit, Einhaltung von Verfahren, Teamwork, Kooperation und Wachsamkeit zu vermitteln, kann die Selbstbewertung mit der Untersuchung einiger dieser Eigenschaften und ihrer Derivate beginnen, und insbesondere ihre kulturellen Wurzeln. Kulturwandel ist ein langfristiger Prozess, in dem Management und Mitarbeiter die nukleare Sicherungskultur kontinuierlich verbessern. Die Sicherungskultur muss regelmäßig bewertet werden, um Fortschritte zu verfolgen und Programme anzupassen, und es ist von Vorteil, diese Aktivität innerhalb der Organisation zu institutionalisieren /IAE 17/.

Die laufenden Kosten des Selbstbewertungsprogramms sollten nach IAEA NSS Nr. 28-T geschätzt und im Budget der Organisation vorgesehen werden. Hierzu zählt auch die Zeit, die Mitarbeiter für Befragungen oder Interviews abseits ihrer eigentlichen Aufgaben aufwenden, sowie die Zeit der Mitglieder des Self-Assessment-Teams für die Vorbereitung, Durchführung und Auswertung der Assessment-Ergebnisse. Wesentlich für eine erfolgreiche Selbsteinschätzung ist, dass die Teilnahme freiwillig ist und die Antworten der Teilnehmenden vertraulich behandelt werden. Vor Beginn der Datenerhebung sollte sorgfältig geprüft werden, auf welche Weise die Vertraulichkeit verletzt werden kann und es sollten explizite Strategien zur Vermeidung solcher Verletzungen eingeführt werden. Der Grundsatz der freiwilligen Teilnahme ist entscheidend, um offene und aufrichtige Antworten zu erhalten /IAE 17/.

Die zur Selbstbewertung zu verwendenden Methoden lassen sich nach IAEA NSS Nr. 28-T in zwei Kategorien einteilen: nicht interaktive Methoden wie Umfragen und Dokumentenprüfungen und interaktive Methoden wie Einzelinterviews. Beobachtungen werden in beiden Kategorien durchgeführt. Alle Methoden haben ihre Stärken und

Schwächen. Daher wird empfohlen, eine Kombination mehrerer Methoden auf dasselbe Phänomen anzuwenden. Außerdem sollten qualitative und quantitative Methoden kombiniert werden (z.B. Umfrage, die quantitative Daten liefert, gefolgt von Interviews, um mögliche Lücken zu schließen, Unklarheiten zu beseitigen und qualitative Daten zu erzeugen). In Kap. 5 von IAEA NSS Nr. 28-T werden verschiedene Methoden zur Selbstbewertung vorgestellt. Hierzu zählen Umfragen, Interviews, Dokumentenprüfung und Beobachtungen /IAE 17/.

2.3.1.3 IAEA NSS No. 38-T: Verbesserung der nuklearen Sicherheitskultur in Organisationen, die mit nuklearem Material arbeiten

Der Standard NSS Nr. 38-T /IAE 21/ der IAEA ergänzt die Standards zur Sicherungskultur NSS Nr. 7 /IAE 08/ und Nr. 28-T /IAE 17/ und soll Organisationen bei der Verbesserung ihrer Sicherungskultur zusätzlich unterstützen. Er behandelt Rollen, Verantwortlichkeiten und Aktivitäten zur Verbesserung der Sicherungskultur auf verschiedenen Ebenen (Staat, Organisation, Individuum) und beschreibt Schlüsselelemente eines Programms zur Verbesserung der nuklearen Sicherungskultur. Hierzu zählen eine regulatorische Grundlage, Selbstbewertung, ein Aktionsplan für die Sicherungskultur, Ausbildung und Training sowie ein Programm zum Umgang mit Betriebserfahrung.

Nach IAEA NSS Nr. 38-T stärkt eine effektive Sicherungskultur die Sicherung, indem sie das Personal, einschließlich der Führungskräfte, ermutigt, folgendes zu tun /IAE 21/:

- Verbesserung ihres Verständnisses von Bedrohungen und Anfälligkeiten sowie sensiblen Informationen
- Aufbau eines gemeinsamen Verständnisses und Bewusstseins für die Sicherung auf allen Ebenen (Staat, Behörden, Einrichtungen, Aktivitäten) und Verbesserung der Koordinierung zwischen Akteuren der Sicherung
- Einbeziehung aller Interessensgruppen in die Förderung der Bedeutung der Sicherung
- Schaffung einer Atmosphäre individueller und kollektiver Verantwortung für die Sicherung
- Stolz sein auf Leistung und Arbeitszufriedenheit
- Erhöhung ihres Engagements für Sicherungsziele
- Förderung einer angemessenen Zuweisung menschlicher, technischer und finanzieller Ressourcen für die Sicherung

- Verringerung menschlicher Fehler und deren Auswirkungen auf die Wirksamkeit von Sicherungssystemen und -maßnahmen
- Schaffung einer Atmosphäre des Respekts gegenüber dem gesamten Sicherungspersonal
- Handlung aufgrund gewonnener Erkenntnisse und Betriebserfahrung, um die Sicherung kontinuierlich zu verbessern

Die Aufgabe des Staates ist nach IAEA NSS Nr. 38-T, eine starke Sicherungskultur zu fördern, indem er eine Politik zur Verbesserung der Sicherung innerhalb seines Regulierungsrahmens festlegt, entwickelt und umsetzt. Außerdem sollte der Staat den zuständigen Behörden entsprechende Ressourcen zuweisen, damit diese Maßnahmen zur Verbesserung der Sicherungskultur ergreifen können. Darüber hinaus können sie eine Gruppe einrichten, welche die Bemühungen zur Verbesserung der Sicherungskultur überwacht und die Strategie und Leitlinien hierfür festlegt /IAE 21/.

Die Aufgabe der Organisation ist nach IAEA NSS Nr. 38-T, ein Programm zur Verbesserung der Sicherungskultur zu entwickeln und umzusetzen. Hierfür sollten zuerst gewünschte Einstellungen und Verhaltensweisen für eine gute Sicherungskultur bestimmt werden. Anschließend sollte die tatsächliche Situation bewertet und die Lücke zwischen aktuellem und gewünschtem Zustand bestimmt werden. Im weiteren Verlauf des Berichts werden Aufgaben, Rollen und Verantwortlichkeiten von Organisationsleitern und Sicherungskultur-Koordinatoren dargestellt. Außerdem werden Aufgaben, Rollen und Verantwortlichkeiten von Führungskräften und Mitarbeitern beschrieben /IAE 21/.

In IAEA NSS Nr. 38-T werden Schlüsselelemente genannt, die in einem Programm zur Verbesserung der Sicherungskultur enthalten sein sollten. Hierzu gehören /IAE 21/

- eine regulatorische Grundlage,
- ein Aktionsplan für die Sicherungskultur, in dem spezifische Ziele und Maßnahmen, das verantwortliche Personal, der Zeitrahmen für die Durchführung der Maßnahmen, die Ressourcen und potentielle Hindernisse sowie zu erwartende Ergebnisse beschrieben sind,
- eine Methode mit Bewertungsindikatoren zur Durchführung von Selbstbewertungen,
- ein effektives Änderungsmanagement,
- Qualitätssicherungspraktiken,
- ein Ausbildungs- und Trainingsprogramm,

- gut funktionierender Informationsaustausch zur Interaktion verschiedener Funktionen innerhalb der Organisationsstruktur.

Anhang I von /IAE 21/ beschreibt für jeden der in /IAE 08/ und /IAE 17/ aufgeführten Indikatoren mögliche Aktivitäten mit Angabe der entsprechenden Verantwortlichkeiten. Beispiele sind in Tab. 2.4 aufgeführt.

Tab. 2.4 Beispiele zu Aufgaben für Indikatoren der Sicherungskultur nach /IAE 17/

Indikator	Aufgabe
Für die Organisation ist eine nukleare Sicherungspolitik festgelegt	Führungskraft/Manager • Entwickelt nukleare Sicherungspolitik, die folgendes umfasst - Verpflichtungserklärung zur Leistungsqualität bei allen Aktivitäten im Bereich der nuklearen Sicherung - Erklärung, der Sicherung hohe Priorität einzuräumen - Prozess für Manager zur Lösung von Konflikten zwischen Sicherheit, Sicherung, Gefahrenabwehr und Betrieb
Das Personal ist mit dem Verhaltenskodex durch laufende Schulungen und Sensibilisierungsmaßnahmen vertraut.	Sicherungskultur-Koordinator • Verteilt den Verhaltenskodex auf einem handlichen Dokument in Referenzgröße, sodass es leicht zugänglich ist oder leicht in einer Tasche getragen werden kann; • Bringt den Verhaltenskodex an Wänden in gemeinschaftlichen Arbeitsbereichen an. Führungskraft/Manager • Erinnert das Personal in Meetings oder anderen Gesprächen an den Inhalt des Verhaltenskodex. Personal • Nimmt an Schulungen teil • Bittet bei Bedarf um Klärung des Verhaltenskodex • Unterzeichnet den Verhaltenskodex • Macht sich mit dem Inhalt des Verhaltenskodex vertraut • Verhält sich in Übereinstimmung mit dem Verhaltenskodex

2.3.2 Erkenntnisse aus internationalen Veröffentlichungen der Nuklearbranche zur Sicherungskultur

Nachfolgend werden Erkenntnisse aus internationalen Veröffentlichungen zusammengefasst, die für das Thema der Sicherungskultur relevant waren:

- Nuclear Industry Safety Directors' Forum: Key Attributes of an Excellent Nuclear Security Culture /NIS 13/

- World Institute for Nuclear Security: Nuclear Security Culture /WIN 16b/
- Khripunov, I. et al: The Human Dimension of Security for Radioactive Sources: From Awareness to Culture /KHR 14/

2.3.2.1 NISD-Forum: Schlüsselattribute einer guten Sicherungskultur

Das Safety Directors Forum (SDF), das Office for Nuclear Regulation (ONR) und das britische Ministerium für Energie und Klimawandel (DECC) haben einen Leitfaden entwickelt, um ein besseres Verständnis für die Merkmaler einer ausgezeichneten Sicherungskultur zu erhalten. Dieser Leitfaden benennt 8 wesentliche Schlüsselattribute, zu denen jeweils wiederum Hinweise gegeben werden, die sich an die verschiedenen Personengruppen richten. Die Schlüsselattribute lauten /NIS 13/:

1. Ein risikoorientiertes Sicherungsprogramm, das die Verhältnismäßigkeit gebührend berücksichtigt.
2. Kompetente, fähige und ausreichende Sicherungsressourcen.
3. Die Sicherungsleistung wird gegebenenfalls auf allen Ebenen in den Organisationen überwacht - von der Vorstandsebene bis zum Bereitstellungsteam.
4. Ein angemessenes, unabhängiges Regierungssystem unter Führung eines Verwaltungsrats.
5. Alle Mitarbeiter verstehen die Sicherungsrisiken und Konsequenzen, die ihrer Rolle und ihrem Anteil an der Bewältigung und Minderung von Risiken angemessen sind.
6. Sicherungserwartungen und -standards werden festgelegt, kommuniziert und verstanden. Alle werden in Bezug auf ihre Einhaltung zur Rechenschaft gezogen.
7. Es gibt Lern- und Leistungsprozesse für die Sicherung, und die Sicherungsleistung der Organisation verbessert sich ständig.
8. Alle Mitarbeiter werden in Sicherungsfragen in angemessener Weise einbezogen, und ihre Ansichten zur Sicherung werden sorgfältig geprüft.

Um diese Schlüsselattribute umzusetzen, werden Anforderungen an die verschiedenen Personengruppen formuliert:

Die **Regierung** sollte

- sicherstellen, dass ein geeigneter gesetzlicher, politischer Rahmen vorhanden ist.

- die strategischen Ziele und Erwartungen festlegen und erläutern. Die Behörde holt von der Industrie Beweise dafür ein, dass diese erreicht werden, und interpretiert die Informationen.

- ihre "Risikobereitschaft" in Bezug auf die zivile nukleare Sicherung spezifizieren. Diese sollte, soweit möglich, verhältnismäßig und eindeutig sein in Bezug auf die Bedrohung von Kernmaterial, sonstigem radioaktivem Material und sensiblen nuklearen Informationen. Sie sollte außerdem im Einklang mit dem kerntechnischen Regelwerk sein. Als Teil dieses Prozesses sollte die Regierung:
  - sich mit der Industrie und der Behörde über die Bedrohung beraten.
  - klar definieren, welche Risiken (die sich aus Sicherungsfragen ergeben) in der Verantwortung welcher Stellen liegen.
  - ein klares Verständnis aller relevanten Interessengruppen über Bedrohungen/Risiken erleichtern.

- wo immer möglich, sicherstellen, dass ausreichend Ressourcen für die Sicherung vorhanden sind.
  - Es sollte versucht werden, politische Konsistenz sicherzustellen, um Behörden und Industrie Planungssicherheit zu geben.
  - Verantwortlichkeiten für die Sicherung sollten klar sein.

- sich darüber im Klaren sein, welche Art von Informationen und welches Maß an Sicherung und Analyse verlangt werden soll.

- sicherstellen, dass eine effektive Informationsarchitektur vorhanden ist und dass eine Strategie für die wirksame Verbreitung von nachrichtendienstlichen Informationen existiert und alle Personen in der Lage sind, im vollen Umfang ihrer Sicherungsfreigabe unterrichtet zu werden.

- ein Engagement ermöglichen, indem sie klar festlegt, welche Informationen im Rahmen der gesetzlichen Bestimmungen weitergegeben werden können (Menschen müssen Bescheid wissen, um sich voll engagieren zu können).

Die **Behörde** sollte

- mit gutem Beispiel vorangehen. Zur Ermöglichung eines risikoorientierten Sicherungsprogramms sollte sie:
  - ein klares Verständnis der Bedrohungen/Risiken bei allen relevanten Beteiligten fördern und sicherstellen

  - sicherstellen, dass die Regulierung auf die vereinbarten Risiken abgestimmt und verhältnismäßig ist und
  - sicherstellen, dass die Inspektoren entsprechend ausgewählt und geschult werden, um auf diese Weise zu regulieren

- sicherstellen, dass die Umsetzung ihrer Vorschriften von Fachleuten durchgeführt oder erleichtert wird und dass die Inspektoren die Auswirkungen ihrer Entscheidungen auf die Organisationen verstehen und dass dieses Verständnis in ihre Beurteilungen und Entscheidungen einfließt.

- kontinuierliche Verbesserung fördern (im Einklang mit ergebnisorientiertem/zielsetzendem System) und
  - bei der Entwicklung eines KPI[2]-Rahmens und der Festlegung von Leistungszielen unterstützen
  - die Leistung beobachten und ein ausgewogenes Feedback geben
  - die Prüfung daran entsprechen anpassen (z.B. gezielte Mittel zur Behebung schlechter Leistung)

- die Weitergabe von Informationen über Bedrohungen im Kontext der Industrie unterstützen und sicherstellen, dass in der gesamten Industrie ein angemessenes und ausreichendes Verständnis der Informationen über Bedrohungen vorhanden ist.

- die zu erreichenden Sicherheitsziele entwickeln und umsetzen, geeignete bewährte Verfahren ermitteln, Arbeiten in Auftrag geben, um Lücken zu schließen, und deren Entwicklung unterstützen. Die Behörde sollte außerdem
  - die Gründe für die Erwartungen erläutern
  - die Bewertungsmethoden erläutern
  - Interventionen auf das Erreichen der Ziele abstimmen
  - bei Bedarf eine angemessene und verhältnismäßige Durchsetzung gewährleisten und
  - die Regierung hinsichtlich der Angemessenheit ihrer Erwartungen beraten

[2] KPI: Key Performance Indicator, Leistungskennzahl in der Betriebswirtschaftslehre, anhand derer der Fortschritt oder der Erfüllungsgrad hinsichtlich wichtiger Zielsetzungen oder kritischer Erfolgsfaktoren innerhalb einer Organisation gemessen und/oder ermittelt werden kann.

- die Industrie dabei unterstützen, die hochrangigen Anforderungen des Gesetzgebers in Ziele umzuwandeln, die von der Industrie zu erreichen sind, sowie zur Entwicklung von Lerninhalten im Bereich der Sicherheit beitragen. Sie sollte außerdem
  - die kontinuierliche Verbesserung fördern (in Übereinstimmung mit dem ergebnisorientierten/ zielorientierten System)
  - die Entwicklung eines Rahmens für Sicherungskompetenzen durch die Industrie und die Festlegung geeigneter Leistungsziele im Bereich Sicherung und Weiterbildung unterstützen
  - die Leistungen im Bereich der Sicherungsbildung und -entwicklung betrachten und ein ausgewogenes Feedback bereitstellen

- sicherstellen, dass ihre eigenen Mitarbeiter in der Lage sind, die Bedeutung der Sicherung zu erklären. Sie sollte außerdem
  - in regelmäßigen Abständen eine Meinungsumfrage über die Wirksamkeit der Regelungen zur gemeinsamen Nutzung von Sicherungsinformationen durchführen
  - die Industrie in die Entwicklung von Verbesserungen einbeziehen und
  - Unternehmen/Organisationen durch Interventionsmaßnahmen unterstützen, Beweise für Engagement suchen und bewerten sowie die Entwicklung lokaler Initiativen unterstützen

Die **Unternehmen und Organisationen** sollten

- sich in einer Erklärung zur nuklearen Sicherung zur Qualität der Leistung bei allen Tätigkeiten der nuklearen Sicherung verpflichten. Als Teil dieses Prozesses sollen sie:
  - über ein wirksames Sicherungsrisikoverfahren verfügen, das in den Risikoprozess des Unternehmens einfließt
  - Bedrohungen als Grundvoraussetzung und als verhältnismäßig für die Sicherung des Standorts akzeptieren
  - sicherstellen, dass das Unternehmen/die Organisation und seine/ihre Mitarbeiter die Sicherungsbedrohungen und Risiken verstehen und
  - sich auf allen Ebenen für Sicherungsfragen einsetzen.

- Standards für die Sicherungskompetenz festlegen und diese in Personalprozesse einbauen.

- sicherstellen, dass

  - die Unternehmensvorstände über die notwendige Kompetenz in Bezug zur Sicherung verfügen
  - sie die Kontrolle über die Sicherungsressourcen haben, um die Erfüllung der Verantwortlichkeiten zu ermöglichen

- Leistungsbereiche identifizieren, die verbessert werden können (oder hervorragende Leistung aufrechterhalten) und
  - einen KPI-Rahmen entwickeln und geeignete Indikatoren für das Unternehmen festlegen
  - ihre Erwartungen an die Belegschaft kommunizieren
  - die Leistung überwachen und an den Vorstand berichten
  - regelmäßige Leistungsvergleiche durchführen und die Entwicklung bewährter Verfahren in der Branche unterstützen

- über Systeme, Verfahren und Kompetenzen verfügen, um allen Mitarbeitern Informationen über Bedrohungen zukommen zu lassen, die auf ihre Sicherheitsüberprüfung und ihre Rolle zugeschnitten sind. Sie sollten auch über ein wirksames Sicherungsrisikoregister und ein System zur Mitteilung von Risiken verfügen. Diese Risiken sollen auch in die Aus- und Weiterbildung einfließen.

- über ein System der Selbstbeurteilung verfügen, um Motivation, Führung und Sicherungskultur im Allgemeinen aufrecht zu erhalten. Als Teil dieses Prozesses sollten sie auch
  - die Sicherungsverantwortung auf Vorstands- und Führungsebene fördern
  - die Erwartungen an die Sicherheit in den normalen Geschäftsbetrieb integrieren
  - Ziele und bewährte Praktiken in lokale Richtlinien und Verfahren integrieren
  - Ressourcen bereitstellen, um die Kommunikation der Erwartungen zu ermöglichen
  - Erwartungen an die Belegschaft vermitteln und das Verständnis überprüfen
  - in der Lage sein, proaktiv und reaktiv zu handeln, um die individuelle Verantwortlichkeit sicherzustellen
  - interne und externe Ressourcen zur Überprüfung des Erfolgs von Initiativen nutzen
  - Maßnahmen gegen Einzelpersonen ergreifen, wenn das angemessen ist (Rehabilitation und Bestrafung)
  - kommunizieren, um zu zeigen, dass gegen Verstöße vorgegangen wurde

  - regelmäßiges Benchmarking der Leistung und Zusammenarbeit mit anderen Unternehmen und Organisationen, um die Entwicklung bewährter Verfahren in der Branche zu unterstützen
  - Einführung einer „Whistleblowing“-Politik

- Bereiche der Sicherungsausbildung und -entwicklung identifizieren, um die Ziele zu erreichen. Sie sollten außerdem
  - Zielvorgaben für die Verbesserung von Sicherung und Ausbildung/Entwicklung festlegen
  - einen Kompetenzrahmen entwickeln und geeignete Leistungsindikatoren festlegen
  - Erwartungen an Ausbildung und Entwicklung an die Belegschaft kommunizieren
  - regelmäßiger Benchmark der Ausbildungs- und Entwicklungsleistung im Sicherungsbereich und Zusammenarbeit mit anderen Unternehmen/Organisationen zur Unterstützung der Entwicklung bewährter Verfahren in der Branche
  - ein Umfeld schaffen, in dem sich das Personal befähigt fühlt, das Sicherungsverhalten bei anderen in Frage zu stellen
  - Bereitstellung von realistischen und effektiven Schulungs- und Entwicklungsmöglichkeiten für Personal in Sicherungsfragen

- den Mitarbeitern die Bedeutung von Sicherung im Zusammenhang mit ihren eigenen organisatorischen Aktivitäten erklären und den Schulungsbedarf ermitteln. Außerdem sollten sie
  - Schulungen anbieten, deren Wirksamkeit überwachen und bei Bedarf regelmäßig auffrischen
  - regelmäßige Meinungsumfragen durchführen und sich intern über Änderungen beraten
  - die Mitarbeiter in die Entwicklung von Verbesserungen einbeziehen und
  - das Engagement gegenüber der Behörde nachweisen

Das **Personal** sollte

- sich über seine Rolle bei der Kontrolle und Bewältigung von Sicherungsbedrohungen im Klaren sein, und alle Vorstandsmitglieder, leitenden Angestellten und Manager sollten eine Führungsrolle in Bezug auf die Sicherung übernehmen.

- Verantwortung für die Sicherung übernehmen.

- die Sicherungsleistung und die Erwartungen verstehen, sich an Verbesserungsmaßnahmen, Lernaktivitäten und Schulungen beteiligen, das Gelernte in die Praxis umsetzen und andere dazu ermutigen.
- die Anforderungen verstehen, sich entsprechend der Ausbildung verhalten. Sie sollten auch einen hinterfragenden und herausfordernden Ansatz verfolgen, wachsam sein und Ereignisse melden.
- dafür verantwortlich sein, das Sicherungsverhalten anderer konstruktiv zu hinterfragen, wenn dies angebracht ist.
- wissen, wie ein „Whistleblowing"-Prozess abläuft und in der Lage sein, auf Beweise zuzugreifen, die eine faire Meldekultur zeigen.
- Sicherungsinformationen verantwortungsbewusst nutzen, um zu managen bzw. einzuschränken, die Leistung zu verbessern und die Konsequenzen eines Missbrauchs zu verstehen.
- die Sicherungserwartungen verstehen und sich bemühen, die Standards zu erreichen.

Alle Stellen müssen sicherstellen, dass angemessene (d.h. wirksame und verhältnismäßige) Informationen und Ratschläge für alle geeigneten Ebenen zur Verfügung stehen, die über die notwendige Kompetenz verfügen, um sie zu interpretieren und

- Maßnahmen entsprechend festzulegen und der Umsetzung zu überwachen.
- sicherstellen, dass jede Stelle/Organisation über ein eigenes Risikoregister für nukleare Sicherung verfügt und Maßnahmen zur Risikominderung ergreift und wichtige Risiken dort einpflegt.
- sicherstellen, dass organisatorische Managementsysteme vorhanden sind, die gewährleisten, dass korrekte Informationen in die Prozesse eingespeist werden.

2.3.2.2 WINS: Leitfaden für bewährte Verfahren zur Sicherungskultur

Nach dem Bericht „*Nuclear Security Culture*" des World Institute for Nuclear Security (WINS) /WIN 16b/ zeichnet sich ein Unternehmen mit starker Sicherungskultur dadurch aus, dass die Mitarbeiter davon überzeugt sind, dass Bedrohungen real sind und dass es ihre Aufgabe ist, zur Sicherung des gesamten Unternehmens beizutragen. Wenn ihnen etwas auffällt, melden sie es, ohne zu zögern. Sie geben bereitwillig einen Fehler

zu, versuchen zu verstehen, wie es dazu kam, und arbeiten aktiv daran, ihre Leistung zu verbessern. Sie teilen Ideen und Vorschläge zur Verbesserung der Sicherung ihren Vorgesetzten mit, weil sie wissen, dass solche Beiträge gefördert, respektiert und belohnt werden.

Viele Instrumente und Techniken, die sich im Zusammenhang mit der Verbesserung der Sicherheitskultur ergeben haben, sind nach /WIN 16b/ unmittelbar auch für die Sicherungskultur relevant. Nach /WIN 16b/ basieren sowohl Sicherheits- als auch Sicherungskultur auf dem Konzept der allgemeinen Organisationskultur. Alle Organisationen haben demnach eine zugrundeliegende Kultur, die auf bestimmten Werten und Überzeugungen beruht. Diese wiederrum führen zu bestimmten Arten von Einstellungen und Verhaltensweisen. In Tab. 2.5 sind Verhaltensweisen dargestellt, die sich aus Werten und Überzeugungen für eine starke Sicherungskultur ergeben.

Tab. 2.5 Werte, Überzeugungen und daraus resultierendes Verhalten /WIN 16b/

Werte und Überzeugungen	Resultierende(s) Verhalten
Eine starke Sicherungskultur ist für den Schutz nuklearer und radioaktiver Materialien von entscheidender Bedeutung.	Die Sicherungspolitik, das Qualitätsmanagementsystem und die Änderungsmanagementprozesse der Organisation tragen dazu bei, dass alle Mitarbeiter konsequent eine starke nukleare Sicherungskultur unter Beweis stellen. Die Organisation verfolgt einen gut definierten, gut dokumentierten Ansatz für das Sicherungsmanagement, weil sie fest davon überzeugt ist, dass die Sicherungskultur wichtig ist.
Eine unabhängige Aufsicht stärkt die Sicherung.	Ein wirksamer, integrierter Aufsichtsprozess - unabhängig vom Linienmanagement und als anerkannter Teil des Managementsystems implementiert - ist vorhanden.
Um eine starke Sicherungskultur zu haben, muss unsere Organisation Wert auf Lernen legen.	Der Vorstand, das Management und die Belegschaft engagieren sich in einem kontinuierlichen Lernprozess, um Sicherungsfragen besser zu verstehen und Kompetenzen auf einer Ebene zu entwickeln, die der jeweiligen Funktion angemessen ist.

Als Beispiele für nukleare Sicherungskultur werden in /WIN 16b/ folgende Charakteristiken genannt:

- Leitung und Motivierung
- Verantwortlichkeit
- Professionalität und Kompetenz
- Integration
- Lernen und Verbesserung

Faktoren, die die Sicherungskultur fördern, hängen nach /WIN 16b/ stark mit der Leitung/Führung zusammen (siehe Abb. 2.2).

Abb. 2.2 Faktoren zur Stärkung der Sicherungskultur nach /WIN 16b/

Nach /WIN 16b/ beginnt eine wirksame Führung bei der Regierung und den Aufsichtsbehörden. Betreiber werden keinen Anreiz zur Verbesserung ihrer Sicherungskultur haben, wenn sie die Bedrohungen nicht verstehen, denen sie ausgesetzt sind. Die Aufsichtsbehörde sollte von den Betreibern ein Programm zur Bewertung und Stärkung der Sicherungskultur verlangen. Außerdem sollte ein Prozess zur Ursachenermittlung und eine Datenbank zu gewonnenen Erfahrungen eingeführt werden.

Organisationen, die eine starke, wirksame Sicherungskultur schaffen, haben Ähnlichkeiten in verschiedenen wichtigen Bereichen des Managements, darunter der strategische Kontext, die organisatorischen Managementsysteme, die Vollständigkeit des Sicherungsprogramms, das Leistungsmanagement, das Engagement und die Einstellung der Mitarbeiter sowie die Einbeziehung externer Interessengruppen.

Im strategischen Kontext sind folgende Punkte für die Sicherungskultur wichtig:

- Die Unternehmensleitung betrachtet Sicherung als eine unternehmerische Verantwortung.
- Die Unternehmensleitung hat ihre Geschäftsziele und die gesetzlichen Anforderungen identifiziert und in die Sicherungsstrategie und -richtlinien aufgenommen.

- Die Unternehmensleitung hat ihre Sicherungserwartungen definiert und setzt sich dafür ein, sie zu erfüllen.
- Die Unternehmensleitung macht das Thema Sicherung zu einem hochkarätigen Thema und kommuniziert dieses Engagement wirksam.

Für Managementsysteme sind folgende Aspekte relevant:

- Die Unternehmensleitung integriert die Sicherung in das gesamte Managementsystem der Organisation.
- Das Führungsgremium der Organisation hat eine schriftliche Sicherungspolitik aufgestellt.
- Die Unternehmensleitung hat ein klar definiertes Programm für ein Sicherungsmanagementsystem (SMS) mit folgenden Punkten geschaffen.
  - Engagement und Kommunikation mit externen Stakeholdern
  - Leistungsprüfung und Wirksamkeit
  - regulatorisches Engagement und Rechtsfragen
  - Unternehmensaufsicht und Berichterstattung
  - finanzielle/budgetäre Bestimmungen und Anforderungen
  - Informationssicherheit und IT-Systeme und Cybersicherheit
  - menschliche Verlässlichkeit und personelle Sicherheit (Prüfung und Nachsorge)
  - Sensibilisierung, Engagement und berufliche Entwicklung/Zertifizierung von Mitarbeitern
  - physischer Schutz und Infrastruktur der Einrichtung, einschließlich Zugangskontrollen
  - Notfallplanung und -reaktion, einschließlich der Evakuierung des Personals
- Die Unternehmensleitung hat die organisatorischen Aufgaben und Zuständigkeiten für die Sicherung klar definiert.
- Die Unternehmensleitung betont, dass Qualitätssicherung und Aufzeichnungen eine hohe Priorität haben.

Ein umfassendes Sicherungsprogramm besteht aus mehreren Punkten. Für die Informationssicherheit werden folgende Punkte aufgeführt:

- Die Unternehmensleitung stellt sicher, dass die Verfahren des Cybersicherheitsmanagements klar festgelegt und umgesetzt wurden, und sie überwacht diese sorgfältig.

  - Die Unternehmensleitung stellt sicher, dass geeignete Maßnahmen für die Sicherung von IT & IC-Systemen umgesetzt wurden. Die zuständige Behörde muss die Möglichkeit haben, diese Maßnahmen zu überwachen. Sie stellen außerdem sicher, dass die Prozesse und Protokolle für den Betrieb von Computersystemen auf internen Erfahrungen und Rückmeldungen in Verbindung mit den besten Praktiken der Branche basieren und dass die Cybersicherheitsrichtlinien und -erwartungen der Organisation allen Mitarbeitern klar kommuniziert werden.

- Die Unternehmensleitung stellt sicher, dass die Richtlinien und Verfahren zur Informationssicherheit effektiv umgesetzt werden.
  - Die Unternehmensleitung kennt die nationalen Anforderungen und geschäftlichen Erwartungen an die Kontrolle sensibler Informationen und stellt sicher, dass diese in Sicherungsrichtlinien und Protokollen zur Klassifizierung und Handhabung sensibler Informationen umgesetzt werden.

Um Mitarbeiter in die Lage zu versetzen, Sicherheit, Sicherung und ihre Arbeit als integriertes Ganzes zu betrachten, sind folgende Aspekte wesentlich:

- Personal über Bedrohung aufklären
- Einbeziehung des Personals in die Entscheidungsfindung
- Festlegung von Sicherungskompetenzen und Verantwortlichkeiten
- Anreize schaffen
- Sicherung einfacher und bequemer machen
- Bildung von Teams zum Auffinden und zur Behebung von Schwachstellen
- Verpflichtung zu einer effektiven Kommunikation
- Einführung von engagierten Ausbildungs- und Schulungsprogrammen
- Kommunikation, Lernen und Korrekturmaßnahmen gegenüber Vergeltungsmaßnahmen in den Vordergrund stellen
- ein starkes Programm zur Meldung von Missverständnissen einrichten
- Herausforderungen verstehen
- Verantwortung des Vorstands zur Erstellung einer Whistleblowing-Politik verstehen

2.3.2.3 Die menschliche Dimension der Sicherung radioaktiver Quellen: Vom Bewusstsein zur Kultur

Im Bericht „*The Human Dimension of Security for Radioactive Sources: From Awareness to Culture*“ von Igor Khripunov et al /KHR 14/ wird neben den bereits beschriebenen Aspekten der Sicherungskultur der IAEA auf Besonderheiten der Sicherung von

radioaktiven Quellen eingegangen. Im Rahmen dessen zeigt /KHR 14/ die vier Stufen von der Sensibilisierung für Sicherung bis hin zu einer wirksamen Sicherungskultur auf (siehe Abb. 2.3):

1. Die Ausbildung vermittelt dem Personal ein Verständnis für die Gründe, Grundprinzipien und Mechanismen des Sicherungssystems für radioaktive Strahlenquellen.
2. Das Training vermittelt Fähigkeiten, Kenntnisse und Informationen, die es dem Personal ermöglichen, seine sicherungsrelevanten Aufgaben und Verantwortlichkeiten wahrzunehmen.
3. Die Sensibilisierung ermöglicht es den Mitarbeitern, Bedrohungen und die sich daraus ergebenden Konsequenzen zu erkennen und ihnen zu begegnen.
4. Engagement wird erreicht, wenn die Mitarbeiter
   a. verstehen, warum Sicherung notwendig ist und was sie bedeutet (Ausbildung),
   b. wissen, wie sie ihre sicherungsrelevanten Aufgaben erfüllen können (Training),
   c. in der Lage sind, ihr Wissen und ihre Fähigkeiten gegebenenfalls zu kombinieren, um sowohl festgelegten als auch unerwarteten Bedrohungen zu begegnen.
5. Sicherungsbewusste Menschen sind motiviert, einen Beitrag zu einer wirksamen Sicherung beizutragen. In diesem Stadium kann die Organisation von sich behaupten, über eine wirksame Sicherungskultur zu verfügen.

Im Anhang von /KHR 14/ ist eine auf radioaktive Quellen angepasste Auflistung der Attribute und Charakteristika der Sicherungskultur nach /IAE 08/ zu finden.

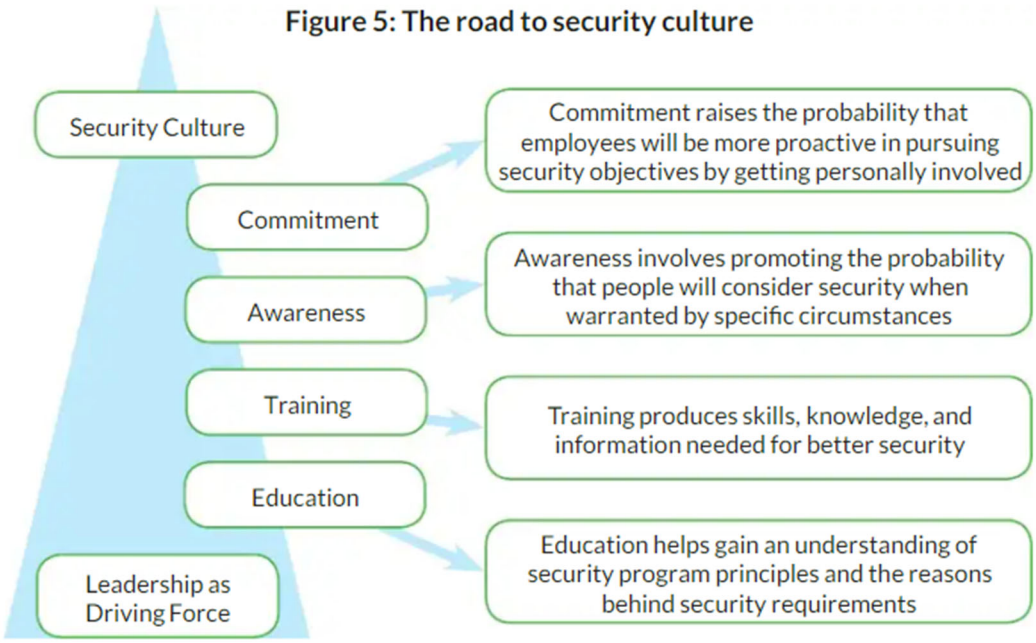

Abb. 2.3 Der Weg von der ersten Sensibilisierung für Sicherung bis zum Erreichen einer wirksamen Sicherungskultur nach /KHR 14/

2.3.3 Erkenntnisse aus nationalen Aktivitäten zur Sicherungskultur – Informationen von UMBW zur Sicherungskultur

Das Ministerium für Umwelt, Klima und Energiewirtschaft Baden-Württemberg (UMBW) hat der GRS zwei Vorträge zur Verfügung gestellt, die im Rahmen dieses Vorhabens ausgewertet wurden:

- The Importance of Security Culture for Computer Security Effectiveness
- Effective Regulatory Oversight/Cooperation between Regulatory Authority and Licensees for Promoting Strong Nuclear Security Culture

The Importance of Security Culture for Computer Security Effectiveness

Im Vortrag „The Importance of Security Culture for Computer Security Effectiveness“, der auf der „International Conference on Computer Security in a Nuclear World“ 2016 bei der IAEA in Wien gehalten wurde, wird die Selbstbeurteilung der Sicherungskultur in deutschen Kernkraftwerken thematisiert /SPE 15/.

Im ersten Teil des Vortrages geht es um die Bedeutung der IT-Sicherheitskultur. Es wird aufgezeigt, dass den häufigsten IT-Sicherheitsverletzungen gemäß BSI fast immer auch

menschliche Fehlhandlungen zu Grunde liegen. Und es werden die verschiedenen Tätergruppen beschrieben. Dabei wird deutlich, dass IT-Sicherheit und Sicherung eng zusammengehören.

Im zweiten Teil des Vortrages geht es um Aspekte der Sicherungskultur im Allgemeinen und die Erstellung eines Fragebogens zur Selbstbeurteilung der Sicherungskultur in deutschen Kernkraftwerken im Speziellen /SPE 15/.

Der im Rahmen eines Pilotprojekts entwickelte Fragebogen, besteht aus 27 Aussagen zur Sicherungskultur, die von den Befragten nach ihrer persönlichen Zustimmung bewertet werden sollten, um eine Selbstbeurteilung der Sicherungskultur der betreffenden Anlagen zu ermöglichen. Der Fragebogen kam 2014 in allen Kernkraftwerken des Bundeslandes Baden-Württemberg zum Einsatz und wurde 2015 auch in anderen kerntechnischen Anlagen der Kategorie I eingesetzt. Der Fragebogen beinhaltet jedoch keine spezifischen Fragen zur Informationssicherheitskultur.

Zunächst werden die Ziele und Vorteile der Selbstbeurteilung der Sicherungskultur formuliert. Da viele Aspekte einer guten Sicherungskultur nicht unmittelbar sichtbar sind, wie z.B. Werte, Prioritäten, Annahmen, Glauben, Erwartungen etc. ist eine Beurteilung der Sicherungskultur nicht ganz leicht. Die Selbstbeurteilung der Sicherungskultur zielt vor allem darauf ab, das persönliche Verhalten der Mitarbeiter in folgenden Bereichen zu stärken /SPE 15/:

- Fachkompetenz
- persönliche Verantwortung
- Einhaltung von Prozeduren
- Teamwork und Kooperation
- Wachsamkeit

Das Führungsverhalten und das Managementsystem tragen bei der Umsetzung dieser Ziele stark zum Erfolg bei. Als weitere Vorteile für die Selbstbeurteilung durch einen Fragebogen werden die folgenden Punkte aufgezählt /SPE 15/:

- tieferes Verständnis von menschlichen Faktoren und nuklearer Sicherungskultur
- klareres Verständnis von Bedenken, Bedürfnissen, Zielen, Motiven der Mitarbeiter

- Identifikation von Verbesserungsmöglichkeiten der Sicherungskultur durch Anreize und Grenzen für Verbesserungen
- Identifikation von Motiven für Änderungen und Grenzen für Änderungen
- Klarheit über die Meinung der Angestellten zu sicherungsrelevanten Themen
- verbesserte Möglichkeiten die Sicherungsregelungen der Organisation selbst zu bewerten, Trend Analysen durchzuführen und die Fortschritte zu überwachen.
- hohe Prioritäten für Aktivitäten, die die Kultur der Organisation gesamtheitlich stärken und Bereiche wie interne Kommunikation und Personalwesen stärken.

Zuletzt wird der Prozess zur Erstellung des Fragebogens und dessen Auswertung beschrieben. Nachdem das Team zur Selbstbeurteilung zusammengestellt ist, beginnt die gemeinsame Planung und Durchführung.

Bei der Auswahl der Indikatoren für die Selbstbeurteilung sollte darauf geachtet werden, dass die Indikatoren die folgenden Kriterien erfüllen /SPE 15/:

- kosteneffizient und verlässlich
- relevant und bewerten, was zu bewerten ist
- auf verfügbaren Daten basierend
- nicht durch Verzerrung oder Manipulation beeinflussbar
- einfach und präzise kommunizierbar
- von unterschiedlichen Gruppen gleich interpretiert werden
- auf den gesamten Betrieb der Organisation anwendbar
- gut bewertbar

Die Gestaltung des Fragebogens ist an die eigene Unternehmenskultur anzupassen. Im Pilotprojekt des Autors wurde der Fragebogen so gestaltet, dass die Befragten eine (subjektive) Bewertung zu den 27 Aussagen zur Informationssicherheitskultur abgeben sollten („trifft zu (1), trifft eher zu (2), trifft eher nicht zu (3), trifft nicht zu (4)“. Zudem gab es die Möglichkeit die einzelnen Fragen zu kommentieren /SPE 15/.

Für den Frageborgen definiert der Autor noch weitere Rahmenbedingungen, die für eine aussagekräftige Auswertung von Bedeutung sind. Dazu zählen /SPE 15/:

- die Selbstbeurteilung ist akzeptiert bei Mitarbeitervertretern
- die Selbstbeurteilung ist akzeptiert bei den Leitern und Managern
- die Anonymität wird garantiert
- freiwillige Teilnahme
- keine regulatorischen Sanktionen der Mitarbeiter als Konsequenz auf die Ergebnisse
- hohe Teilnahme
- Einbeziehung von eigenem und Fremdpersonal
- Einbeziehung von „sicherungsrelevantem“ Personal und „nicht-sicherungsrelevantem“ Personal
- Einbeziehung aller Hierarchie Level
- gleiche Fragen für alle Befragten
- Zeit zum Ausfüllen des Fragebogens < 30 min

Nach der Daten-Erfassung folgt dann die Analyse der Daten und die Vertiefung der Ergebnisse. Im Rahmen des Pilotprojektes wurde ein dreistufiges Ergebnis-Model entwickelt, das die Punkte für die Aussagen in einen Bereich oberhalb des Mittelwertes (Rot), in einen Bereich um den Mittelwert herum (Gelb) und einen Bereich unterhalb des Mittelwertes (Grün) einteilt. Die Rot und Gelb markierten Aussagen liefern dann Anhaltpunkte, für Verbesserungen, Änderungen etc. In dem vorgestellten Pilotprojekt gab es 6 Fragen, die mit Gelb markiert wurden und 4 Fragen, die von weniger als 80% der Befragten beantwortet wurden. Im Fazit und Ausblick gibt der Autor an, dass einige Fragen noch einmal überarbeitet werden sollten und zudem noch einige Fragen zur IT-Sicherung hinzugefügt werden sollen /SPE 15/.

Als Ergebnis des Fragebogens wird ein Abschlussbericht erstellt und ein Aktionsplan entwickelt, der Verbesserungen in der Sicherungskultur ermöglichen soll.

Effective Regulatory Oversight/Cooperation between Regulatory Authority and Licensees for Promoting Strong Nuclear Security Culture

Im Vortrag “Effective Regulatory Oversight/Cooperation between Regulatory Authority and Licensees for Promoting Strong Nuclear Security Culture”, der auf dem “International Workshop on Nuclear Security Culture” der IAEA in Madrid 2016 gehalten wurde, geht es um die vielen Aspekte der Sicherung /SPE 16/.

Zunächst wird aufgezeigt, welche unterschiedlichen Interessenvertreter es gibt und in welcher Beziehung sie zueinanderstehen. An den Betreiber, dem die Verantwortung für Sicherung und Sicherheit obliegt, werden von vielen Seiten unterschiedliche Forderungen herangetragen, die einen sicheren und geschützten Betrieb ermöglichen sollen. Dabei geht es um internationale Verpflichtungen (z.B. durch die IAEA, UN etc.), staatliche Auflagen, Forderungen von Bürgern, Interessenvertretern und Aktivisten etc. Für die Betreiber sollten Regulierungen trotz allem nicht als Hürden angesehen werden, sondern als eine soziale Verpflichtung, die auf Kooperation basiert /SPE 16/.

Da die Sicherung auf dem Prinzip „Defence in Depth“ basiert, ist es wichtig, dass Sicherungsmaßnahmen, die einen potenziellen Angriff hinauszögern können, auch greifen. Dazu zählen z.B. das Design, die Sicherungskultur, das Training mit Bezug zur Sicherung und das sicherheits- und sicherungsgerichtete Handeln der Hauptakteure /SPE 16/.

Das Arbeitsgebiet der Sicherung birgt einige Herausforderungen, da es ein „unsichtbares Nicht-Ereignis“ ist, das bei guter Leistung nicht honoriert wird. Schließlich gibt es keine Erfolgsmeldungen wie zum Beispiel „93 Tage ohne ein sicherheitsrelevantes Ereignis“. Die Schwierigkeiten auf dem Arbeitsgebiet der Sicherung liegen folglich darin, dass sie keine klar messbaren Ergebnisse liefert, unklare Zusammenhänge aufweist, sich ihre Vorteile nur erkennen lassen, wenn es über einen sehr langen Zeitraum keine sicherheitsrelevanten Ereignisse gibt und sie statt eines sichtbaren Erfolges nur bei Misserfolg und Versagen sichtbar wird /SPE 16/.

Der Autor weist in seinem Vortrag auch darauf hin, dass kleine Verstöße in der Sicherung selten berichtet werden. Gemäß Helmreichs Fehler-Pyramide kommen auf ein schwerwiegendes Ereignis 1000 Ereignisse, die nur kleiner Verstöße darstellen und nicht berichtet werden /SPE 16/.

Als Gründe dafür, dass kleinere Verstöße selten berichtet werden, werden die folgenden Ursachen genannt:

- scheinbar keine Bedeutung
- werden nicht erkannt
- Angst vor Überstunden
- Angst vor Sanktionen
- Angst sich zu blamieren
- Motivationsverlust: „Ich habe doch schon so viele Ereignisse gemeldet und niemand nimmt mich ernst“.

Im letzten Teil des Vortrags werden Lösungsvorschläge für diese Problematiken gezeigt. Dazu werden folgende Vorschläge gemacht, was die Regulierungsbehörde tun kann, um nukleare Sicherheitskultur zu fördern und zu stärken /SPE 16/:

- motiviere die Behörde eine Kampagne zu durchzuführen
- begleite und unterstütze die Selbstbeurteilungs-Kampagne
- trage zum Erfahrungsaustausch bei
- überwache, dass der Prozess weiterläuft
- wirke mäßigend darauf ein, dass Statistiken und Leistungsvergleiche nicht übertrieben werden
- beobachte aufmerksam die eigene Sicherungskultur

Eine gut gepflegte Sicherungskultur zeichnet sich dadurch aus, dass sie definiert, trainiert, belohnt, gemessen und gelebt wird /SPE 16/.

2.4 Schnittstelle zwischen Sicherungskultur und Sicherheitskultur

Nachfolgend wird auf einige Dokumente eingegangen, die sich mit der Schnittstelle zwischen Sicherheits- und Sicherungskultur auseinandergesetzt haben:

- INSAG-24 – The Interface Between Safety and Security at Nuclear Power Plants /IAE 10/
- World Institute for Nuclear Security: An Integrated Approach to Nuclear Safety and Nuclear Security /WIN 16a/
- Igor Khripunov et al: Final report on the Proceedings of the International Workshop in Serpong, Indonesia /KHR 18/

2.4.1 IAEA INSAG-24: Schnittstelle zwischen Sicherheits- und Sicherungskultur in Kernkraftwerken

Nach INSAG-24 „*The Interface Between Safety and Security at Nuclear Power Plants*“ /IAE 10/ der IAEA haben nukleare Sicherheit und Sicherung einen gemeinsamen Zweck – den Schutz von Menschen, Gesellschaft und Umwelt. In beiden Fällen wird ein solcher Schutz erreicht, indem eine große Freisetzung von radioaktivem Material verhindert wird. Viele der Grundsätze zur Gewährleistung des Schutzes sind in beiden Fällen gleich, auch wenn ihre Umsetzung unterschiedlich sein kann. Darüber hinaus dienen viele Elemente oder Maßnahmen gleichzeitig dazu, sowohl die Sicherheit als auch die Sicherung zu erhöhen. Beispielsweise dient die Containment-Struktur eines Kernkraftwerks dazu, bei einem Unfall eine signifikante Freisetzung radioaktiver Stoffe in die Umwelt zu verhindern und gleichzeitig eine robuste Struktur bereitzustellen, die den Reaktor vor einem terroristischen Angriff schützt. In ähnlicher Weise dienen Kontrollen zur Beschränkung des Zugangs zu wichtigen Bereichen nicht nur einer Sicherheitsfunktion, indem sie die Exposition von Arbeitern verhindern oder begrenzen und den Zugang zu Wartungszwecken für qualifiziertes Personal kontrollieren, sondern dienen auch einem Sicherungszweck, indem sie unbefugten Zugang durch Eindringlinge verhindern /IAE 10/.

Nichtsdestotrotz gibt es nach INSAG-24 auch Umstände, unter denen Handlungen, die einem Ziel dienen, der Erreichung des anderen Ziels entgegenstehen können. Beispielsweise kann die Einführung von Verzögerungsbarrieren aus Sicherungsgründen den schnellen Zugang zur Reaktion auf ein Sicherheitsereignis oder den Notausstieg durch das Anlagenpersonal einschränken /IAE 10/.

Tatsächlich können Sicherungsüberlegungen dazu dienen, Anlagenpersonal im Falle eines Angriffs von bestimmten Bereichen der Anlage auszuschließen, auf die aus Sicherheitsgründen möglicherweise zugegriffen werden muss. Auch könnten durch Kämpfe kritische Sicherheitsausrüstung oder der Zugang dazu beeinträchtigt werden /IAE 10/.

Auch unterscheiden sich nach INSAG-24 die betrachteten Ereignisse in beiden Bereichen. Sicherheitsbewertungen konzentrieren sich auf Risiken, die sich aus unbeabsichtigten Ereignissen ergeben, die durch Naturereignisse (wie Erdbeben, Tornados oder Überschwemmungen), Hardwareausfälle, andere interne Ereignisse oder Unterbrechungen (wie Feuer, Rohrbruch oder Ausfall der Stromversorgung) oder menschliche Fehler (wie falsche Anwendung von Verfahren oder falsche Ausrichtung von Schaltkreisen) ausgelöst werden. Im Fall der Sicherung ergeben sich die befürchteten Risiken oder

Ereignisse aus böswilligen Handlungen mit der Absicht, Material zu stehlen oder Schäden zu verursachen. Sicherungsereignisse beruhen daher auf „intelligenten“ oder „absichtlichen“ Handlungen, die gezielt zu Diebstahl oder Sabotage und mit der Absicht durchgeführt werden, Schutzmaßnahmen zu umgehen /IAE 10/.

Diese Tatsachen unterstreichen nach INSAG-24 die Bedeutung eines koordinierten Ansatzes für die nukleare Sicherheit und Sicherung. Ziel des Berichts ist es daher, die Schnittstellen zwischen Sicherheit und Sicherung in Kernkraftwerken besser zu verstehen und Wege zu diskutieren, um beide Ziele optimal zu erreichen. Es informiert über vorhandene einschlägige Dokumentation, untersucht bestimmte gemeinsame Grundsätze und schlägt allgemeine Lösungen vor, die zu einem integrierten Ansatz beitragen können. Es werden Schlussfolgerungen gezogen und Empfehlungen mit dem Ziel gegeben, den Schutz der Öffentlichkeit, des Eigentums, der Gesellschaft und der Umwelt durch eine verbesserte und verstärkte Schnittstelle zwischen Sicherheit und Sicherung zu maximieren /IAE 10/.

In Hinblick auf Gemeinsamkeiten und Unterschiede zwischen Sicherheit und Sicherung adressiert INSAG-24 verschiedene Themen, die im Folgenden beschrieben werden.

Führung und Management

Führung in Sicherheitsfragen muss auf den höchsten Ebenen einer Organisation nachgewiesen und in beiden Bereichen durch ein wirksames Managementsystem erreicht werden. Um ein ausgewogenes Verhältnis zwischen Sicherheit und Sicherung und ein koordiniertes Handeln im Notfall zu gewährleisten, sollte die letztendliche Verantwortung für Sicherheit und Sicherung am Standort durch eine einzige, einheitliche Managementstruktur in der Betriebsorganisation erreicht werden.

In das Managementsystem sollte eine Sicherheits- und Sicherungskultur integriert werden, die die Einstellungen und das Verhalten des Einzelnen bestimmt. Es gibt einige Elemente, die für jede Kultur einzigartig sind. Ein Unterschied zwischen den beiden Kulturen betrifft beispielsweise die Art und Weise, wie Informationen gehandhabt werden. Im Sicherungsbereich sollte die Weitergabe von Informationen in der Regel auf einen kleinen und ausgewählten Personenkreis beschränkt werden, um zu verhindern, dass sensible Informationen im Zusammenhang mit Schutzmaßnahmen oder Anlagenschwächen in die Hände von Gegnern gelangen. Darüber hinaus ist es auch wichtig,

Maßnahmen zu ergreifen, um sicherzustellen, dass das Wissen um böswillige Handlungen nicht zu ähnlichen Ereignissen anregt.

Im Sicherheitsbereich hingegen gilt die allgemeine Regel nach Transparenz. Beispielsweise kann es besonders wichtig sein, Erfahrungsberichte auszutauschen und so zu verhindern, dass sich Störfälle oder Unfälle in einem Kernkraftwerk in anderen wiederholen. Aufgrund dieser Unterschiede ist es erforderlich, dass das Management Systeme einführt, die eine wesentliche Transparenz hinsichtlich der meisten sicherheitsrelevanten Informationen und gleichzeitig die Vertraulichkeit der meisten Sicherungsinformationen gewährleisten.

Das Management sollte sich auch um die Förderung der Sicherheits- und der Sicherungskultur bemühen. Diese Kulturen beinhalten oft Individuen mit unterschiedlichem Hintergrund und Erfahrungen. Das heißt, Sicherungspersonal hat im Gegensatz zu Sicherheitspersonal oft einen militärischen oder polizeilichen Hintergrund. Da Kultur ein Attribut sowohl von Organisationen als auch von Einzelpersonen ist, ist es wichtig, sowohl dem Sicherungspersonal als auch dem Sicherheitspersonal die Bedeutung jedes Bereichs zu nahezubringen und gleichzeitig die Bedeutung von Zusammenarbeit und Ausgewogenheit zu betonen, um einen optimalen Schutz zu erreichen.

In diesem Zusammenhang ist die Geschäftsleitung dafür verantwortlich, angemessene Vorkehrungen zu treffen, um die Kompetenz und Integrität der Mitarbeiter zu gewährleisten, deren Handlungen die Sicherheit oder die Sicherung beeinträchtigen könnten.

Optimierung des Schutzes

Der Grundsatz der Schutzoptimierung, der sowohl für Sicherheit und Sicherung gilt, beruht auf dem Gedanken, dass Strahlenrisiken so gering wie vernünftigerweise erreichbar zu halten sind. Alle Risiken, auch die aus böswilligen Handlungen, müssen bewertet werden. Das Risiko ist im Hinblick auf die Festlegung angemessener und verhältnismäßiger Maßnahmen zu analysieren. Die Identifizierung von Risiken aufgrund von Naturereignissen, Geräteausfällen oder menschlichen Fehlern beruht auf deterministischen Methoden (Expertenurteil, Auswertung von Betriebserfahrungen), die häufig durch probabilistische Methoden ergänzt werden. Die Identifizierung von Risiken im Sicherungsbereich ist üblicherweise deterministisch, da es schwierig ist, probabilistische Techniken anzuwenden. Unabhängig von der Methodik müssen jedoch die Risiken identifiziert und bewertet werden. Darüber hinaus sollten diese Risiken regelmäßig neu bewertet

werden, um die Entwicklung der Technologie, mögliche Änderungen der Bedrohungen und alle damit verbundenen Änderungen der Sicherheits- und/oder Sicherungsanforderungen widerzuspiegeln.

Vermeidung von Sicherheits- und Sicherungsereignissen

Defense in Depth ist ein grundlegendes Konzept, das von Experten für nukleare Sicherheit bei der Planung und beim Betrieb angewendet wird. Im Sicherungskontext umfasst das Defense in Depth Konzept die Einrichtung einer Reihe von Schutzebenen für potenzielle Ziele für Sabotage oder Diebstahl. Dieser Ansatz berücksichtigt die Robustheit von Systemen, Strukturen und Komponenten (SSC) durch die Gestaltung von Schutzsystemen gegen feindliche Fähigkeiten, berücksichtigt Unfallmanagementmaßnahmen und Eindämmungssysteme und ist bestrebt, die Funktion dieser SSC durch physische Schutzmaßnahmen zu schützen. Ein integrierter Bestandteil der Prävention sind Systeme zur kontinuierlichen Überwachung und Frühwarnung bei einem möglichen Versuch, eine Schutzebene zu umgehen oder den Ausfall zu verursachen.

Sicherheitsexperten sollten in enger Zusammenarbeit mit Sicherungsexperten die Folgen böswilliger Handlungen im Kontext der staatlichen Bedrohungslage bewerten und die Mindestausstattung an Ausrüstung, Systemen oder Geräten ermitteln, die geschützt werden sollten. Zu diesem Zweck sollten bei Sicherungsbewertung auch Maßnahmen berücksichtigt werden, die in der Einrichtung zu Sicherheitszwecken vorgesehen sind.

Die erste Verteidigungslinie für die Sicherung besteht aus Abschreckungsschritten, die dazu dienen, einen Angreifer von einem Angriffsversuch abzuhalten. Abschreckung könnte beispielsweise die Verhinderung des Zugangs zu Informationen umfassen, die für einen Angriff erforderlich sind, die Hervorhebung der strafrechtlichen Sanktionen, die für einen potenziellen Angreifer gelten, und/oder die Einrichtung von Überwachungs- und Erfassungssystemen für nachrichtendienstliche Erkenntnisse, die ein frühzeitiges Abfangen von Angreifern ermöglichen.

Die zweite Verteidigungslinie besteht in der Umsetzung eines Sicherungsplans, der verhindert, dass ein Angreifer einen erfolgreichen Angriff ausführt, oder den Angreifer zumindest so lange aufhält, dass externe Unterstützung durch Polizeikräfte möglich ist. Diese zweite Verteidigungslinie besteht aus mehreren Schichten. Der Sicherungsplan beinhaltet typischerweise eine umfassende Strategie zur Verteidigung der Einrichtung vor einem Angriff auf der Ebene der Auslegungsbedrohung. Die Abwehr von

Bedrohungen, die über die Auslegungsgrundlage hinausgehen, erfordert eine umfassende Koordination zwischen dem Einrichtungspersonal und externen Verstärkungen.

Notfallvorbereitung

Betreiber sowie staatliche Behörden sind verpflichtet, Pläne zur Begrenzung der Folgen eines radiologischen Unfalls zu entwickeln. Solche Pläne sollten sowohl Sicherheits- als auch Sicherungsereignisse umfassen.

Die Bewältigung einer aus einem terroristischen Akt resultierenden Krise kann die Beteiligung einer größeren Zahl staatlicher Stellen (Strafverfolgungsbehörden, Bombenentsorgungsdienste und Justizbehörden) erfordern, als dies bei einem Sicherheitsereignis der Fall ist.

Sicherheitspläne für ein Kernkraftwerk sollten nicht nur die Verhinderung böswilliger Handlungen umfassen, sondern auch die Festlegung wirksamer Gegenmaßnahmen (sogenannte Notfallpläne), einschließlich beispielsweise der Standortsicherung. Es besteht offensichtlich die Notwendigkeit sicherzustellen, dass der Sicherungsplan mit dem Sicherheitsplan kompatibel ist und diesen ergänzt. Daher muss sichergestellt werden, dass im Rahmen der Gesamtnotfallplanung die Koordination zwischen den Sicherheitskräften und den Sicherungskräften organisiert wird.

Das Notfallmanagement kann im Falle eines Terroranschlags einige ganz besondere Probleme mit sich bringen. Sicherheitsmaßnahmen vor Ort unter der Verantwortung des Betreibers müssen ergriffen werden, um mögliche Folgen zu minimieren oder abzumildern. Sicherungsmaßnahmen, zu denen auch der Einsatz staatlicher Eingreiftruppen zählen kann, werden sich auf die Neutralisierung der Gegner konzentrieren, um dadurch weiteren Schaden zu verhindern und Einsatzkräfte zu schützen. Diese Aktionen müssen koordiniert werden. Es ist daher erforderlich, gemeinsame Übungen durchzuführen, um die Koordinierung der Sicherheitsorganisationen zu ermöglichen.

2.4.2 WINS: Integrierter Ansatz für nukleare Sicherheit und Sicherung

Im Bericht „*An Integrated Approach to Nuclear Safety and Nuclear Security*“ /WIN 16a/ des World Institute for Nuclear Security (WINS) werden die Begriffe nukleare Sicherheit und Sicherung definiert (siehe Kap. 2.1).

Nukleare Sicherheit und Sicherung haben nach /WIN 16a/ gemeinsame Ziele, nämlich den Schutz der Öffentlichkeit, des Personals und der Anlage. Durch die Stärkung der Schnittstellen zwischen dem Sicherungspersonal und dem übrigen Personal der Anlage können alle Mitarbeiter zusammenarbeiten, um dieses gemeinsame Ziel zu erreichen. Die Leitung einer kerntechnischen Anlage hat schon immer die verschiedenen Elemente der Sicherheit, wie nukleare Sicherheit, Personal, Strahlenschutz, Brandschutz und Umweltschutz, integriert. Dies hat sich als erfolgreich erwiesen, wie an den WANO-Sicherheitsindikatoren und den damit verbundenen Peer-Reviews gemessen wird. Die Schnittstelle zwischen Sicherheit und Sicherung hat jedoch aus verschiedenen Gründen nicht den gleichen Grad an Integration erreicht. Dies kann zu Reibungen an den verschiedenen Schnittstellen und zu einer mangelnden Beteiligung der Mitarbeiter an Initiativen zur Verbesserung der Sicherung führen.

Während alle Mitarbeiter für die Notwendigkeit einer kontinuierlichen Verbesserung der Sicherheit sensibilisiert wurden, ist ihre Beteiligung an sicherungsrelevanten Angelegenheiten möglicherweise noch nicht optimal. Infolgedessen kann beispielsweise die wirksame Umsetzung eines Programms für Insider-Bedrohungen gefährdet sein, wenn die Sicherungs- und Sicherheitsdienste nicht enger zusammenarbeiten. Außerdem ist das für die nukleare Sicherheit zuständige Personal zwar mit den Einzelheiten des Auslegungsstörfalls (DBA) in ihrer Anlage vertraut, aber weniger mit der Auslegungsbedrohung (DBT). Auch wird das Sicherungspersonal höchstwahrscheinlich nicht mit den Einzelheiten der DBA vertraut sein. Eine engere Integration soll die Wissenslücke auf beiden Seiten zu schließen.

Kommt in einer Anlage nukleares Material zum Einsatz, besteht potenziell die Gefahr, dass Kriminelle oder Terroristen versuchen könnten, dieses Material zu stehlen oder die Anlage anzugreifen. Diese Bedrohungen bestehen sowohl mit als auch ohne Hilfe von Insidern. Das Risiko eines erfolgreichen Angriffs kann durch ein integriertes Konzept für die nukleare Sicherheit und Sicherung verringert werden. Darüber hinaus kann nach /WIN 16a/ der sichere Betrieb durch Verwendung von Zugangsberechtigungsfunktionen verbessert werden, die darauf ausgelegt sind, vertrauenswürdiges und zuverlässiges Personal bereitzustellen.

Nach /WIN 16a/ ist es für die Entwicklung eines integrierten Konzepts für die nukleare Sicherheit und Sicherung hilfreich, drei verschiedene Ebenen der Organisation zu betrachten: die strategische, die operative und die personelle Ebene.

- Die strategische Ebene befasst sich mit Maßnahmen, die leitende Angestellte ergreifen können, um die Politik in ihrer Organisation zu beeinflussen.
- Die operative Ebene befasst sich mit Maßnahmen, die von den Abteilungen ergriffen werden müssen, die mit der Sicherung zu tun haben, um die Integration zu gewährleisten.
- Die personelle Ebene befasst sich mit Maßnahmen, die von der Belegschaft oder von Besuchern ergriffen werden müssen.

Im weiteren Verlauf fasst /WIN 16a/ verschiedene Aspekte zusammen, die auf jeder Ebene zu berücksichtigen sind, und beschreibt praktische Maßnahmen und Leistungskriterien für die Umsetzung eines integrierten Ansatzes innerhalb einer Organisation.

2.4.3 Harmonisierung von Sicherheits- und Sicherungskultur in nuklearen Einrichtungen

Um zu motivieren, warum es notwendig ist, die Sicherheits- und die Sicherungskultur zu harmonisieren, wird im „*Final report on the Proceedings of the International Workshop in Serpong, Indonesia“ von Igor* Khripunov /KHR 18/ zunächst die Organisationsstruktur der IAEA beschrieben. Die Verantwortung für beide Themenfelder liegt hier zwar in einer gemeinsamen Abteilung, die Aufgaben werden jedoch in zwei verschiedenen Fachbereichen bearbeitet. Nach /KHR 18/ ist es entscheidend für die Pflege einer beides umfassenden Kultur zu verstehen, wo sich Sicherheit und Sicherung überschneiden und zu erkennen, wo Möglichkeiten zur Nutzung von Synergien zwischen beiden Kulturen bestehen. Da beide Elemente untrennbar miteinander verbunden sind, ist zu bestimmen, welche Funktionen sich ergänzen und welche nicht.

Nach /KHR 18/ beinhaltet das Management der Schnittstelle zwischen Sicherheitskultur und Sicherungskultur:

1. Das Verständnis gemeinsamer Ansätze der nuklearen Sicherheits- und Sicherungskultur.
2. Überlegungen, wie diese Gemeinsamkeiten gehandhabt werden können, um beide Kulturen zu stärken und zu unterstützen.

3. Verständnis der Unterschiede zwischen nuklearer Sicherheit und Sicherung und Verständnis dafür, wie diese Unterschiede zu unterschiedlichen Einstellungen und Ansätzen zwischen den beiden Kulturen führen können.

4. Überlegungen zum Umgang mit diesen unterschiedlichen Einstellungen, um sowohl die nukleare Sicherheit als auch die nukleare Sicherung zu unterstützen.

Ansätze und Bemühungen zur Verbesserung der Harmonisierung der Sicherheits-Sicherungs-Kultur-Schnittstelle können umfassen /KHR 18/:

1. Sensibilisierung und Verständnis für den Zusammenhang zwischen nuklearer Sicherheit und Gefahrenabwehr.

2. Regelmäßige Einberufung hochrangiger Sitzungen zu Sicherheits-Sicherungs-Protokollen, um sicherzustellen, dass die Schnittstelle angemessene Aufmerksamkeit erhält und Konflikte gelöst werden.

3. Vereinfachung der Kommunikation zwischen dem für die nukleare Sicherheit und die nukleare Sicherung zuständigen Personal.

In /KHR 18/ werden verschiedene Themen genannt, die nach Meinung der Autoren entscheidend sind für den Harmonisierungsprozess zwischen Sicherheits- und Sicherungskultur. Hierzu zählen:

- <u>Sichtbares Engagement auf allen Managementebenen</u>

  Es ist notwendig, dass das Management auf allen Führungsebenen die Harmonisierung der Sicherheits- und Sicherungskultur voll unterstützt, indem es ein sichtbares, tragfähiges und nachhaltiges Engagement für diesen Prozess demonstriert. Führungskräfte müssen die Vorteile der Sicherheits- und Sicherungskultur erkennen und kommunizieren. Zum Beispiel könnte das Management bestimmte Zeit einplanen, um diese Themen in Routinebesprechungen wie einem morgendlichen Briefing zu behandeln. Manager könnten Erklärungen und/oder Präsentationen vorlegen, die aktuelle Themen der Sicherheit berücksichtigen.

  Bei der Überprüfung der Dokumentation sollten sich die Manager der Notwendigkeit bewusst sein, eine Harmonisierung der Sicherheitskultur in Grundsatzerklärungen, Leitlinien, Richtlinien usw. aufzunehmen. Außerdem muss sich das Management zur Teilnahme an Weiterbildungs- und Schulungsprogrammen verpflichten und sollte sicherstellen, dass es eine gemeinsame Schulung zu Sicherheit und Sicherung gibt.

- Verbreitung von Informationen, Wissen und Daten

  Die Verbreitung von Informationen, Wissen und Daten erfordert ein vielschichtiges interaktives Programm, das kontinuierlich weiterentwickelt und instandgehalten werden muss. Eine wirksame Methode der Informationsverbreitung ist die Vermittlung von Informationen über Schulungen und Seminare. Die Harmonisierung von Sicherheits- und Sicherungskulturen könnte erleichtert werden, indem in gemeinsam abgehaltenen Schulungen die Ergebnisse der Sicherheits-Selbstbewertungen kommuniziert werden. Eine Harmonisierung könnte durch Schulungen zu Sicherheits- und Sicherungskultur für nicht sicherheitsrelevantes Personal und die Gewährleistung von Sicherheitsinformationen bei nicht sicherheitsrelevanten Mitarbeitern durch E-Learning-Informationssysteme erreicht werden.

- Kontinuierliche Motivation zur Vermeidung von Selbstzufriedenheit

  Ein Programm oder Konzept muss – auch wenn es gut ist - kontinuierlich verstärkt und motiviert werden, um sicherzustellen, dass es in die Routinearbeit integriert wird.

  Zu motivierenden Maßnahmen gehören kontinuierliche Schulungen, Coachings und die Ermutigung der Mitarbeiter auf der untersten Ebene in Bezug auf die Sicherheitskultur.

  Plakate, Flyer und Banner zum Thema Sicherheit können zwar wichtige Ideen untermauern, aber diese Erinnerungen allein reichen nicht aus, um eine wirksame Motivation zu gewährleisten. Zusätzliche Maßnahmen zur Motivationsförderung umfassen:

  (1) Feedback willkommen heißen und Teamgeist fördern, um Verbesserungen anzuregen
  (2) Bedenken in Hinblick auf Selbstzufriedenheit bei Mitarbeiterversammlungen besprechen
  (3) daran arbeiten, das Vertrauen zwischen Mitarbeitern und Management zu erhöhen
  (4) Erstellung eines langfristigen Änderungsmanagementplans als Teil der kontinuierlichen Verbesserung.

- Einbeziehung von Themen bei Sonder- und Generalversammlungen

  Ein wichtiges Element der Harmonisierung der Sicherheitskultur ist die Sensibilisierung für die gemeinsame Verantwortung für Sicherheit und Schutz. Meetings sind ein idealer Ort für Diskussionen zu verwandten Themen. Sitzungen, die

Diskussionen über eine integrierte nukleare Sicherheits-/Sicherungskultur beinhalten, könnten in einer Vielzahl von Formaten durchgeführt werden.

Organisationen führen häufig separate interne Meetings zu Sicherheitsthemen durch. Es sollte ein Plan erstellt werden, wie Sitzungen eingerichtet und koordiniert werden könnten, um eine Sicherheits-Sicherungs-Harmonisierung bei gleichzeitiger Minimierung der Auswirkungen auf Zeit, Aufwand und Ressourcen einzuschließen.

- Klar definierte Verantwortlichkeiten für Einzelpersonen

  Es ist sehr wahrscheinlich, dass der Prozess der Harmonisierung der Sicherheits- und Sicherungskultur unscharf wird oder an Bedeutung verliert, es sei denn, es gibt Personen, die speziell damit beauftragt sind, sicherzustellen, dass dieser Prozess so lange aufrechterhalten wird, bis er in den Betrieb und die Aktivitäten integriert wird.

  Eine der wichtigsten Aufgaben verantwortlicher Personen wäre es, die Bemühungen zu leiten, den Wettbewerb zwischen Sicherheits- und Sicherungspersonal zu beseitigen oder zu mildern und die Zusammenarbeit zu fördern.

- Lernen und kontinuierliche Verbesserung

  Damit der Prozess der Harmonisierung der Sicherheits- und Sicherungskultur ausgereift und nachhaltig ist, muss ein Programm des fortlaufenden Lernens und der kontinuierlichen Evaluierung und Verbesserung zur Unterstützung der Harmonisierungsbemühungen vorhanden sein. Dies sollte eine Offenheit zwischen Sicherung und Sicherheit beinhalten, um die Kommunikation und das Lernen zu erleichtern. Dies könnte die Erstellung einer kombinierten Datenbank mit Erkenntnissen aus dem Bereich Sicherheit und Sicherung, die Abhaltung von vierteljährlichen Sitzungen zur Überprüfung von Vorfällen und die Berichterstattung über den aktuellen Status sowie den Austausch bewährter Verfahren zur Harmonisierung von Sicherheit und Schutz umfassen.

- Tracking-Mechanismen zur Messung des Fortschritts

  Es ist wichtig, die Fortschritte zu verfolgen, um festzustellen, ob Initiativen zur Entwicklung und Verbesserung der Harmonisierung oder Integration der Sicherheits- und Sicherungskultur umgesetzt werden und wirksam sind. Dies könnte die Erstellung allgemeiner und spezifischer Sicherheitsleistungsindikatoren umfassen, um den Fortschritt zu messen. Ein Schlüsselparameter, der verfolgt werden sollte, könnte die Durchführung gleichzeitiger Selbstbewertungen sein, um Sicherheit und Sicherung effizienter zu machen.

- Aktualisieren von Richtlinien, Verfahren und Protokollen

  Ein wichtiger Teil eines nachhaltigen integrierten nuklearen Sicherheitskulturprogramms besteht darin, sicherzustellen, dass die einschlägigen Richtlinien, Verfahren und Protokolle aktualisiert werden, um das aktuelle und sich entwickelnde nukleare Sicherheitsumfeld der Operationen widerzuspiegeln. Es sollte ein Programm erstellt werden, um sicherzustellen, dass Richtlinien, Verfahren und Protokolle routinemäßig überprüft und entsprechend den Sicherheitsentwicklungen aktualisiert werden.

- Beitrag der Aufsichtsbehörde

  Ein Beitrag der Regulierungsbehörde kann für die Harmonisierung der Sicherheits- und Sicherungskultur von Vorteil sein.

Als mögliche Maßnahmen werden in /KHR 18/ folgende vorgeschlagen:

- Leitbilder und Aktionspläne

  Der Inhalt eines Leitbildes sollte das Ziel der Mission angeben. Es sollte klar definieren, warum Sicherheit und Sicherung integriert sind. Der Inhalt eines typischen Aktionsplans kann u.a. umfassen:

  1. Bewertung der aktuellen Situation, die die Rechtfertigung für die Aktion durch Ermittlung des Bedarfs liefert;
  2. klare Ziele;
  3. gute Maßnahmen für diese Ziele – diese Maßnahmen sollten vor Beginn des Plans entwickelt werden;
  4. Rollen und Verantwortlichkeiten;
  5. Hindernisse für den Erfolg;
  6. Zeitleiste;
  7. Budget und andere Ressourcen;
  8. Meilensteine und wichtige Umsetzungsschritte zur Messung des Fortschritts;
  9. erwartete Ergebnisse und Enddatum;
  10. Kommunikationsplan zur Unterstützung bei der Umsetzung;
  11. Liste der Interessengruppen/Interdependenzen.

- Ausbildung und Qualifizierung

  Die Schritte zur Entwicklung einer effektiven Ausbildung sind:

  1. Analyse der aktuellen Situation und Entwicklung eines Plans für die Ausbildungsentwicklung;

2. Spezialisten mit entsprechenden Kenntnissen und Qualifikationen auswählen, um die Schulungsmaterialien zu präsentieren;

3. durch Benchmarking die Verwendung geeigneter Schulungsmaterialien zu Sicherheit, Schutz und Sicherheitskultur sicherstellen;

4. die Dauer der Schulungen und den Gesamtverlauf festlegen;

5. zu schulende Zielgruppen und für die Zielgruppe anwendbare Ausbildungsniveaus ermitteln;

6. sicherstellen, dass sich jeder bewusst ist und zustimmt, dass eine glaubwürdige Bedrohung besteht und nukleare Sicherheit und Gefahrenabwehr wichtig sind;

7. laufende, integrierte Sicherheitsschulungen abhalten;

8. gemeinsame Schulungen durchführen, um das Sicherheitsbewusstsein zu schärfen.

Es kann ratsam sein, Sicherheitstrainingsmaterialien zu überprüfen und nach Möglichkeiten zur Entwicklung integrierter Trainingsmodule zu suchen, wo immer dies möglich ist.

- Selbsteinschätzung und Verbesserung

  Es könnte von Vorteil sein, bei der Durchführung von Selbstbewertungen für Sicherheits- und/oder Sicherungsbewertungen sowohl Sicherheitsgutachter als auch Sicherungsgutachter einzubeziehen. Darüber hinaus wäre es hilfreich, den Prozess der Suche nach Möglichkeiten zur Harmonisierung von Sicherheits- und Sicherungs-Selbstbewertungen fortzusetzen, um gemeinsame Elemente in einem einzigen Bewertungsprozess zu behandeln.

  Zur Gestaltung eines harmonisierten Sicherheits-Sicherungs-Selbstbewertungsprogramms gehören

  (1) die Entscheidung über die Zusammensetzung des Selbstbewertungsteams;

  (2) Festlegung des Geltungsbereichs und der Ziele für die Harmonisierung;

  (3) Definieren des Umsetzungszeitplans;

  (4) Verantwortung für den Prozess;

  (5) Identifizierung möglicher Herausforderungen, die angegangen werden müssen.

- Korrekturmaßnahmenpläne

  Korrekturmaßnahmenpläne sind die letzte Stufe der Selbstbewertung, aus denen Korrekturmaßnahmen zur Verbesserung der Sicherheits- und Sicherungskultur entwickelt werden. Anhand der Pläne werden Probleme und Mängel festgestellt.

- Verbreitung von *Lessons Learned* und Fallstudien

  Zu den gewonnenen Erkenntnissen gehört die Nutzung von Erfahrungen aus einem Projekt, einer Operation oder einem Auftrag, die bei zukünftigen Bemühungen berücksichtigt werden sollten. Ein Ziel der gewonnenen Erkenntnisse sollte darin bestehen, die Kommunikation über die Harmonisierung zu verstärken, wobei dem menschlichen Element Aufmerksamkeit geschenkt wird.

  Da der Lessons-Learned-Prozess Diskussionen über Fehler beinhaltet, ist es wichtig, bei der Dokumentation und Verbreitung von Informationen Vorsicht und Sensibilität walten zu lassen und die Auswirkungen auf Personal und Einzelpersonen bei der Erstellung der Beschreibungen zu berücksichtigen. Schwierigkeiten können auftreten, wenn die gewonnenen Erkenntnisse vertrauliche oder geheime Informationen beinhalten. Bei der Entscheidung, wie und wann Informationen für die Verbreitung von gewonnenen Erkenntnissen freigegeben werden sollen, muss eine Beurteilung vorgenommen werden.

- Notfallpläne

  Sicherheit und Sicherung sind aufgrund der Natur von Notfallplänen bereits zu einem gewissen Grad integriert; unter Notfallbedingungen teilen sich Sicherheit und Sicherung einige Ressourcen. Sicherheits- und Sicherungsbeauftragte sollten zusammenarbeiten, um Notfallpläne zu erstellen und zu aktualisieren, um sicherzustellen, dass Sicherheit und Sicherung gleichermaßen berücksichtigt werden.

Abschließend wird in /KHR 18/ ein Prozess vorgestellt, um Sicherheits- und Sicherungskultur zu harmonisieren. Er umfasst insgesamt 6 Phasen:

1. Bewusstsein

   In der Anfangsphase wird anerkannt, dass die Organisation wenig oder keine kulturelle Koordination zwischen ihren Sicherheits- und Sicherungsfunktionen hat. Unter dieser Bedingung ist die Organisation, die für die nukleare Sicherheit verantwortlich ist, möglicherweise nicht vollständig über die Sicherungskultur, Sicherheitsentscheidungen, Vereinbarungen etc. informiert. Umgekehrt ist die Sicherungsorganisation

möglicherweise nicht gut mit der Sicherheitskultur vertraut, die dem Schutz des Personals oberste Priorität einräumt. Diese Situation kann dazu führen, dass Aktionen, die in der einen Kultur durchgeführt werden, die Aktionen der anderen erheblich beeinflussen, ohne dass ein vollständiges Bewusstsein der Auswirkungen dieser Aktionen vorhanden ist. Der erste Schritt in diesem Prozess besteht darin, das Bewusstsein sowohl der Sicherheits- und Sicherungsfunktionen als auch ihrer gegenseitigen Auswirkungen, ihre Gemeinsamkeiten und Konfliktpunkte sowie die Vorteile einer Zusammenarbeit im Rahmen der Praktikabilität zu stärken, um für beide Seiten vorteilhafte kulturelle Ziele zu erreichen.

2. Kommunikation

Sobald das Bewusstsein dafür besteht, dass eine Zusammenarbeit zwischen Sicherheits- und Sicherungsfunktionen sehr wünschenswert und nützlich ist, besteht der zweite Schritt des Prozesses darin, eine effektive Kommunikation aufzubauen. Um eine zielgerichtete Harmonisierung der Sicherheits- und Sicherungskultur zu bewirken, muss das Kommunikationsniveau erhöht werden, damit beide Organisationen aktiv zusammenarbeiten, um Informationen zu verbreiten und sich gegenseitig über Themen von gegenseitigem Interesse zu informieren.

3. Verständnis

Die Einrichtung eines funktionierenden Kommunikationssystems bietet eine Plattform für den Austausch von Informationen und ein tieferes Verständnis dafür, wie die Funktionen von Sicherheit und Sicherung miteinander verbunden sind. Es ist wichtig, dass die Informationen nicht nur weitergegeben werden, sondern dass sie von beiden Kulturen im Hinblick darauf, wie sich Sicherheit auf die Sicherung auswirkt und umgekehrt, vollständig verstanden werden müssen. Ein umfassendes Verständnis der gemeinsamen kulturellen Elemente schafft eine Grundlage für das Erkennen von Kooperationsmöglichkeiten und proaktives Handeln auf allen Ebenen der Organisation. Umgekehrt begründet das Verständnis dieser Zusammenhänge auch das Wissen, dass eine mangelnde Kommunikation und Koordination zwischen seinen Sicherheits- und Sicherungsfunktionen zu einem erhöhten Bedrohungsrisiko und einer erhöhten Anfälligkeit für beide führt.

4. Kooperation

Mit zunehmendem Verständnis für den Wert der Harmonisierung werden die Kooperationsmöglichkeiten selbstverständlicher. An dieser Stelle kann erwartet werden,

dass die Einzelpersonen innerhalb der Organisation aktiv nach Möglichkeiten zur Zusammenarbeit suchen, um den gegenseitigen Nutzen einer solchen Zusammenarbeit zu verstehen. In dieser Phase lernen die Sicherheits- und Sicherungsorganisationen, wann immer möglich zusammenzuarbeiten, um das Protokoll zu rationalisieren, sowohl Sicherheits- als auch Sicherungsprinzipien zu erleichtern und betriebsbedingte Risiken zu managen.

5. Harmonisierung

   Mit zunehmender Zusammenarbeit kann die Organisation beginnen, eine echte Integration gemeinsamer Sicherheitselemente aus funktionaler Sicht zu realisieren. Diese Harmonisierung bedeutet nicht, dass eine Organisation ihre internen Ziele opfern oder Verantwortungsbereiche aufgeben muss; es bedeutet vielmehr, dass jede Organisation einen systematischen Prozess implementiert hat, um sicherzustellen, dass die gesamte Organisation von einem gut koordinierten und harmonisierten Sicherheits- und Sicherungsprozess profitiert. Dieses Bekenntnis zu einem höheren kulturellen Ziel ist die ultimative Phase der kulturellen Harmonisierung und kann die Grundlage für große Vorteile wie optimierte Abläufe, reduzierte Kosten und erhöhte Sicherheit sein. An dieser Stelle müssen sich nicht nur die Mitarbeiter oder Betriebsleiter, sondern die gesamte Organisation von oben bis unten auf harmonisierte Ziele der Sicherheitskultur verpflichten.

6. Instandhaltung

   Nachdem ein Programm vollständig harmonisiert und etabliert ist, muss das fortlaufende Programm aufrechterhalten werden, um sicherzustellen, dass die Harmonisierung für neues Personal, betriebliche Veränderungen und andere Faktoren innerhalb der Unternehmenskultur beibehalten wird. Dies sollte eine regelmäßige Bewertung der nuklearen Sicherheits- und Sicherungskultur umfassen, um die Wirksamkeit der Harmonisierung zu bewerten. Die Instandhaltung würde auch die Durchführung von Korrekturmaßnahmen und den Austausch von gewonnenen Erkenntnissen umfassen.

2.5 Informationssicherheit und Informationssicherheitskultur

Nachfolgend werden einige Dokumente zur IT-Sicherheit dargestellt und ihre Inhalte zusammengefasst.

2.5.1 IT-Grundschutz-Kompendium des BSI

Beim IT-Grundschutz-Kompendium /BSI 22/ handelt es sich um einen vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten und jährlich aktualisierten Katalog, der eine grundlegende Basis zu berücksichtigender Aspekte im Zusammenhang mit dem Thema Informationssicherheit darstellt. Thematisch umfasst das IT-Grundschutz-Kompendium des BSI ein breites Spektrum von organisationalen, konzeptionellen und technischen Aspekten mit Bezug zur Informationssicherheit:

- Sicherheitsmanagement
- Organisation und Personal
- Konzeption und Vorgehensweise (z.B. Kryptokonzept, Datensicherungskonzept, Informationssicherheit auf Auslandsreisen, Informationsaustausch)
- Betrieb (z.B. IT-Administration, Schutz vor Schadprogrammen, Protokollierung, Archivierung, Outsourcing für Kunden/Dienstleister)
- Detektion und Reaktion (z.B. Detektion von sicherheitsrelevanten Ereignissen, Behandlung/Bereinigung von Sicherheitsvorfällen, Audits und Revisionen)
- Anwendungen (z.B. Office-Produkte, Webanwendungen und Webservices, Allgemeiner E-Mail-Client und -Server, Entwicklung von Individualsoftware)
- IT-Systeme (z.B. Speicherlösungen, Laptops, Mobiltelefone, Wechseldatenträger)
- Industrielle IT (z.B. Prozessleit- und Automatisierungstechnik, Maschinen, Fernwartung im industriellen Umfeld)
- Netze und Kommunikation (z.B. Netzarchitektur- und design, Netzmanagement, Firewall)
- Infrastruktur (z.B. allgemeines Gebäude, Büroarbeitsplatz, häuslicher Arbeitsplatz, mobiler Arbeitsplatz, technisches Gebäudemanagement)

Jedes dieser aktuell 10 Themengebiete ist in mehrere sogenannte Bausteine[3] aufgeteilt. Diese Bausteine enthalten wiederum jeweils eine Sammlung von möglichen Gefährdungen und diesen zugeordneten Sicherheitsanforderungen. Den Bausteinen des

[3] Aktuell umfasst das IT-Grundschutzkompendium 104 Bausteine.

Kompendiums sind zudem Umsetzungshinweise für die Implementierung einzelner Maßnahmen zur Erfüllung der Sicherheitsanforderungen zugeordnet. Der Prozess der jährlichen Aktualisierung bzw. Ergänzung der Bausteine beinhaltet die Möglichkeit zur Kommentierung der Entwürfe von Bausteinen durch Anwender, was zu einer möglichst großen Praxisnähe des Kompendiums beitragen soll.

Eine Zusammenfassung des Inhalts ist aufgrund des großen Umfangs des IT-Grundschutz-Kompendiums an dieser Stelle nicht möglich. Eine Vielzahl der Bausteine und der in diesen enthaltenen Sicherheitsanforderungen diente als wesentliche Informationsbasis bei der Erstellung des in Kap. 3 beschriebenen Kriterienkatalogs.

2.5.2 ENSRA/WENRA-Aktivitäten

Aufgrund der Corona-Situation während der Laufzeit dieses Vorhabens wurden die Workshops als Webkonferenzen durchgeführt, in denen nicht über vertrauliche Informationen gesprochen werden durfte. Eine inhaltliche Arbeit war daher nur in sehr begrenztem Umfang möglich. Es wurde jedoch über die verschiedenen Definitionen zur IT-Sicherheit diskutiert, die international verwendet werden. Die Ergebnisse dieser Diskussion sind in Kap. 2.1 eingeflossen.

2.5.3 IAEA NSS 17-T: IT-Sicherheit in nuklearen Einrichtungen

Schwachstellen von Computersystemen werden mit zunehmender Häufigkeit und Auswirkung böswillig ausgenutzt. Die zunehmende Bedrohung durch Cyberterrorismus zum Angriff auf kritische Infrastrukturen haben Behörden in verschiedenen Ländern dazu veranlasst, Abwehrmaßnahmen vorzubereiten und neue Vorschriften zu erlassen. Diese legen auch Anforderungen an die IT-Sicherheit fest. Der Standard NSS No. 17-T *„Computer Security at Nuclear Facilities“* /IAE 11/ der IAEA befasst sich daher mit den spezifischen Bedingungen, die die IT-Sicherheit in Kernkraftwerken beeinträchtigen können und stellt bestehende Leitlinien und Standards zur IT-Sicherheit sowie technische und administrative Leitlinien zur Umsetzung eines IT-Sicherheitsplans dar.

Ziele der IT-Sicherheit werden nach IAEA NSS No. 17-T als Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von elektronischen Daten oder Computersystemen und -prozessen verstanden (siehe hierzu auch Kap. 2.1.4.3) /IAE 11/.

Nach IAEA NSS No. 17-T sollte das staatliche Rechtssystem auch in Fragen der IT-Sicherheit einen gesetzlichen Rahmen schaffen, der den Schutz sensibler Daten abdeckt. Die IT-Sicherheit kann besondere Rechtsvorschriften erfordern, um den einzigartigen Verbrechen und der Funktionsweise von Computersystemen Rechnung zu tragen. Entsprechend sollte die Aufsichtsbehörde in ihren Leitlinien die einschlägigen Rechtsvorschriften berücksichtigen und den Betreibern Instrumente und Mittel zur korrekten Auslegung und Umsetzung rechtlicher Verpflichtungen zur Verfügung stellen /IAE 11/.

Alle Kernkraftwerke sollten über eine IT-Sicherheitsrichtlinie verfügen, die vom Geschäftsführer befürwortet und durchgesetzt wird. Diese Richtlinie legt die allgemeinen IT-Sicherheitsziele der Anlage fest und muss die entsprechenden behördlichen Anforderungen erfüllen. Die Anforderungen der IT-Sicherheitsrichtlinie sollten in Dokumenten auf niedrigerer Ebene berücksichtigt werden, die verwendet werden, um die Richtlinien zu implementieren und zu kontrollieren. Darüber hinaus muss die Richtlinie durchsetzbar, erreichbar und überprüfbar sein /IAE 11/.

Der Computersicherheitsplan (CSP) ist die Umsetzung dieser Richtlinie in Form von organisatorischen Rollen, Verantwortlichkeiten und Verfahren. Der Plan spezifiziert die Mittel zum Erreichen der IT-Sicherheitsziele in der Anlage. Der Plan sollte die wichtigsten Maßnahmen in Bezug auf die Anfälligkeit für Schwachstellen, Schutzmaßnahmen, Folgenanalyse und Minderungsmaßnahmen enthalten, um das akzeptable Cyberrisiko des Kernkraftwerks zu ermitteln und aufrechtzuerhalten und die Wiederherstellung eines sicheren Betriebszustands zu erleichtern /IAE 11/.

Managementsysteme werden in IAEA NSS No. 17-T als wesentliches unterstützendes Element einer nuklearen Sicherungskultur angesehen. Sie sind von Natur aus dynamisch und müssen sich an sich ändernde Randbedingungen stetig anpassen. Auch in Hinblick auf die IT-Sicherheit ist das Managementsystem zu ergänzen /IAE 11/.

Um angemessene Prozess- und Unterstützungsorganisationen in Hinblick auf die IT-Sicherheit einzurichten, hat die Geschäftsführung folgende Aufgaben /IAE 11/:

- Sie übernimmt die Gesamtverantwortung für alle Aspekte der IT-Sicherheit,
- Sie definiert die Sicherungsziele der Anlage,
- Sie stellen die Einhaltung von Gesetzen und Vorschriften sicher,
- Sie legen die Risikoakzeptanzstufe für die Anlage fest,
- Sie weisen organisatorische Verantwortlichkeiten für die IT-Sicherheit zu,

- Sie gewährleisten eine angemessene Kommunikation zwischen den verschiedenen Sicherungsaspekten
- Sie stellen sicher, dass eine durchsetzbare IT-Sicherheitsrichtlinie erstellt wird,
- Sie stellen angemessene Ressourcen für die Implementierung eines praktikablen IT-Sicherheitsprogramms bereit
- Sie stellen regelmäßige Audits und Aktualisierungen der IT-Sicherheitsrichtlinie sicher
- Sie stellen Unterstützung für Schulungs- und Sensibilisierungsprogramme sicher

Die verschiedenen Managementebenen innerhalb einer Organisation müssen in ihrem Verantwortungsbereich ein angemessenes Maß an Computersicherheit gewährleisten. Typische Aufgaben sind /IAE 11/:

- Betrieb gemäß den Richtlinien des IT-Sicherheitsplans des Standorts;
- Bereitstellung von betrieblichen Anforderungen und Rückmeldungen an den CSO (Computer Security Officer) in Bezug auf die IT-Sicherheit und Lösung potenzieller Konflikte zwischen Betriebs-, Sicherheits- und Sicherungsanforderungen;
- Benachrichtigen des CSO über alle Bedingungen, die zu Änderungen des IT-Sicherheitszustands führen können, wie Personaländerungen, Ausrüstungsänderungen oder Prozessänderungen;
- Gewährleistung, dass die Mitarbeiter ausreichend geschult und über IT-Sicherheitsfragen, die für ihre Rolle relevant sind, informiert sind;
- Gewährleistung, dass Subunternehmer und Drittanbieter, die für die Vertragseinheit arbeiten, im Rahmen des Standortsicherheitsplans arbeiten;
- Nachverfolgung, Überwachung und Meldung von sicherungsrelevanten Ereignissen;
- Durchsetzung von Personalsicherungsmaßnahmen.

Jede Person innerhalb einer Organisation ist nach /IAE 11/ für die Durchführung des IT-Sicherungsplans verantwortlich. Zu den spezifischen Verantwortlichkeiten gehören:

- Kenntnis über grundlegende IT-Sicherheitsverfahren;
- Kenntnis über berufsspezifische IT-Sicherheitsverfahren;
- Betrieb innerhalb der Parameter der IT-Sicherheitsrichtlinien;

- Benachrichtigen des Managements über alle Änderungen, die zu einer verringerten IT-Sicherheit führen können;
- Benachrichtigen des Managements über alle Vorfälle oder mögliche Vorfälle, die eine Gefährdung der IT-Sicherheit beinhalten;
- Regelmäßige Teilnahme an Erst- und Auffrischungs-Sicherungsschulungen.

Eine robuste IT-Sicherungskultur ist darüber hinaus nach /IAE 11/ ein wesentlicher Bestandteil eines effektiven Sicherungsplans. Für das Management ist es wichtig sicherzustellen, dass das Bewusstsein für IT-Sicherheit vollständig in die Sicherungskultur integriert ist. Die Merkmale der nuklearen Sicherungskultur sind die Überzeugungen, Einstellungen, Verhaltensweisen und Managementsysteme, deren Zusammenführung zu einem wirksamen Sicherungsprogramm führt. Die IT-Sicherungskultur ist nach /IAE 11/ eine Teilmenge der gesamten Sicherungskultur und basiert auf einer Anwendung der oben genannten Merkmale auf das Bewusstsein der IT-Sicherheit.

Die Erfahrung hat nach IAEA NSS No. 17-T gezeigt, dass die Mehrheit der IT-Sicherheitsvorfälle menschlicher Natur sind und die Sicherheit eines Computersystems weitgehend vom Verhalten seiner Benutzer abhängt. Die IT-Sicherungskultur wird durch eine Sammlung vieler Aktivitäten entwickelt, die darauf abzielen, das Personal zu informieren und das Bewusstsein für IT-Sicherheit zu erhöhen /IAE 11/.

Die Attribute der IT-Sicherungskultur sollten nach IAEA NSS No. 17-T regelmäßig gemessen, überprüft und kontinuierlich verbessert werden. Die folgenden Indikatoren können verwendet werden, um die IT-Sicherungskultur in einer Organisation zu bewerten /IAE 11/:

- Die Anforderungen an die IT-Sicherheit sind klar dokumentiert und werden von den Mitarbeitern gut verstanden.
- Es gibt klare und wirksame Prozesse und Protokolle für den Betrieb von Computersystemen innerhalb und außerhalb der Organisation.
- Die Mitarbeiter verstehen und wissen, wie wichtig es ist, die Kontrollen innerhalb des IT-Sicherheitsprogramms einzuhalten.
- Computersysteme werden gewartet, um sicherzustellen, dass sie sicher sind und gemäß den Grundsätzen und Verfahren der IT-Sicherheit betrieben werden.

- Das Management setzt sich voll und ganz für Sicherheitsinitiativen ein und unterstützt diese.

Darüber hinaus wird in /IAE 11/ ein starkes Schulungsprogramm als einer der Eckpfeiler einer IT-Sicherungskultur angesehen. Es ist von entscheidender Bedeutung, Mitarbeiter, Auftragnehmer und Drittanbieter über die Bedeutung der Einhaltung der Sicherungsverfahren und der Aufrechterhaltung der Sicherungskultur zu schulen. Das Sensibilisierungsprogramm sollte nach /IAE 11/ folgende Anforderungen beinhalten:

- Der erfolgreiche Abschluss einer IT-Sicherheitsschulung und/oder eines Sensibilisierungsprogramms sollte eine Voraussetzung für den Zugang zu Computersystemen sein. Die Schulung sollte dem Sicherheitsniveau des Systems und der erwarteten Rolle der Benutzer entsprechen.
- Personen mit wichtigen Sicherheitsaufgaben (z. B. CSO, Computersicherheitsteam, Projektmanager, IT-Administratoren) sollten erweiterte Schulungen/Qualifikationen angeboten werden.
- Die Schulung sollte für alle Mitarbeiter regelmäßig wiederholt werden, um neue Verfahren und aufkommende Bedrohungen einzubeziehen.
- Mitarbeiter sollten anerkennen, dass sie ihre Sicherungsverantwortung verstehen.
- Das Schulungsprogramm sollte Metriken zur Bewertung des Bewusstseins für IT-Sicherheit, der Schulungseffektivität und von Prozessen zur kontinuierlichen Verbesserung oder Umschulung umfassen.

Darüber hinaus geht IAEA NSS No. 17-T auf die Interaktion mit anderen Sicherungsbereichen ein. Der anlagenspezifische IT-Sicherheitsplan sollte in enger Absprache mit physischen Schutz-, Sicherheits-, Betriebs- und IT-Spezialisten entwickelt werden. Der CSP muss regelmäßig überprüft und aktualisiert werden, um Sicherheitsereignisse aus allen Sicherheitsbereichen und Betriebserfahrungen des Standortsicherheitssystems widerzuspiegeln /IAE 11/.

Der physische Sicherheitsplan und der CSP sollten sich ergänzen. Computergestützte Vermögenswerte unterliegen physischen Zugangskontrollanforderungen, und ebenso kann eine elektronische Kompromittierung zu einer Verschlechterung oder einem Verlust bestimmter physischer Schutzfunktionen führen. Angriffsszenarien können durchaus die Koordination sowohl eines elektronischen als auch eines physischen Angriffs beinhalten.

Die für den physischen Sicherheitsplan verantwortlichen Teams und des CSP sollten sich gegenseitig informieren und ihre Bemühungen koordinieren, um die Konsistenz der Pläne während des Entwicklungs- und Überprüfungsprozesses sicherzustellen.

Neben der Sensibilisierung und Schulung sind andere Sicherheitsaspekte, die normalerweise im Bereich der Personalsicherung behandelt werden, für die Einrichtung einer konsistenten IT-Sicherheit unerlässlich. Die notwendigen Vorkehrungen zur Festlegung eines angemessenen Niveaus von Sicherheitsüberprüfungen, Geheimhaltungsverpflichtungen und Kündigungsverfahren sowie zur Definition der erforderlichen beruflichen Kompetenzen sollten zwischen dem EDV- und dem Personalsicherungsmanagement abgestimmt werden. Insbesondere Mitarbeiter mit zentralen Sicherungsaufgaben (Systemadministratoren, Sicherungsteam) benötigen möglicherweise eine höhere Überprüfung /IAE 11/.

2.5.4 IAEA NSS 23-G: Nukleare Sicherung von Informationen

Der Standard NSS No. 23-G „*Security of Nuclear Information*“ /IAE 15/ der IAEA bietet Leitlinien zur Umsetzung des Grundsatzes der Vertraulichkeit und zu umfassenden Aspekten der Informationssicherheit. Dabei liegt der Fokus darauf, die Lücke zwischen Industriestandards und besonderen Konzepten und Betrachtungen für die nukleare Sicherung in Hinblick auf Informationssicherheit zu schließen.

Vertrauliche Informationen sollte nach IAEA NSS No. 23-G auf die Personen beschränkt sein, die für den Zugriff autorisiert sind, und auf die Umstände, für die sie benötigt werden. Die Regeln "wissen müssen" und "aufbewahren müssen" sind für die Sicherung sensibler Informationen von grundlegender Bedeutung. Für die Verwaltung und Kontrolle von Zugriffsrechten sollten diese Regeln maßgeblich sein /IAE 15/.

Informationssicherheit sollte im Kontext des gesamten Sicherheitsrahmens betrachtet und angewendet werden. Sie ist eng mit anderen Sicherungsbereichen wie dem physischen Schutz und dem Personenschutz verflochten /IAE 15/.

Für die Informationssicherheit muss eine Hierarchie (Staat, Organisation, Individuum) existieren. Der Staat muss Gesetze erlassen, es müssen Regulierungsbehörden existieren, Richtlinien müssen Anforderungen stellen und die Abläufe in einer Organisation müssen den Sicherheitsanforderungen entsprechen /IAE 15/.

Die Implementierung von Informationssicherheitsschemata und zugehörigen Kontrollen erfordert Ressourcen und Zeit. Es ist weder machbar noch wünschenswert, alle Informationen an einem Standort oder einer Einrichtung gleichermaßen zu sichern. Einige Informationen sind nicht sensibel und erfordern keine besonderen Sicherungsmaßnahmen. Sogar für vertrauliche Informationen können verschiedene Informationsobjekte unterschiedliche Sicherheitsniveaus benötigen. Daher ist es wichtig zu identifizieren, welche Informationen sensible Informationen sind und welches Sicherheitsniveau sie erfordern. Die zuständigen Behörden in jedem Staat sollten festlegen, welche Informationen über Kernmaterial, anderes radioaktives Material, zugehörige Einrichtungen und Aktivitäten sensible Informationen darstellen /IAE 15/.

Es sollte ein nationales Klassifizierungssystem eingerichtet und aufrechterhalten werden, um Informationen in Klassen zu gruppieren, sodass die unbefugte Offenlegung von Informationen innerhalb einer Klasse ähnliche Folgen hätte und daher alle Informationen in einer bestimmten Klasse ähnlichen Sicherheitsanforderungen unterliegen sollten. Dabei sollte es sich um ein nationales System handeln, das nicht spezifisch für eine bestimmte Branche oder von einer einzelnen Einrichtung entwickelt wurde /IAE 15/.

Jede Organisation sollte zudem eigene interne Richtlinien, Pläne und Verfahren zur Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit aller in ihrem Besitz befindlichen oder von ihr bearbeiteten sensiblen Informationen im Zusammenhang mit der nuklearen Sicherung festlegen. Alle Mitarbeiter sollten sich der Notwendigkeit der Informationssicherheit voll bewusst sein und die Regeln und Verfahren ihrer Organisation zur Informationssicherheit befolgen /IAE 15/.

Auf der Ebene der Organisation kann die Bedeutung bestimmter Informationen im Sicherheitsplan der Organisation angegeben werden, in dem beschrieben werden soll, wie bestimmte sensible Informationen in Übereinstimmung mit den nationalen Gesetzen und Vorschriften zu schützen sind /IAE 15/.

Unter anderem können folgende Punkte für die Identifizierung sensibler Informationen herangezogen werden /IAE 15/:

- Einzelheiten der physischen Schutzsysteme und aller anderen Sicherheitsmaßnahmen, die für Kernmaterial, anderes radioaktives Material, zugehörige Einrichtungen und Aktivitäten gelten, einschließlich Informationen über Wach- und Einsatzkräfte;

- Informationen über die Menge und Form von Kernmaterial oder anderem radioaktiven Material, das in Gebrauch ist oder gelagert wird, einschließlich Informationen über die Kernmaterialbuchhaltung;
- Informationen bezüglich der Menge und Form von Kernmaterial oder anderem radioaktiven Material beim Transport;
- Einzelheiten über Computersysteme, einschließlich Kommunikationssysteme, die direkt oder indirekt Informationen verarbeiten, handhaben, speichern oder übertragen, die für die Sicherheit wichtig sind;
- Notfall- und Reaktionspläne für Ereignisse im Bereich der nuklearen Sicherheit;
- Persönliche Informationen über Mitarbeiter, Lieferanten und Auftragnehmer;
- Bedrohungseinschätzungen und Informationen zu Sicherheitswarnungen;
- Einzelheiten über sensible Technologie;
- Einzelheiten über Schwachstellen oder Schwächen, die sich auf die oben genannten Themen beziehen;
- Historische Informationen zu einem der oben genannten Themen.

Der Austausch von sensiblen Informationen ist zulässig, auch auf Ad-hoc-Basis, muss jedoch unter besonderer Vorsicht geschehen damit die sensiblen Informationen nicht versehentlich für Unbefugte offengelegt werden. Die Regeln für die Weitergabe von Informationen zwischen Behörden, Organisationen oder dem Staat, sollte sich nach den Sicherheitsverfahren richten, die in dem betreffenden Staat gelten /IAE 15/.

Beim Informationsaustausch zwischen Staaten oder bei internationalen Organisationen kann ein sicherer Informationsaustausch durch bilaterale oder multilaterale Verträge oder durch bilaterale oder multilaterale Vereinbarungen gewährleistet werden /IAE 15/.

Die Offenlegung sensibler Informationen ist durch Gesetzeserlasse verboten. Es dürfen aber nicht alle Informationen zurückgehalten werden. So müssen bei Anforderung, Informationen ausgehändigt werden. Es gibt darüber hinaus sogar Gesetze, welche eine explizite Veröffentlichung bestimmter Informationen fordern. Es sollen auch Leitlinien für die Vorbereitung zu Offenlegung von Informationen existieren /IAE 15/.

Die Informationssicherheit sollte nach IAEA NSS No. 23-G in das bestehende Managementsystem der Anlage integriert werden, um die Vertraulichkeit, Integrität und

Verfügbarkeit von Informationen zu gewährleisten. Die Gewährleistung der Vertraulichkeit, Integrität und Verfügbarkeit sensibler Informationen hängt ab von /IAE 15/

- einer effektiven Zuweisung von Rollen und Verantwortlichkeiten,
- einer Klassifizierung, anhand dessen festgestellt werden kann, welche Informationen sensibel sind und gesichert werden müssen, warum und auf welcher Ebene sie gesichert werden müssen
- Entscheidungen, wie solche Informationen gesichert werden
- der Umsetzung der erforderlichen Sicherungsmaßnahmen
- der Reaktion, wenn Informationen kompromittiert, gestohlen oder verloren werden

Das Management trägt die Gesamtverantwortung dafür, dass die Informationssicherheit in der gesamten Anlage vorhanden und wirksam ist, um sensible Informationen zu schützen. Die Mitarbeiter, die mit sensiblen Informationen umgehen, sind dafür verantwortlich, deren Sicherung in Übereinstimmung mit den entsprechenden nationalen Gesetzen und Richtlinien sowie den Prozessen innerhalb der Organisation zu gewährleisten /IAE 15/.

Zu den Führungsaufgaben gehören nach /IAE 15/:

1. Übernahme der Gesamtverantwortung für die Sicherung sensibler Informationen und sensibler Informationsressourcen;
2. Sicherstellung der Einhaltung relevanter Gesetze und Vorschriften;
3. Zuweisung von organisatorischen Sicherheitsverantwortungen;
4. Bereitstellung einer effektiven Sicherheitsschulung und -ausbildung;
5. Sicherstellen, dass eine wirksame Informationssicherheitspolitik erstellt wird;
6. Bereitstellung angemessener Ressourcen zur Umsetzung eines wirksamen Informationssicherheitsprogramms;
7. Gewährleistung der Entwicklung des Informationssicherheitsprogramms und der zugehörigen Pläne und Verfahren;
8. Gewährleistung eines effektiven Änderungsmanagements in Bezug auf Pläne, Verfahren und Richtlinien;
9. Gewährleistung regelmäßiger Audits, Überprüfungen und Überarbeitungen von Richtlinien und Verfahren zur Informationssicherheit.

Als Teil einer wirksamen Sicherungskultur sollten alle Organisationen, Mitarbeiter und Auftragnehmer ihre Sicherheitsverantwortung und deren Bedeutung vollständig verstehen. Es ist von entscheidender Bedeutung, dass Mitarbeiter und Auftragnehmer Sicherheitsausbildung und -schulungen erhalten, die ihren individuellen Verantwortlichkeiten und Bedürfnissen entsprechen /IAE 15/.

Mitarbeiter und Auftragnehmer mit spezifischer Sicherungsverantwortung und Personen mit Zugang zu sensiblen Informationen sowie das Management auf allen Ebenen einer Organisation benötigen spezifische Schulungen und Einweisungen zu ihren Verantwortlichkeiten. Es ist auch wichtig sicherzustellen, dass andere Kategorien von Mitarbeitern (z. B. Boten, Sicherungspersonal und Sachbearbeiter), die mit sensiblen Informationen umgehen, ohne deren Inhalt unbedingt zu kennen, ebenfalls aufgabenspezifische Sicherungsschulungen erhalten /IAE 15/.

Einmalige Informationssicherheitsschulungen werden die Ausbildung nicht ausreichend verstärken und können langfristig dazu führen, dass Mitarbeiter selbstgefällig werden. Jeder, der mit sensiblen Informationen umgeht, einschließlich aller Führungskräfte, Mitarbeiter und Auftragnehmer, sollte kontinuierlich am Arbeitsplatz geschult und regelmäßig an Auffrischungskursen teilnehmen. Aufzeichnungen, über die von allen Mitarbeitern und Auftragnehmern erhaltenen und abgeschlossenen formalen Schulungen, sollten geführt werden. Es ist besonders wichtig, dass alle relevanten Mitarbeiter und Auftragnehmer so bald wie möglich über Änderungen der Sicherungsregeln und -verfahren informiert werden /IAE 15/.

2.5.5 Informationssicherheitskultur nach A. Martins, J. Elofe

In jeder Organisation entsteht nach A. Martins und J. Elofe /MAR 02/ eine Informationssicherheitskultur aus dem Umgang der Menschen mit Informationen und deren Sicherheit. Die Verfahren, die Mitarbeiter in ihrer täglichen Arbeit anwenden, könnten das schwächste Glied in der Informationssicherheitskette darstellen. Daher ist es wichtig, die Informationssicherheitskultur durch ein strukturiertes Modell zu entwickeln und zu verbessern, das sich mit dem Verhalten der Mitarbeiter befasst. In /MAR 02/ werden das Konzept der Informationssicherheitskultur und ein Bewertungsansatz erörtert, die entwickelt wurden, um eine solche Kultur zu implementieren und zu verbessern.

Nach /MAR 02/ reicht die Implementierung technischer Lösungen zur Informationssicherheit nicht aus. Die Wirksamkeit von Kontrollen zur Informationssicherheit hängt von

der Kompetenz und Zuverlässigkeit der Personen ab, die sie implementieren und verwenden. Wenn das Management und die Nutzer einer Firewall beispielsweise nicht wissen, wie man sie effektiv verwaltet oder bedient, stellt der menschliche Faktor das Risiko dar und nicht die Technologie selbst. Die Interaktion zwischen Menschen und Computertechnik stellt daher nach /MAR 02/ die größte Schwäche dar. Es ist daher wichtig, dass das richtige Verhalten in Bezug auf die Informationssicherheit Teil der Organisationskultur wird.

Einige Forscher haben nach /MAR 02/ darauf hingewiesen, dass Informationssicherheit als ganzheitliches Thema betrachtet werden sollte, das Teil der Organisationskultur ist. Es sollte Themen wie Menschen, Training, Prozesse und Kommunikation umfassen. Daher spielt die Organisationskultur eine wichtige Rolle bei der Umsetzung von Informationssicherheit als ganzheitliches Thema.

Die Organisationskultur ist nach /MAR 02/ für jede Organisation anders, jede hat ihre eigenen Eigenschaften, die sie schätzt, wie z. B. die Arbeit in Teams statt als Einzelpersonen. Jede Organisation hat auch bestimmte Informationssicherheitspraktiken. Ein Beispiel ist die wöchentliche Änderung von Passwörtern oder die Beauftragung eines Wirtschaftsprüfers mit der Bewertung der Computernetzwerke der Organisation.

Demnach kann nach /MAR 02/ die Informationssicherheitskultur als eine Reihe von Informationssicherheitsmerkmalen angesehen werden. Diese Eigenschaften, wie Integrität und Verfügbarkeit von Informationen, müssen von der Organisation geschätzt und verfolgt werden. Die Informationssicherheitskultur ist auch eine Annahme darüber, was in Bezug auf Informationssicherheit akzeptabel ist und was nicht. Es kann beispielsweise nicht akzeptabel sein, ein vertrauliches Dokument in einen Papierkorb zu werfen, sondern es eher zu schreddern. Ein weiteres Beispiel ist, dass es nicht akzeptabel ist, wichtige Geschäftsinformationen in Bürobereichen zu hinterlassen, wo jeder darauf zugreifen oder sie lesen könnte; es sollte lieber weggeschlossen werden.

Eine gute Informationssicherheitskultur entsteht nach /MAR 02/ u. a. durch die Förderung eines akzeptablen Verhaltens in Hinblick auf Informationssicherheit. Menschen könnten z. B. ermutigt werden, Sicherheitsvorfälle über entsprechende Managementkanäle zu melden. Das Management könnte die Mitarbeiter ermutigen, ihre Arbeit als Teil des geistigen Eigentums der Organisation zu betrachten, das geschützt werden muss. Informationssicherheitskultur kann somit über die Art und Weise, wie Informationssicher-

heitsmerkmale in der Organisation integriert werden und darüber, welches Informationssicherheitsverhalten akzeptiert und gefördert wird, definiert werden.

Zur Einführung einer Informationssicherheitskultur müssen nach /MAR 02/ Themen wie Informationssicherheitsrichtlinien und Informationssicherheitsbewusstsein angegangen werden. Kultur hat mit der Art und Weise zu tun, wie Dinge in einer Organisation erledigt werden, und damit mit dem Verhalten von Menschen. Daher hat auch Organisationsverhalten Auswirkungen auf die Informationssicherheitskultur einer Organisation. Organisationsverhalten konzentriert sich nach /MAR 02/ auf drei unterschiedliche Ebenen, nämlich die Individual-, Gruppen- und Organisationsebene. Die Auswirkungen der Informationssicherheit auf diese drei Ebenen müssen berücksichtigt werden, wenn eine Organisation ihren Mitarbeitern ein akzeptables Informationssicherheitsverhalten vermitteln möchte. Abb. 2.4 zeigt die drei Ebenen des Organisationsverhaltens nach /MAR 02/.

Auf individueller Ebene könnten Mitarbeiter ermutigt werden, Informationssicherheitsvorfälle zu melden. Die Unterstützung des Managements bei Informationssicherheitsprozessen könnte auch auf Gruppenebene gefördert werden. Ein Beispiel für ein solches Verhalten auf Organisationsebene könnte sein, dass eine Informationssicherheitsrichtlinie implementiert werden muss.

Einzelpersonen müssen auch an Schulungen und Sensibilisierungssitzungen teilnehmen, um sie in die Lage zu versetzen, die Prozesse umzusetzen. Dies wird einen Einfluss auf die Art und Weise haben, wie sich Menschen in Bezug auf die Sicherung von Informationswerten in der Organisation verhalten.

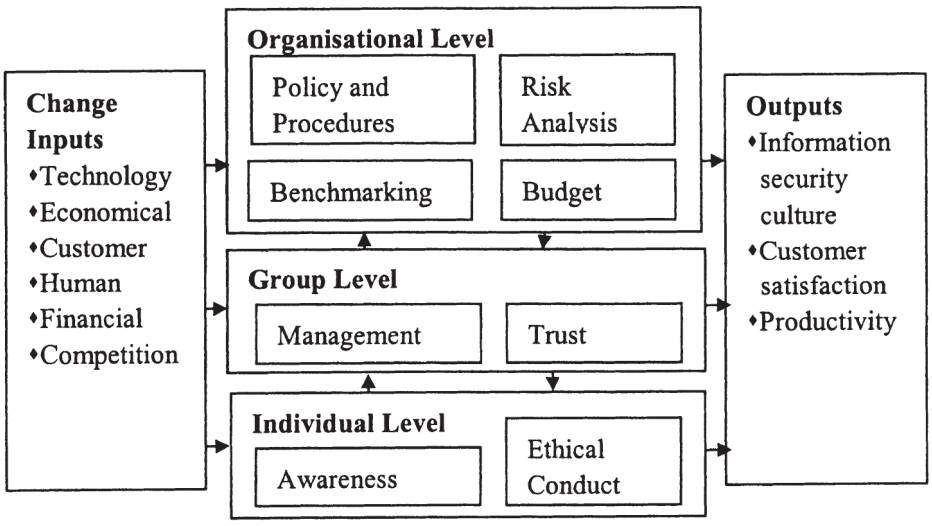

Abb. 2.4 Ebenen der Informationssicherheitskultur nach /MAR 02/

Organisationsebene

Alle Prozesse und Strukturen beginnen auf organisatorischer Ebene. Auf diese Ebene müssen

- Prozesse wie Risikobewertung und Verfahren zur Meldung von Sicherheitsvorfällen entwickelt werden.
- Strukturen für Informationssicherheitsprozesse durch Richtlinien eingerichtet werden, die das Layout und den Rahmen für die Implementierung der Prozesse bereitstellen.
- Richtlinien zum Mitarbeiterverhalten zusammengestellt werden, z. B. darüber was akzeptabel ist und was nicht.

Die Informationssicherheitsrichtlinie schreibt das Verhalten der Mitarbeiter vor und legt fest, was von den Mitarbeitern erwartet wird. Damit sich die Mitarbeiter den Erwartungen entsprechend verhalten, müssen sie sensibilisiert, aufgeklärt und geschult werden.

Durch die Risikoanalyse können Vermögenswerte der Organisation, Bedrohungen für sie und Sicherheitsmaßnahmen identifiziert werden, um die Informationssicherheitsrichtlinie zu entwickeln. Mitarbeiter müssen die Risikoanalyse als akzeptierte Aktivität und Teil des täglichen Lebens in der Organisation wahrnehmen, um sie als Teil der Informationssicherheitskultur zu integrieren.

Zur Umsetzung der Themen einer Informationssicherheitskultur ist ein Finanzplan notwendig. Beispielsweise müssen Mitarbeiter geschult, technische Kontrollen implementiert und Teams in die Lage versetzt werden, die Sicherheit von Netzwerken zu bewerten. Ausgaben für die umzusetzenden Themen, z. B. die Erstellung einer Informationssicherheitsrichtlinie, müssen als alltägliche Tätigkeit akzeptiert werden.

Gruppenebene

Richtlinien haben keine Bedeutung, wenn das Management sein Engagement und seine Beteiligung an ihnen nicht sicherstellt. Das Management muss seine Unterstützung gewährleisten und ein Umfeld des Vertrauens in der Organisation schaffen, um die Themen auf Organisationsebene umzusetzen.

Verantwortlich für die Informationssicherheit ist die Geschäftsleitung. Das Management entwickelt die Visionen und Strategien einer Organisation, die zum Schutz von Informationswerten erforderlich sind und in der Organisation implementiert werden.

Menschen verhalten sich auf eine bestimmte Weise, geleitet von der Philosophie und Strategie, die sie verfolgen, um den Schutz von Informationswerten zu gewährleisten. Daher muss das Management das richtige Verhalten modellieren.

Wenn das Management seinen Mitarbeitern vertraut und die Mitarbeiter dem Management vertrauen, ist es einfacher, neue Verfahren zu implementieren und Mitarbeiter durch Verhaltensänderungen in Bezug auf die Informationssicherheit zu führen. Die Wahrnehmung der Mitarbeiter und das Vertrauensverhältnis zwischen Managern und Mitarbeitern muss gut sein und sollten als eines der Merkmale der Organisation angesehen werden, das zur Einführung einer Informationssicherheitskultur beiträgt.

Individuelle Ebene

Einzelne Mitarbeiter in einer Organisation haben jeweils ihre eigenen Einstellungen, die zu bestimmten Verhaltensweisen führen. Sie müssen sich der Prozesse bewusst sein, die auf Organisationsebene definiert wurden, um sich entsprechend zu verhalten, da ihr Verhalten den Erfolg der Angelegenheiten auf Organisations- und Gruppenebene bestimmen. Aber wenn sie nicht geführt und für die Probleme sensibilisiert werden, werden sie nicht in der Lage sein, entsprechend zu handeln, selbst wenn sie dazu auf individueller Ebene bereit wären.

Da die Wirksamkeit von Informationssicherheitskontrollen von den Personen abhängt, die sie implementieren und verwenden, müssen Mitarbeiter durch Sensibilisierung und Schulung dazu befähigt werden, sich gemäß den Erwartungen an sie zu verhalten, um die Sicherheit von Informationsressourcen zu gewährleisten. Erstrebenswert ist eine Informationssicherheitskultur, in der Mitarbeiter befähigt und ausgerüstet werden, sich so zu verhalten, dass sie keine Bedrohung für die Sicherheit von Informationswerten in der Organisation darstellen.

Gute Praktiken werden in einer Organisation nicht durch Vorschriften, Anreize und Überwachung erreicht. Sie müssen vielmehr Teil der Kultur sein, die in der gesamten Organisation etabliert ist. Daher müssen Mitarbeiter ethisches Verhalten in Bezug auf Informationssicherheit in ihren Alltag in der Organisation integrieren. Ethisches Verhalten,

z.B. Informationen der Organisation nicht zu Hause zu kopieren oder das Internet nicht zur persönlichen Bereicherung während der Arbeitszeit zu nutzen, muss als akzeptierte Verhaltensweise im Arbeitsumfeld durchgesetzt werden, damit sich rechtzeitig die richtige Informationssicherheitskultur herausbildet.

Veränderungen in der Informationssicherheit müssen positiv aufgenommen und so gemanagt werden, dass die Mitarbeiter die Veränderungen in ihr Arbeitsumfeld integrieren können. Die akzeptierten Änderungen werden dann mit der Zeit Teil der Informationssicherheitskultur.

2.5.6 Soziokulturelle Dimension der Informationssicherheitskultur

T. Schlinger diskutiert in „*Information Security Culture: The Socio-Cultural Dimension in Information Security Management*“ /SCH 02/, dass das Informationssicherheitsmanagement meist das Hauptaugenmerk auf technische und verfahrenstechnische Maßnahmen legt und die menschliche Dimension außer Acht lässt. Der Benutzer wird dabei als Sicherheitsfeind und nicht als Sicherheitsfaktor angesehen. T. Schlinger schlägt diesbezüglich einen Paradigmenwechsel von einem technischen zu einem menschenzentrierten Fokus vor. In /SCH 02/ werden einige Aspekte diskutiert, die nach Ansicht der Autoren helfen können, ein Sicherheitsmanagement aufzubauen, das auch die menschliche Dimension berücksichtigt.

Nach /SCH 02/ kommen zwei verschiedene Studien zu dem Schluss, dass rund die Hälfte der in den Studien untersuchten Sicherheitsvorfälle von Insidern begangen wurden. Sicherheitsmaßnahmen, die sich an diese Gruppe richten, sollten daher helfen, die interne Täterzahl zu verringern. An erster Stelle sollten potenzielle Mitarbeiter gründlich geprüft werden, bei gleichzeitiger Berücksichtigung der individuellen Privatsphäre und des Datenschutzrechts. Zweitens müssen die eingestellten Personen geschult und ermutigt werden, sich korrekt zu verhalten und so die organisatorische Informationssicherheit zu unterstützen. Darüber hinaus helfen hochmotivierte und qualifizierte Mitarbeiter auch dabei, externe Bedrohungen wie E-Mail-Viren und -Würmer zu verringern.

Nach /SCH 02/ waren sich Sicherheitsspezialisten in den letzten Jahren darüber einig, dass Sicherheitsmanagement nur dann erfolgreich sein kann, wenn es in eine Organisations- und Führungsstruktur innerhalb der Organisation eingebettet ist.

Eine herkömmliche Methode zum Schutz von Informationssystemen ist die Verwendung von Passwörtern. Gemäß /SCH 02/ verwenden 91 % aller Systeme Passwörter, obwohl es alternative Techniken gibt, die sicherer und auch benutzerfreundlicher sind. Rund 38 % der Nutzer müssen sich für ihre tägliche Arbeit vier oder mehr Passwörter merken. Etwa 46 % der Benutzer müssen ihre Passwörter mindestens alle sechs Monate ändern.

Die Einführung neuer Sicherheitsprodukte und -verfahren kann nach /SCH 02/ nur erfolgreich sein, wenn erstens die Anwender das Warum und das Wie verstehen und zweitens die Anwender motiviert werden können, einen solchen Wandel mitzutragen.

Die Unternehmenskultur ist nach /SCH 02/ ein kollektives Phänomen, das im Laufe der Zeit wächst, sich verändert und von der Führung der Organisation beeinflusst oder sogar gestaltet werden kann. Die Kernsubstanzen der Unternehmenskultur sind Grundannahmen und Überzeugungen. Diese Annahmen betreffen die Natur der Menschen, ihr Verhalten und ihre Beziehung. Die Unternehmenskultur drückt sich folglich in den kollektiven Werten, Normen und dem Wissen von Organisationen aus. Diese kollektiven Normen und Werte wiederum wirken sich auf das Verhalten der Mitarbeiter aus. Sie werden in Form von Artefakten und Kreationen wie Handbüchern, Ritualen und Anekdoten ausgedrückt. Unternehmenskultur entsteht und wächst mit der Zeit. Es wird durch das Verhalten dominanter Organisationsmitglieder wie Gründer und Top-Manager geformt.

Die Unternehmenskultur sollte nach /SCH 02/ alle Aktivitäten so unterstützen, dass Informationssicherheit zu einem selbstverständlichen Aspekt im täglichen Handeln jedes Mitarbeiters wird. Die Informationssicherheitskultur konzentriert sich auf die soziokulturellen Aspekte des Informationssicherheitsmanagements.

Auf unternehmenspolitischer Ebene sollte Informationssicherheit als Unternehmensziel definiert werden. Das bedeutet, dass das Top-Management für die Definition der Sicherheitspolitik verantwortlich ist. Folglich müssen sie ausreichende Ressourcen bereitstellen, um diese Politik umzusetzen. Diese Aufgabe könnte delegiert werden, z.B. an einen Chief Security Officer, aber das Top-Management als Ganzes bleibt verantwortlich.

Für die Einhaltung der Informationssicherheitspolitik und für die Umsetzung in ihren Einheiten sind die jeweiligen Abteilungsleiter zuständig. Sie müssen ausreichend motiviert sein, die Sicherheitspolitik einzuhalten. Um die Sicherheitsrichtlinie umzusetzen, muss das Management die verschiedenen Sicherheitsmaßnahmen definieren und kontrollieren. Zusätzlich müssen sie sich qualifizieren und ihre Mitarbeiter schulen. Sicherheits-

konformes Verhalten muss belohnt, böswillige Sicherheitsverletzungen verfolgt werden. Außerdem muss die Sicherheitsstrategie regelmäßig überprüft und einem Benchmarking unterzogen werden.

Auf der individuellen Ebene muss jeder Mitarbeiter selbst zur Sicherheit der Organisation beitragen. Er/sie muss eine kritische Haltung einnehmen, indem er/sie fragt:

- Habe ich meine Aufgabe verstanden?
- Was sind meine Aufgaben?
- In welcher Beziehung stehen sie zur Informationssicherheit?
- Verfüge ich über ausreichende Kenntnisse, um meine Aufgabe zu erfüllen?
- Brauche ich Hilfe?

Er hat sorgfältig und mit der gebotenen Sorgfalt zu handeln. Abnormales Verhalten von Personen oder Computersystemen einschließlich Fehlfunktionen müssen registriert und gemeldet werden. Weiterhin muss der Nutzer in den Prozess der Risikoanalyse eingebunden werden und das Unternehmen sollte ein betriebliches Vorschlagswesen installieren. In Bezug auf die Sicherheitskultur sind die wichtigsten Punkte:

- Das vorbildliche Verhalten der Führungskräfte
- Sicherheitsschulung der Mitarbeiter, dazu gehört die Sensibilisierung für die Risiken der Informationstechnologie und die Schulung im Umgang mit Sicherheitsprodukten
- Auszeichnung von sicherheitskonformem Verhalten

Es ist wichtig zu beachten, dass sicherheitskonformes Verhalten auch das Begehen und Eingeständnis von Sicherheitsverletzungen beinhalten kann. Die Information des Managements über Fehler kann der Organisation helfen, das Sicherheitsverhalten zu verbessern, indem die möglichen Risiken und Fehler besser verstanden werden. Nur böswilliges Verhalten sollte strafrechtlich verfolgt werden.

2.5.7 Informationssicherheitskultur: Von der Analyse zur Veränderung

Die Informationssicherheitskultur kann nach T. Schlinger /SCH 03/ ebenso wie die Unternehmenskultur nicht einmal erstellt und dann ohne weitere Maßnahmen oder Änderungen endgültig verwendet werden. Um sicherzustellen, dass sie mit den Zielen der Organisation übereinstimmt und die Organisationsmitglieder dies nicht vergessen, muss Kultur kontinuierlich geschaffen, gepflegt oder verändert werden. Es ist ein nie endender

Prozess, ein Kreislauf von Evaluation und Veränderung bzw. Pflege. Der erste Schritt ist die Analyse der aktuellen Informationssicherheitskultur (Pre-Evaluation). Wenn die Kultur nicht zu den Zielen der Organisation passt, muss die Kultur geändert werden. Wenn es passt, sollte es verstärkt werden. Anschließend muss der Erfolg der getroffenen Maßnahmen kontrolliert werden (Post-Evaluation).

Damit die Sicherheitskultur einen substanziellen Beitrag zum Bereich der Informationssicherheit leisten kann, ist es notwendig, eine Reihe von Methoden für ihre Untersuchung zu haben. Leider gibt es kein einzigartiges Instrumentarium und keine Methode zur Untersuchung der Organisations- und damit der Sicherheitskultur. Auf diesem Gebiet besteht also noch Forschungsbedarf. Der Forscher muss nach /SCH 03/ zwei Hauptfragen lösen:

1. Was ist zu analysieren? Je nach verwendetem Kulturmodell könnte man die kollektiven Werte, Normen und das Wissen messen, oder man könnte die kulturellen Indikatoren, die Artefakte, messen. Werte können offiziell angegeben werden, aber stimmen sie dann mit den wirklichen – bewussten oder unbewussten – Werten überein? Werte mit negativen gesellschaftlichen Sanktionen werden dabei nicht aufgedeckt, sondern bewusst ausgeblendet. /SCH 03/ unterscheidet daher zwischen offiziellen und wahren Werten.

2. Wie ist zu analysieren? Für die Messung beobachtbarer Indikatoren schlagen die Sozialwissenschaften oft vor, Dokumente zu analysieren, physische Indikatoren zu beobachten und die Mitglieder einer Organisation zu befragen. Für die Messung von Normen, Werten und Überzeugungen wird vorgeschlagen, narrative Interviews, teilnehmende Beobachtungen und Gruppensitzungen zu verwenden.

In Anbetracht der Schwierigkeiten, Kultur überhaupt zu erfassen, liegt der Einsatz einer Kombination von Messgrößen und -methoden nahe. Dies ermöglicht die Überprüfung der Ergebnisse mit anderen Methoden und die Verwendung verschiedener Sichtweisen bei der Interpretation. Der Forscher ist nun in der Lage, die geeigneten Methoden auszuwählen, die ihm helfen, die Sicherheitskultur in seiner Organisation zu bewerten.

Es müssen klare Ziele für die Entwicklung einer angemessenen Sicherheitskultur gesetzt werden. In /SCH 03/ wird die angestrebte Sicherheitskultur durch die Sicherheitsrichtlinie definiert. Es ist ein übergeordnetes Dokument für alle Maßnahmen zur Informationssicherheit und definiert die Grundlagen für Sicherheitsverhalten. Die Definition einer Zielkultur basiert nicht auf einem klaren Top-Down-Ansatz. Eine Sicherheitspolitik sollte

nicht unabhängig vom wirklichen Leben entwickelt werden. Es kommt auf die tatsächliche Unternehmenskultur und die manifestierten Arbeitsprozesse an. Eine Vorabbewertung kann die Notwendigkeit aufzeigen, zuerst die Sicherheitsrichtlinie neu zu gestalten.

Um die richtigen kulturellen Maßnahmen definieren zu können, ist es wichtig zu wissen, welche Personen man beeinflussen möchte. Ein weit verbreiteter Ansatz besteht darin, drei Gruppen zu definieren: IT-Personal, Führungskräfte und Mitarbeiter, und für jede einzelne spezielle Maßnahmen umzusetzen. Nach /SCH 03/ zeigten sich bei der Gruppierung nach Funktion (IT vs. Business) oder Position (Mitarbeiter vs. Führungskraft) statistisch signifikante Unterschiede, die auf die Notwendigkeit hindeuten, spezielle Kulturmaßnahmen für bestimmte Abteilungen oder Führungsebenen zu definieren.

Durch den Abgleich der Ist- mit der Soll-Sicherheitskultur lassen sich die richtigen Instrumente zur Umsetzung der Soll-Kultur auswählen. Kultur lässt sich nicht durch Vorschriften verordnen; subtilere Aktionen sind möglich und notwendig. Auf der Grundlage von interner Kommunikation, Schulung, Ausbildung und vorbildlichem Handeln von Führungskräften kann Schritt für Schritt eine Kultur entwickelt werden. Ziel der Kulturmaßnahmen ist es, das Sicherheitsbewusstsein bei Führungskräften und Mitarbeitern zu fördern. Gesteigertes Bewusstsein schafft und unterstützt eine gute Sicherheitskultur.

Die interne Kommunikation hat sowohl Informationsfunktion (führen, koordinieren und orientieren) als auch Dialogfunktion (Orientierung und Kontaktaufnahme). Außerdem lassen sich zwei Hauptformen der internen Kommunikation ausmachen, die zwischenmenschliche Kommunikation (Gespräche zwischen Arbeitnehmer und Arbeitgeber, Seminare, Schulungen und Workshops) und die Kommunikation über Medien (Unternehmenszeitung, Intranet, Leitfäden und Schwarzes Brett). Ein gutes Kulturprogramm braucht die richtige Mischung an Kommunikationsinstrumenten.

Schulungen sind eines der Kernelemente, um ein Sicherheitsbewusstsein zu schaffen. Es ist wichtig, Sicherheitsrichtlinien umzusetzen. Der Chief Security Officer ist verantwortlich für die Entwicklung des geeigneten Schulungsprogramms und/oder die Implementierung von Sicherheitselementen in das bestehende IT-Schulungsprogramm. Ein Sicherheitsschulungs- und Sensibilisierungsprogramm kann in drei verschiedene Teile unterteilt werden:

- Bildung: Der Mitarbeiter muss verstehen, warum Informationssicherheit für die Organisation wichtig ist. Er/sie muss verstehen, dass jeder in seinem/ihrem

Einflussbereich für die Sicherheit verantwortlich ist. Die Ausbildung kann z.B. mit einem speziellen Informationssicherheitskurs umgesetzt werden. Es kann auch eine grundlegende Informationssicherheitsausbildung in Schulen und Universitäten sein.

- Schulung: Der Mitarbeiter muss wissen, wie er sicher operieren kann. Er/sie muss wissen, wie er/sie die Sicherheitsfunktionen innerhalb der Anwendungen und in seinem/ihrem eigenen Arbeitsprozess nutzt. Schulungen zu speziellen Sicherheitstools oder Funktionen innerhalb von Anwendungen müssen angeboten werden.

- Bewusstsein: Aus- und Weiterbildung sind die Grundlage für Sicherheitsprogramme. Sie garantieren jedoch kein konformes Sicherheitsverhalten im Arbeitsalltag. Awareness-Maßnahmen außerhalb des Seminarraums erinnern die Mitarbeiter an das Gelernte. Artikel wie Poster, Mousepads und Stifte mit Sicherheitsslogans tragen dazu bei, das Thema Sicherheit allgegenwärtig zu machen. Anreiz- und Vorschlagssysteme regen die Mitarbeiter zur Teilnahme an. Kontrollen, Regeln und Sanktionen zeigen die Bedeutung der Informationssicherheit.

2.5.8 Messung der Wirksamkeit eines Schulungs- und Sensibilisierungsprogramms zur Informationssicherheit

In /DHA 18/ diskutiert R. Dhakal, dass die Informationssicherheitspolitik in den meisten Organisationen für die Endnutzer nicht ohne weiteres zugänglich ist, was wissentlich oder unwissentlich zu menschlichen Fehlern führt. Viele Organisationen gehen davon aus, dass der Mensch das schwächste Glied und anfällig für Verletzungen der Informationssicherheit ist. In /DHA 18/ wurde daher untersucht, wie Nutzer über die Informationssicherheitspolitik aufgeklärt, geschult und sensibilisiert werden können, wie Risiken identifiziert, Sicherheitsvorfälle über ein Schulungs- und Sensibilisierungsprogramm gemeldet werden können und wie die Wirksamkeit der Maßnahmen gemessen werden kann.

Viele Forscher sind der Ansicht, dass technische Gegenmaßnahmen für die vollständige Informationssicherheit einer Organisation nicht ausreichen, und glauben, dass mehr als die Hälfte (50-75 %) der Informationssicherheitsmängel einer Organisation durch Fahrlässigkeit der Mitarbeiter entstehen. Daher erfordern Investitionen in die Informationssicherheit eines Unternehmens sowohl technische als auch personelle Gegenmaßnahmen. Programme zur Sicherheitserziehung, -ausbildung und -bewusstsein (SETA – Security, Education, Training, Awareness) sind als die bestmögliche Lösung für

Informationssicherheitsverhalten bekannt, da sie eine wichtige Rolle in der Leistungsstrategie der Mitarbeiter spielen /DHA 18/.

Der Hauptzweck der Informationssicherheits-Ausbildung, -Schulung und -Bewusstseinsbildung besteht darin, die Mitarbeiter für die Informationssicherheitspolitik (ISP – Information Security Policy) und die Verfahren der Organisation zu sensibilisieren und sie zu einem sicheren und verantwortungsvollen Umgang mit dem Informationssicherheitssystem der Organisation zu befähigen. Wenn sich die Mitarbeiter der ISP bewusst sind, werden sie die Risiken und Bedrohungen der Organisation kennen und verstehen, und sie werden auch hart daran arbeiten, das Informationssicherheitssystem der Organisation zu erhalten /DHA 18/.

Nach /DHA 18/ haben viele Forscher unterschiedliche Ansichten über die Definition der Informationssicherheitskultur und es gibt keine spezifische Abgrenzung dieser Kultur:

- Dhillon definiert Informationssicherheitskultur als ein Beispiel für die gesamte Leistung innerhalb einer Organisation, die für den Schutz von Informationen verantwortlich ist.
- Schlienger und Teufel definieren Informationssicherheitskultur als die gesamte soziale und kulturelle Einstellung zur Praxis, die den technologischen Handlungsmodus aufrechterhält, so dass Informationssicherheit ein integraler Bestandteil der täglichen Handlungen des Benutzers wird. Sie argumentieren, dass die Informationssicherheitskultur einer Organisation alle Gemeinschaften und Traditionen umfassen sollte, die ihre Informationssicherheits-Methoden technisch unterstützen. Dies führt dazu, dass die organisatorische Informationsgesellschaft ein integraler Bestandteil der täglichen Aktivitäten aller Mitarbeiter ist. Die Kultur der Informationsgesellschaft in einer Organisation spielt eine wichtige Rolle bei der Verbesserung des Vertrauens zwischen den Mitarbeitern.
- Sasse, Brostoff, und Weirich klassifizieren und assoziieren die Hauptmerkmale der Informationssicherheitskultur in einer Organisation, wie z. B. geschäftliche Auswirkungen, Belohnung und Bestrafung und Bewusstsein, während sie für die Einführung einer angstbasierten Methode plädieren, um die Nutzer davon zu überzeugen, sich an die Informationssicherheitsmaßnahmen zu halten.
- Adams und Blandford machen deutlich, dass die Informationssicherheitskultur einer Organisation die Geschäftspolitik des Unternehmens in Kombination mit einem allgemeinen Betriebsplan unterstützen muss. Außerdem weisen sie darauf hin, dass

die Nutzer durch die Einführung eines Schulungs- und Sensibilisierungsprogramms für die Problematik sensibilisiert werden sollten. Sie erörtern ferner die Bedeutung eines bewussten Managements, da die Informationssicherheitskultur und ein Informationssicherheitsschulungs- und Sensibilisierungsprogramm ohne die volle Unterstützung der Organisationsleitung nicht erfolgreich sein würden.

- Thomson, von Solms und Louw stellen fest, dass die Unternehmenskultur die Informationssicherheitskultur inspiriert und dass das Management und die Nutzer einen gleichwertigen Einfluss haben. Der Erwerb von Wissen und Reife ist von entscheidender Bedeutung, um das Bewusstsein der Nutzer für die Belange der Informationsgesellschaft zu schärfen und sie zu ermutigen, an den sozialen Aktivitäten der Organisation teilzunehmen, damit sie durch das Beobachten anderer lernen können.

- Ruighaver, Maynard und Chang argumentieren, dass die Messung der Leistung der Informationssicherheitskultur nicht von der gesamten Organisationskultur abgekoppelt werden kann, da diese einen massiven Einfluss auf die Informationssicherheitskultur hat.

- Whiteman und Mattord argumentieren, dass sich die Einstellungen der Mitarbeiter aus verschiedenen Kulturen und Hintergründen auf die Informationssicherheitskultur einer Organisation auswirken, wobei die Ausbildung zusammen mit der Schulung und der Sensibilisierung für den Aufbau der Informationssicherheitskultur einer Organisation erhebliche Veränderungen bewirkt. Darüber hinaus erklären sie, dass Unwissenheit, Unfälle und absichtliche Handlungen die Informationssicherheitskultur einer Organisation beeinflussen können. Unwissenheit und Unfälle könnten durch Bewusstseinsbildung und Schulungen minimiert werden. Die absichtliche Handlung ist schwer zu steuern, kann aber durch die Schulung der Benutzer verringert werden. Die Durchführung neuer Aktivitäten, wie z. B. Belohnungen, zusammen mit einem Schulungs- und Sensibilisierungsprogramm, das die Gedanken von negativem zu positivem Denken umlenken könnte, sowie geeignete Informationssicherheits-Richtlinien und -verfahren können helfen.

Informationssicherheitsrichtlinie

Die ISP (information security policy) ist nach /DHA 18/ eine Gruppe von Plänen der Organisation, die veröffentlicht wurden, um sicherzustellen, dass alle Benutzer die Regeln und Vorschriften befolgen. Der Hauptzweck einer ISP besteht darin, sicherzustellen, dass geeignete Methoden vorhanden sind, um die Geschäftsprozesse und das

IT-System der Organisation zu schützen. Demnach handelt es sich beim ISP um ein formales Dokument der Organisation, das festlegt, wie sie ihre physischen, rationalen und technischen Vermögenswerte schützen kann. Zu den physischen Vermögenswerten gehören beispielsweise alle elektronischen Geräte und die Räumlichkeiten der Organisation, zu den rationalen Vermögenswerten gehören geistiges Eigentum und vertrauliche Dokumente, und zu den technischen Vermögenswerten gehören Firewalls, Einbruchmeldeanlagen, Virenschutz und Server. Beim ISP handelt es sich um ein Dokument, das nie endet und kontinuierlich aktualisiert werden muss, wenn sich die Technologie und die organisatorischen Ziele ändern. Damit dient sie auch zur Aufrechterhaltung von Standards innerhalb der Organisation. Gleichzeitig stellt das ISP ein Handbuch mit detaillierten Informationen darüber dar, was Mitarbeiter tun und lassen sollten. Es beschreibt außerdem, wie Nutzer über den Schutz von Verwaltungsressourcen unterrichtet und Informationssicherheits-Verfahren angewendet und ausgeführt werden. Sie soll Nutzer in die Lage versetzen, potenzielle geschäftliche Bedrohungen und Informationssicherheits-Risiken zu erkennen und sie zu mindern /DHA 18/.

Für die Entwicklung der ISP sind die Manager und Sicherheitsmanager einer Organisation verantwortlich. Vor der Erstellung einer ISP müssen sich die Manager mit Endnutzern und Managern aus verschiedenen Bereichen beraten und die von den jeweiligen Abteilungen ermittelten Risiken einbeziehen. Nach ihrer Fertigstellung muss sie allen Nutzern ausgehändigt werden. Außerdem müssen sie sicherstellen, dass die Nutzer die Richtlinie verstehen, sie an ihrem Arbeitsplatz umsetzen und ihren Erfolg messen. Hierzu soll sie u.a. im Schulungs- und Sensibilisierungsprogramm zur Informationssicherheit eingebunden werden /DHA 18/.

Bewusstsein für Informationssicherheit

ISA (Information Security Awareness) ist ein offizielles Organisationsprogramm, mit dem sichergestellt werden soll, dass die Organisationsleitung und die Benutzer sich der Minimierung von Informationssicherheits-Bedrohungen und -Risiken bewusst sind und sich an die ISP halten. ISA wäre erfolglos, wenn die Nutzer die organisatorische ISP zwar kennen, aber nicht gemäß den Richtlinien und Verfahren handeln. Nach /DHA 18/ ist die ISA demnach ein entscheidender Faktor bei der Verhinderung des Missbrauchs von Informationssystemen. Die Einstellung und das Verhalten der Nutzer spielen bei der Umsetzung eines ISA-Programms eine wesentliche Rolle /DHA 18/.

Für eine wirkungsvolle ISA sind nach /DHA 18/ kognitive, verhaltensbezogene und prozessbezogene Merkmale relevant:

- **Kognitive Perspektive**: In dieser Perspektive beschreibt ISA die Denkweise eines Nutzers, die durch das Wissen und die Wahrnehmung der Bedeutung eines Informationssicherheitssystems beeinflusst wird. Solche Nutzer sind an Informationssicherheit interessiert, wissen darüber Bescheid, sind sich Informationssicherheitsbedrohungen und -Risiken bewusst und können mit dem Informationssicherheitssystem der Organisation umgehen. Nach /DHA 18/ hat ISA sowohl einen kognitiven als auch einen verhaltensbezogenen Gesichtspunkt. Dabei stellt das Informationssicherheits-Bewusstsein der Nutzer den kognitiven Standpunkt dar und die Loyalität oder Treue der Nutzer gegenüber den Sicherheitszielen den verhaltensbezogenen Standpunkt, da die Nutzer die vorgegebenen Regeln und Vorschriften der organisatorischen Ziele verfolgen.
- **Verhaltensperspektive**: Das Verhalten reicht von der Identifizierung und Kenntnis des Informationssicherheitsmanagements der Organisation bis hin zur Reaktion und dem Engagement für die Ziele der Organisation /DHA 18/.
- **Prozessperspektive**: Diese Perspektive definiert den tatsächlichen Prozess der Erhöhung des Sicherheitsbewusstseins einer Organisation und der Durchführung von Sensibilisierungskampagnen.

Die Wirksamkeit von Programmen zur Sensibilisierung für Informationssicherheit

Die Nutzer sind nach /DHA 18/ das kritischste Element der Informationsgesellschaft, denn sie stellen eine potenzielle Schwachstelle und einen unkontrollierbaren Faktor dar. Demnach sind sie entscheidend für die Gewährleistung der Informationssicherheit in einer Organisation. Den meisten Nutzern ist jedoch nicht bewusst, wie ihr Verhalten und ihre Handlungen zu Informationssicherheitsvorfällen beitragen. Darüber hinaus empfinden viele Nutzer Informationssicherheit als Belastung. Die daraus resultierende Ablehnung von Informationssicherheitsmaßnahmen stellen daher ein Problem bei der Sicherstellung der Informationssicherheit in einer Organisation dar. Nutzer, die sich der Informationssicherheit bewusst sind, können dagegen informationssicherheitsbezogene Vorfälle intellektuell erkennen und damit umgehen. Für die Informationssicherheit müssen daher technische, organisatorische und menschliche Aspekte berücksichtigt werden. Eine Änderung des Verhaltens, der Einstellung und der Meinung ist von wesentlicher Bedeutung, um ein angemessenes Niveau der Informationssicherheit zu erreichen.

Außerdem haben Spears und Barki in einer Untersuchung herausgefunden, dass die Einbindung der Nutzer in ein Risikominderungsprogramm einen erheblichen Einfluss auf die Verbesserung des Sicherheitsverhaltens hat /DHA 18/.

Neue Nutzer müssen ein Informationssicherheits-Schulungs- und Sensibilisierungsprogramm durchlaufen und eine Einweisung absolvieren, bevor sie eine Aufgabe ausführen /DHA 18/.

Implementierung eines effektiven Schulungsprogramms zur Informationssicherheit

Die Organisation sollte Sicherheitsschulungen für jeden Benutzer durchführen. Um den Inhalt effektiv zu gestalten, sollte sie sich auf den ordnungsgemäßen Umgang mit organisatorischer Informationssicherheit und die möglichen Folgen einer falschen Handhabung konzentrieren. Sicherheitsschulungen sind ein effizienter Weg, um das Wissen des Benutzers zu verbessern. Sie sollten kontinuierlich durchgeführt werden und regelmäßig aktualisiert werden, um neue Bedrohungen und Risiken einzubinden /DHA 18/.

Verfahrensbasiertes Informationssicherheitsverhalten

In der Klassifikationstheorie wird das Verhalten eines Nutzers nach den Begriffen Adaption, Meinung und Charakter der Idee klassifiziert. Laut Stanton, Stam, Mastrangelo und Jolton ist es aus Sicht des Sicherheitsverhaltens unerlässlich, angemessene regelmäßige Beurteilungen und Überprüfungen von Benutzern durchzuführen. Die Klassifikationstheorie hebt die Merkmale organisatorischer Probleme hervor, bei denen eine Handlung rechtmäßig ist oder gegen das Gesetz verstößt. Sie unterscheidet vier Kategorien: 1. Nicht wissen – nicht tun 2. Nicht wissen – tun 3. Wissen – nicht tun 4. Wissen – tun.

- Nicht wissen – nicht tun

  In dieser Kategorie haben Nutzer weder eine Vorstellung von den organisatorischen Anforderungen an das Sicherheitsverhalten noch Kenntnisse über Informationssicherheit. Wenn sie nicht wissen, was sie tun sollen, und nichts tun, verstoßen sie gegen Informationssicherheits-Regeln und -Vorschriften, was zu einer Gefährdung der organisatorischen Informationssicherheit führt.

- Nicht wissen – tun

  In dieser Kategorie kennen Benutzer die ISP nicht und haben kein angemessenes Verständnis von Informationssicherheit, verfügen aber über ein angemessenes Informationssicherheitsverhalten (beispielsweise berät sich ein Nutzer mit Kollegen und Vorgesetzten, bevor er Maßnahmen ergreift).

- Wissen – nicht tun

  In dieser Kategorie hat der Nutzer das notwendige Wissen, legt jedoch kein angemessenes Informationssicherheitsverhalten an den Tag.

- Wissen–Tun

  In dieser Kategorie verfügen Benutzer über alle Kenntnisse und Fähigkeiten zur Gewährleistung einer hohen Informationssicherheit.

Aufbau eines effektiven Schulungs- und Sensibilisierungsprogramms für Informationssicherheit

Ein Schulungs- und Sensibilisierungsprogramm für die Informationssicherheit ist ein ideales Mittel, um den Nutzern die Informationssicherheit und die Sicherheitspolitik der Organisation nahezubringen und sicherzustellen, dass die Nutzer bei ihrer Arbeit die Richtlinien befolgen. Vor der Entwicklung eines solchen Programms müssen bestimmte Dinge berücksichtigt werden, wie z. B. die organisatorischen Bedürfnisse, das Ziel des Sicherheitsprogramms, das Risikomanagement und die Geschäftskontingenz. Die drei Attribute der Informationssicherheit – Vertraulichkeit, Integrität und Verfügbarkeit – sind die Hauptpfeiler des Schulungsprogramms. Das Programm muss mit der Mission der Organisation übereinstimmen, um ihre Geschäftsziele zu erreichen. Der Zweck eines Schulungs- und Sensibilisierungsprogramms ist es, die Sichtweise der Nutzer zu verbessern /DHA 18/.

Im Allgemeinen ist in den meisten Organisationen die IT- und Sicherheitsabteilung für den Schutz der physischen und technischen Ressourcen der Organisation verantwortlich. Das primäre Ziel eines Schulungs- und Sensibilisierungsprogramms für Informationssicherheit ist es, deutlich zu machen, dass die Informationssicherheit der Organisation die Angelegenheit aller Nutzer auf allen Ebenen ist und nicht nur in der Verantwortung der IT- und Sicherheitsabteilung liegt. Das Schulungs- und Sensibilisierungsprogramm zur Informationssicherheit sollte sich daher an alle Nutzer in einer

Organisation richten und die Geschäftsleitung sollte als Vorbild fungieren. Es sollte zudem in Abhängigkeit der Aufgabe und Position des Nutzers umgesetzt werden, und nicht einheitlich für alle /DHA 18/.

Die Messung der Effektivität des Schulungs- und Sensibilisierungsprogramms ist von entscheidender Bedeutung, um sicherzustellen, dass es eine signifikante Wirkung hat. Durch die Messung der Effektivität des Programms wird sichergestellt, dass alle Bedürfnisse der Endnutzer, der Organisation und des Schulungsprogramms selbst angesprochen und erfüllt werden. Wenn beispielsweise die Schulungsressourcen und -materialien den Schulungsanforderungen nicht gerecht werden, z. B. durch die Verwendung ungeeigneter Themen, die veraltet und für den heutigen Kontext nicht geeignet sind, dann entspricht das Schulungs- und Sensibilisierungsprogramm nicht den Anforderungen der Nutzer und der Organisation /DHA 18/.

3 Entwicklung eines Kriterien- und Fragenkatalogs zur Informationssicherheitskultur

3.1 Kriterienkatalog und Vergleich mit Kriterien der Sicherungs- und Sicherheitskultur

Um einen Kriterienkatalog für die Informationssicherheitskultur zu entwickeln, wurden im ersten Schritt die in den in Kap. 2 dargestellten Dokumenten enthaltenen Informationen gesichtet und bzgl. ihrer Übertragbarkeit und Anwendbarkeit auf die Informationssicherheitskultur analysiert. Wesentliche Erkenntnisquellen stellten hierbei insbesondere das IT-Grundschutz-Kompendium des BSI /BSI 22/ (siehe Kap. 2.5.1) sowie die IAEA-Dokumente NSS 17-T und NSS 23-G zur IT-Sicherheit (siehe Kap. 2.5.3 und 2.5.4) dar.

Die aus dieser Recherche gewonnenen Informationen wurden in Form von Kriterien für eine gute Informationssicherheitskultur formuliert und thematisch in die folgenden Gruppen eingeordnet:

A) Ziele und Politik der Organisation – Sicherheitsrichtlinien

B) Arbeitsbedingungen

C) Personelle Organisation
   1. Rollen und Verantwortlichkeiten
   2. Ressourcen
   3. Einsatz von Fremdpersonal

D) Schulungs- und Sensibilisierungsmaßnahmen
   1. Bewusstsein schaffen
   2. Schulungen - Durchführung
   3. Schulungen – Wirksamkeit
   4. Schulungen – Einstellungen
   5. Schulungen – Qualitätssicherung von Schulungsmaßnahmen
   6. Schulungen – Qualifikationsanforderungen

E) Ereignis- und Notfallmanagement
   1. Notfallmanagement
   2. Beweissicherung
   3. Umgang mit Sicherheitsvorfällen

4. Auswertung von interner und externer (nationaler und internationaler) Betriebserfahrung zur ständigen Verbesserung

F) Qualitätssicherung

G) Änderungsmanagement

H) Sicherer Umgang mit Informationen
   1. Sichere Email-Kommunikation
   2. Sicherer Umgang mit Informationen im Unternehmen
   3. Sicherer Umgang mit Informationen auf Reisen
   4. Zugriffs-, Zugangs- und Zutrittsrechte
   5. Vertraulichkeit von Informationen
   6. Aufzeichnungen

I) Einstellungen und Erwartungen
   1. Einstellungen und Überzeugungen
   2. Erwartungen

J) Führungs- und Personalverhalten

K) Motivation, Fehlerkultur, Selbsteinschätzung
   1. Motivation
   2. Fehlerkultur
   3. Selbsteinschätzung
   4. Leistungsmessung

L) Zuverlässigkeit

M) Betrieb und Instandhaltung

N) Kommunikation
   1. Interne Kommunikation
   2. Kommunikation mit externen Organisationen
   3. Schnittstelle zur Überwachungsbehörde

Die in diesem Vorhaben entwickelten Kriterien zur Informationssicherheitskultur sind zusammen mit den von der IAEA erarbeiteten Kriterien der Sicherheits- und Sicherungskultur in Anhang A dargestellt. Auch wenn die Informationssicherheitskultur als Teil der Sicherungskultur angesehen wird, wird sie hier getrennt von den Sicherungskultur-Kriterien der IAEA dargestellt, um eine vergleichende Analyse der Ergebnisse aus diesem

Vorhaben mit den übergeordneten Kriterien der IAEA zu ermöglichen. Die Kriterien der IAEA zur Sicherungskultur gelten aber ebenfalls für den Bereich der Informationssicherheitskultur. Zudem ergeben sich zusätzliche Kriterien in der Informationssicherheitskultur, die es in der Sicherungskultur nicht gibt (z.B. sicherer Umgang mit Emails, sicherer Umgang mit Daten im Betrieb und auf Reisen).

Der Vergleich der Kriterien aus Informationssicherheitskultur, Sicherungs- und Sicherheitskultur zeigt, dass in jeder Kulturfacette bei der Entwicklung der Kriterien eine etwas andere Herangehensweise verwendet wurde. Dadurch ergeben sich zum Teil Überschneidungen als auch Lücken bei den Kriterien der unterschiedlichen Facetten. Teilweise werden dieselben Aspekte in mehreren Kulturfacetten behandelt, jedoch mit unterschiedlichem Themenschwerpunkt oder anderer Formulierung:

Informationssicherheitskultur	Sicherungskultur	Sicherheitskultur
Ziele und Politik der Organisation - Sicherheitsrichtlinien		
Es existieren Richtlinien und klar definierte Ziele zur Informationssicherheit	Für die Organisation wird eine Sicherungsrichtlinie erstellt Es existiert ein Verhaltenskodex für das Personal, der die Bedürfnisse der nuklearen Sicherung abdeckt	Die strategische geschäftliche Bedeutung der Sicherheit spiegelt sich im Geschäftsplan wider: Ziele, Strategien, Pläne, Zielsetzungen bzgl. Sicherheit sollten klar identifiziert und in den Geschäftsplan integriert werden
	Es existiert eine dokumentierte Richtlinie zur Informationssicherheit, die alle Informationsträger umfasst	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: Die Sicherheitspolitik sollte dokumentiert werden
Arbeitsbedingungen		
Führungskräfte schaffen best-mögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a.	Arbeitsklima unterstützt Teamarbeit und Wissensaustausch Teamwork und Kooperation wird auf allen Ebenen und über organisatorische	

Informationssicherheitskultur	Sicherungskultur	Sicherheitskultur
Förderung von Teamwork	und bürokratische Grenzen hinweg gefördert	
	Führungskräfte helfen, Vertrauen aufzubauen und die Teamarbeit innerhalb der Organisation zu fördern	Vertrauen durchdringt die Organisation

Umgekehrt werden manche Themen nur in einer Kulturfacette behandelt, die aber genauso Anwendung in den anderen Kulturfacetten finden könnten. Beispielsweise wird das Thema „Bewusstsein schaffen“ in der Sicherungskultur sehr ausführlich adressiert, während es bei den Kriterien der Sicherheitskultur nicht zu finden ist. Ebenso werden die Qualitätssicherung bei Schulungsmaßnahmen und die Qualifikationsanforderungen in den Kriterien der Sicherheitskultur nicht adressiert.

3.2 Fragenkatalog

Um das Vorhandensein und die Ausprägung der in Kap. 3.1 behandelten und in Anhang A dargestellten Kriterien in einer Organisation erfassen und bewerten zu können, wurde ein grundlegender Fragenkatalog entwickelt. Zu diesem Zweck erfolgte zunächst eine Recherche des Standes von W&T zu Methoden, die bei der Formulierung von Fragen bzw. Aussagen (in der Fachliteratur allgemein als „Items“ bezeichnet) und zur Entwicklung eines Fragebogens herangezogen werden können. Es wurden hierzu zunächst stichprobenartig die folgenden Quellen herangezogen:

Beris, Beautement, Sasse (2015) - Employee Rule Breakers, Excuse Makers and Security Champions: Mapping the risk perceptions and emotions that drive security behaviors /BER 15/

In dieser Veröffentlichung stellen die Autoren eine Methodologie zur Identifikation von Faktoren, die das Sicherungsverhalten von Mitarbeitern einer Organisation beeinflussen, vor. Basierend auf 93 Interviews mit Angestellten aus zwei multinationalen Organisationen stellen sie, als die zwei wesentlichen Säulen des Sicherungsverhaltens, zum einen das Risikoverständnis und zum anderen die emotionale innere Einstellung des Einzelnen zur Sicherungspolitik der Organisation dar. Basierend auf den Umfrageergebnissen

wurden insgesamt 16 verschiedene Verhaltenstypen kategorisiert. Anhand dieser Kategorien wird es Organisationen ermöglicht, potenzielle Schwachstellen und Verbesserungspotenziale im Verhalten der Belegschaft zu identifizieren. An diesen kann durch gezielte Maßnahmen angesetzt werden, um das Verhalten einzelner Personen und von Personengruppen im Sinne der Sicherung zu verbessern.

Kirlappos, Parkin, Sasse (2014) - Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security /KIR 14/

In dieser Veröffentlichung wird der Zusammenhang zwischen der Nicht-Einhaltung von Sicherungsrichtlinien und der Einhaltung anderweitiger Arbeitsziele betrachtet. Anstatt die Einhaltung oder Nicht-Einhaltung von Sicherungsrichtlinien als eine reine „Ja-oder-nein"-Entscheidung zu sehen, soll den Autoren zufolge stärker berücksichtigt werden, dass eine Nicht-Einhaltung auch daraus entstehen kann, dass eine Person mit ausgeprägtem Bewusstsein für Sicherungsaspekte schlicht keine Vereinbarkeit mit der Erfüllung ihrer Arbeitsaufgaben sieht und sich daher eine Alternative zu den Sicherungsrichtlinien und -prozessen sucht. Diese von den Autoren als „Shadow-Security" bezeichnete Vorgehensweise stellt eine Kompromisslösung dar, die die Sicherungsziele nur teilweise erfüllt, aber schwieriger zu erkennen ist als eine vollständige Nicht-Einhaltung. Anstatt diese Kompromisslösung abzulehnen, solle diese aber von der Organisation als Ausgangspunkt für eine besser mit den Arbeitszielen vereinbare Sicherungsstrategie gesehen werden.

Kirlappos, Sasse (2015) - Fixing Security Together: Leveraging trust relationships to improve security in organizations /KIR 15/

Diese Veröffentlichung kritisiert den in der Vergangenheit zu starken Fokus auf formale Sicherungsmechanismen und- richtlinien und deren Kommunikation an das Personal. Ein aus Sicht der Autoren zu lange vernachlässigter Faktor ist hingegen der Einfluss dieser Mechanismen und Richtlinien auf die Vertrauensverhältnisse der einzelnen Personen zueinander und zur Organisation als Ganzes. Durch Veränderungen dieser Vertrauensverhältnisse wird auch das Sicherungsverhalten des Einzelnen beeinflusst. Aus einer Analyse von 208 vertieften Interviews mit Angestellten zweier multinationaler Organisationen schließen die Autoren, dass die Verbesserung eines dieser beiden Vertrauensverhältnisse sich negativ auf das jeweils andere auswirken kann (z.B., wenn die Einhaltung einer Sicherungsrichtlinie der Organisation eine Belastung des Vertrauens der Angestellten untereinander bedeutet). Daher wird den Designern von Sicherungs-

architekturen innerhalb einer Organisation empfohlen, die beiden genannten Formen von Vertrauensverhältnissen zu berücksichtigen, um negative Wechselwirkungen zu vermeiden und stattdessen Synergien zu nutzen, die die Angestellten zu einem sicherungskonformen Verhalten motivieren und die Notwendigkeit für technische Lösungen verringern können.

Bühner, M. (2010). Einführung in die Test- und Fragebogenkonstruktion. Pearson Deutschland GmbH /BUE 10/

In diesem Werk werden die grundlegenden zu beachtenden Aspekte bei der Erstellung von Fragebögen ausführlich dargelegt. Wesentlich sind die Definition der Zielgruppe und des Messgegenstandes sowie das Format und die Formulierung der im Fragebogen enthaltenen einzelnen Fragen (sogenannte Items). Da durch die Wahl dieser Parameter und die daraus resultierende Gestaltung des Fragebogens das Ergebnis beeinflusst oder gar verfälscht werden kann (beispielsweise durch eine für die Zielgruppe nicht angemessene Schwierigkeit einer oder mehrerer Fragen, die Verwendung verschieden interpretierbarer Begriffe oder einen zu großen Umfang, der zu Ermüdung bei den Befragten führt), müssen diese bei der Fragebogenerstellung angemessen berücksichtigt werden.

Entwicklung des Fragenkatalogs

Bei der Analyse der oben beschriebenen Auswahl von Quellen wurde festgestellt, dass neben einer Ausweitung der Literaturrecherche eine komplexe Vielzahl von Kriterien herangezogen werden müsste, um den Fragenkatalog tatsächlich für Umfragen praktisch anwendbar zu machen. Darüber hinaus können über einen Fragebogen ggf. zu manchen Kriterien keine aussagekräftigen Antworten gefunden werden. Es müssen demnach zusätzlich andere Methoden herangezogen werden, um eine aussagekräftige Bewertung der IT-Sicherungskultur vornehmen zu können. Eine solche tiefgehende Recherche und Anwendung der Methoden überschreitet jedoch den Umfang dieses Vorhabens und wurde daher nicht weiterverfolgt. Um dennoch einen Fragenkatalog zur Kriterienliste erstellen zu können, wurden einige grundlegende Kriterien aus der durchgeführten Literaturrecherche ausgewählt und angewandt. Hierbei handelt es sich um folgende Kriterien:

- keine Negativformulierungen
- keine Verwendung doppelter Verneinungen
- Verwendung kurzer und einfach nachvollziehbarer Items
- nur ein Merkmal pro Item
- Verwendung klar definierter Begrifflichkeiten

Für die Erfassung der einzelnen Kriterien wurden jeweils eines oder mehrere Items formuliert, auf die, je nach behandeltem Aspekt, auf unterschiedliche Weise geantwortet werden kann. Es wurden dazu die folgenden Beantwortungsmöglichkeiten ausgewählt:

- Ja/Nein-Antwort
- Antwort in Freitextform
- Antwort durch Angabe von Zahlenwerten
- Antwort mit Bewertungsskala
- Mehrere Antwortmöglichkeiten (Multiple Choice)

Bevor mit der eigentlichen Formulierung der Items begonnen wurde, erfolgte eine Festlegung der Zielgruppe jedes Kriteriums des Kriterienkatalogs, die mit den im nächsten Schritt zu formulierenden Items angesprochen werden soll. Folgende Zielgruppen wurden identifiziert:

- Mitarbeitende
- Führungskräfte
- Fremdpersonal
- IT-Fachpersonal
- Personen mit vollständigen Kenntnissen der internen Regelwerke und Prozesse[4]
- Personen mit Beteiligung an internen Prüfungen
- Personen, die Schulungen durchführen
- Personen mit administrativen Aufgaben
- Mitglieder des Notfallmanagement-Teams
- Personen bei der Aufsichtsbehörde
- Personen mit direkter Beteiligung an forensischen Untersuchungen

Eine detaillierte, den Anforderungen für die praktische Anwendung vollständig genügende Ausarbeitung des Fragenkatalogs war im Rahmen dieses Vorhabens aufgrund der dafür erforderlichen zeitlichen Ressourcen nicht im vollen Umfang möglich. Der hier erarbeitete Fragenkatalog stellt daher eine Basis dar, auf der mögliche Folgevorhaben aufbauen können. Der Fragenkatalog ist in Tab. 3.1 aufgeführt.

[4] Das können z.B. Führungskräfte sein oder Personen, die an der Erstellung der Regelwerke mitgewirkt haben.

Tab. 3.1 Fragenkatalog zu den Kriterien des Kriterienkatalogs

Kriterium		Zielgruppe	Item	Art der Beantwortung
A (1)	Es existieren Richtlinien und klar definierte Ziele zur Informationssicherheit.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Meine Organisation hat klar definierte Ziele mit Bezug auf die Informationssicherheit.	Bewertungsskala
A (2)	Die Richtlinien zur Informationssicherheit wurden zielgruppen- und bedarfsgerecht erstellt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Die Richtlinien, Regelungen, Vorgaben und Konzepte meiner Organisation sind zielgruppenorientiert formuliert.	Bewertungsskala
A (3)	In den Richtlinien zur Informationssicherheit wurden konkrete Maßnahmen festgelegt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Meine Organisation hat in Richtlinien, Regelungen, Vorgaben und Konzepten konkrete Maßnahmen für den Erhalt der Informationssicherheit festgelegt.	Ja/Nein
A (4)	Die Anforderungen der Informationssicherheitsrichtlinien entsprechen den rechtlichen und behördlichen Vorschriften.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Die Anforderungen der Informationssicherheitsrichtlinie entsprechen den rechtlichen und behördlichen Vorschriften.	Ja/Nein
A (5)	Die Informationssicherheitsrichtlinien sollten durchsetzbar, erreichbar und überprüfbar sein.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	

Kriterium		Zielgruppe	Item	Art der Beantwortung
A (6)	Richtlinien und klar definierte Ziele zur Informationssicherheit sind für das Personal sichtbar, ihnen bekannt und allgegenwärtig (z.B. über ihnen zugängliche Medien wie Intranet, Newsletter, Poster, etc.).	Mitarbeitende	Die Richtlinien, Regelungen, Vorgaben und Konzepte zur Informationssicherheit sind für mich jederzeit leicht zugänglich.	Bewertungsskala
		Mitarbeitende	Ich werde von meiner Organisation an die Richtlinien zur Informationssicherheit bei Bedarf/regelmäßig erinnert.	Bewertungsskala
A (7)	Richtlinien zur Informationssicherheit werden eingehalten und gelebt		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
A (8)	Es gibt Prozesse, mit denen die Einhaltung der Informationssicherheitsrichtlinien überprüft wird.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Einhaltung der Richtlinien zur Informationssicherheit.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Der schriftlich festgelegte Prozess zur Überprüfung der Einhaltung der Richtlinien zur Informationssicherheit hat sich als effektiv erwiesen.	Bewertungsskala
A (9)	Mögliche sich ändernde Anforderungen an Informationssicherheitsrichtlinien werden in Form eines festgelegten Prozesses regelmäßig überprüft und bei Bedarf aktualisiert.	Personen mit Kenntnis der internen Regelwerke und Prozesse	In meiner Organisation existiert ein schriftlich festgelegter Prozess zur regelmäßigen Überprüfung und Aktualisierung von Informationssicherheitsrichtlinien.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
A (10)	Dem Personal ist aufgrund der Richtlinien zur Informationssicherheit klar, wie sie sich im täglichen Umgang mit IT-Systemen, bei sicherheitsrelevanten Ereignissen und bei Notfällen zu verhalten haben.	Mitarbeitende	Die bestehenden Richtlinien zur Informationssicherheit geben mir eine klare Vorstellung davon, wie ich mich im täglichen Umgang mit IT-Systemen mit Blick auf die Informationssicherheit zu verhalten habe.	Bewertungsskala
		Mitarbeitende	Die bestehenden Richtlinien zur Informationssicherheit geben mir eine klare Vorstellung davon, wie ich mich bei sicherheitsrelevanten Ereignissen zu verhalten habe.	Bewertungsskala
		Mitarbeitende	Die bestehenden Richtlinien zur Informationssicherheit geben mir eine klare Vorstellung davon, wie ich mich bei Notfällen zu verhalten habe.	Bewertungsskala
		Führungskräfte	Im vergangenen [Monat/Jahr] kamen Angestellte __ Mal mit Fragen zum Verhalten bei informationssicherheitsrelevanten Ereignissen auf mich zu.	Zahlenwert
		Führungskräfte	Im vergangenen [Monat/Jahr] kamen Angestellte __ Mal mit Fragen zum Verhalten bei informationssicherheitsrelevanten Notfällen auf mich zu.	Zahlenwert
B (1a)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a.	Mitarbeitende	Wir verfügen über ausreichend Personal, um das Arbeitspensum zu bewältigen.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	• Vermeidung von Zeitdruck bei der Arbeit			
B (1b)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Förderung von Teamwork	Mitarbeitende	Ich fühle mich von meinen Kollegen unterstützt.	Bewertungsskala
B (1c)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Schaffung eines vertrauensvollen Umfelds (Belohnung vs. Bestrafung, offene Fehlerkultur)	Mitarbeitende	Ich habe das Gefühl, dass mir unbeabsichtigtes Fehlverhalten nicht zur Last gelegt wird.	Bewertungsskala
		Mitarbeitende	Ich mache mir Sorgen, dass es in meiner Personalakte vermerkt wird, wenn ich einen Fehler im Umgang mit der Informationssicherheit mache.	Bewertungsskala
B (1d)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Multidisziplinäre Teams zur Lösung von Problemen	Mitarbeitende	Wir arbeiten oft in Teams mit unterschiedlichem fachlichem Hintergrund, wenn dies für die Lösung eines Problems hilfreich ist.	Bewertungsskala
		Mitarbeitende	Ich habe das Gefühl, dass wir uns bei der Teamarbeit gut ergänzen.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
B (1e)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Einbindung der Mitarbeitenden in den Entscheidungsprozess	Mitarbeitende	Ich werde von meinen Vorgesetzten in Entscheidungen bei informationssicherheitstechnischen Fragestellungen einbezogen.	Bewertungsskala
B (1f)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Es gibt einen Feedback- und Verbesserungsprozess	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Feedback- und Verbesserungsprozess für Belange des gesamten Unternehmens.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Feedback- und Verbesserungsprozess für Belange einzelner Abteilungen.	Ja/Nein
		Mitarbeitende	In [Abteilung, Bereich] herrscht ein konstruktives Miteinander, in dem auch Fehler gegenseitig angesprochen werden.	Bewertungsskala
B (1g)	Als zugrundeliegende Basis wird beim Personal eine kritisch hinterfragende Grundhaltung gefördert. Dies beinhaltet auch den Schutz der Personen, die Probleme melden (z.B. durch	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur anonymen Meldung von Missständen.	Ja/Nein
		Führungskräfte	Eine kritisch hinterfragende Grundhaltung der Angestellten wird in [Abteilung/Bereich] aktiv gefördert.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	die Möglichkeit der anonymen Meldung).	Mitarbeitende	Wenn ich auf einen Missstand hinweise, wird wertschätzend/abwehrend/abwertend damit umgegangen.	Multiple Choice
B (1h)	Wenn ein Fehler oder ein Ereignis auftritt, lautet die Frage "Was ist schiefgelaufen?" und nicht "Wer hat sich geirrt?", wobei der Schwerpunkt auf Verbesserung und nicht auf Schuldzuweisung liegt.	Mitarbeitende	In meiner Abteilung werden aufgetretene Fehler dazu genutzt, die bestehenden Prozesse und Verhaltensweisen stetig zu verbessern.	Bewertungsskala
		Mitarbeitende	Mit unabsichtlichen Fehlern wird in [Abteilung, Bereich] sachlich und ohne persönliche Schuldzuweisungen umgegangen.	Bewertungsskala
		Führungskräfte	Ich lege Wert darauf, dass mit Fehlern von Einzelpersonen sachlich umgegangen wird.	Bewertungsskala
B (1i)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Ermutigung zu Verbesserungsvorschlägen	Mitarbeitende	Ich fühle mich dazu ermutigt, Verbesserungsvorschläge zu äußern.	Bewertungsskala
C (1)	Die Organisation hat klar definierte und dokumentierte Rollen und Verantwortlichkeiten für	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren klar definierte Rollen und Verantwortlichkeiten für alle Positionen im Bereich der Informationssicherheit.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	alle Positionen im Bereich der Informationssicherheit.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Die Rollen und Verantwortlichkeiten für die Informationssicherheit sind in der Organisation gut dokumentiert.	Bewertungsskala
C (2)	Die Institutionsleitung übernimmt die Gesamtverantwortung.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
C (3)	Für das Personal ist offensichtlich, dass die Gesamtverantwortung für die Informationssicherheit beim Management der Geschäftsführung angesiedelt ist.	Mitarbeitende	Mir ist bewusst, dass die Geschäftsführung die Gesamtverantwortung für die Informationssicherheit trägt.	Bewertungsskala
C (4)	Alle Mitglieder der Organisation sind sich sowohl ihrer individuellen als auch der gemeinsamen Verantwortung in Bezug auf die Informationssicherheit bewusst.	Mitarbeitende	Ich bin mir meiner individuellen Verantwortung, einen Beitrag zur Informationssicherheit zu leisten, bewusst.	Bewertungsskala
		Mitarbeitende	Ich bin mir der Tatsache bewusst, dass meine Kollegen und ich eine gemeinsame Verantwortung für die Informationssicherheit tragen.	Bewertungsskala
C (5)	Das Personal versteht seine Rollen und Verantwortlichkeiten für die	Mitarbeitende	Mir sind alle für meine Tätigkeit relevanten Rollen und Verantwortlichkeiten der Informationssicherheit bekannt.	Bewertungsskala oder Freitext

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Informationssicherheit, fühlt sich dafür verantwortlich und kommt diesen vollumfänglich nach.	Mitarbeitende	Ich verstehe meine Rollen und Verantwortlichkeiten in Bezug auf die Informationssicherheit	Bewertungsskala oder Freitext
		Mitarbeitende	Ich fühle mich verantwortlich dafür, meinen Beitrag zur Informationssicherheit zu leisten.	Bewertungsskala
		Führungskräfte	Die Angestellten in (Abteilung/Bereich) kommen ihrer Verantwortung für die Informationssicherheit zuverlässig nach.	Bewertungsskala
C (6)	Hierarchische Lücken, die durch Abgänge von Personal entstehen, werden schnellstmöglich geschlossen.	Mitarbeitende	Ich habe den Eindruck, dass die Arbeitsabläufe durch Personalabgänge deutlich beeinträchtigt werden.	Bewertungsskala
		Führungskräfte	Ich habe den Eindruck, dass die durch Personalabgänge entstehenden Lücken in kurzer Zeit geschlossen werden.	Bewertungsskala
C (7)	Es existieren Vertretungs- und Nachfolgeregelungen, falls einzelne Personen ausfallen (Krankheit, Abwesenheit, Abgang).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Für Personalausfälle (z.B. durch Krankheit, Abwesenheit) existieren Vertretungsregelungen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Für Personalabgänge existieren Nachfolgeregelungen.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
C (8)	Es existieren Absprachen, vertragliche Festlegungen zu Rollen und Verantwortlichkeiten sowie Vertretungsregelungen im Umgang mit externen Dienstleistern/Unterauftragnehmern etc.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren vertragliche Festlegungen zu Rollen und Verantwortlichkeiten im Umgang mit externen Dienstleistern.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren Vertretungsregelungen für den Fall von Personalausfällen an verantwortlichen Stellen für den Umgang mit externen Dienstleistern.	Ja/Nein
		Führungskräfte	Es existieren vertragliche Festlegungen zu Rollen und Verantwortlichkeiten im Umgang mit externen Dienstleistern.	Ja/Nein
		Führungskräfte	Es existieren Vertretungsregelungen für den Fall von Personalausfällen an verantwortlichen Stellen für den Umgang mit externen Dienstleistern.	Ja/Nein
C (9)	Fremdpersonal kennt die für sie relevanten Gesetze, Vorschriften und internen Regelungen. Sie werden dem Fremdpersonal über ihnen zugängliche Medien (z.B. Poster,	Fremdpersonal	Mir werden durch den Auftraggeber Gesetze, Vorschriften und interne Regelungen sichtbar gemacht, die Bedeutung für meine dortige Arbeit haben.	Bewertungsskala
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Ich wurde vor Arbeitsbeginn durch Schulungen über relevante unternehmens-/branchenspezifische Gesetze/Regeln informiert.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Hinweisschilder) allgegenwärtig und sichtbar gemacht.	Führungskräfte	Das mir unterstellte Fremdpersonal wurde mit unternehmens-/branchenspezifischen Gesetzen, Vorschriften und Regelungen vertraut gemacht.	Bewertungsskala
C (10)	Es ist dafür Sorge zu tragen, dass Fremdpersonal, das kurzfristig/einmalig in sicherheitsrelevanten Bereichen eingesetzt wird, überwacht und in dem für die auszuführenden Arbeiten notwendigen (ggf. reduzierten) Umfang eingewiesen wird.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Einweisung von Fremdpersonal vor einmaligen/kurzfristigen Tätigkeiten	Ja/Nein
		Führungskräfte	Fremdpersonal wird auch vor kurzfristigen/einmaligen Tätigkeiten eingewiesen.	Ja/Nein
C (11)	Fremdpersonal hält die geltenden Gesetze, Vorschriften und internen Regelungen ein.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
C (12)	Bei längerfristiger Beschäftigung muss Fremdpersonal in die Aufgaben eingewiesen werden. Schulungen werden vertraglich festgelegt und durchgeführt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Einweisung von Fremdpersonal vor langfristiger Tätigkeit	Ja/Nein
		Führungskräfte	Fremdpersonal wird vor langfristigen Tätigkeiten eingewiesen.	Ja/Nein
C (13)	Beim ausscheidenden Fremdpersonal bestehen	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren mit den Prozessen für Eigenpersonal vergleichbare Prozesse für das Ausscheiden von Fremdpersonal.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	vergleichbare Prozesse wie für eigenes Personal.	Führungskräfte	Beim Ausscheiden von Fremdpersonal kommen vergleichbare Nachfolgeregelungen wie für Eigenpersonal zum Einsatz.	Ja/Nein
D (1)	Die Bedrohung, gegen die IT-Systeme geschützt werden sollten, ist festgelegt und wird von allen an der Konzeption, Anwendung und Bewertung der Sicherheitsmaßnahmen beteiligten Parteien gut verstanden.	IT-Fachpersonal	Ich verstehe, gegen welche Bedrohungen IT-Systeme zu schützen sind.	Multiple Choice oder Freitext
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Bedrohungen sind festgelegt, gegen die IT-Systeme zu schützen sind.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Die Bedrohungen, gegen die IT-Systeme zu schützen sind, werden im Schutzkonzept vollständig berücksichtigt.	Bewertungsskala
D (2)	Allen Parteien sind die Synergien, die sich durch die verschiedenen Systeme der Sicherheit und Sicherung ergeben, bekannt.	Führungskräfte	Den Angestellten in meinem Verantwortungsbereich sind die Synergien, die sich durch die verschiedenen Systeme der Sicherheit und Sicherung ergeben, bekannt.	Bewertungsskala
		Mitarbeitende	Mir sind die Synergien, die sich durch die verschiedenen Systeme der Sicherheit und Sicherung ergeben, bekannt.	Multiple Choice oder Freitext
D (3)	Personal und Führungskräfte engagieren sich für die Ziele der Informationssicherheit und	Führungskräfte	Angestellte in meinem Verantwortungsbereich engagieren sich über die bloße Erfüllung ihrer Arbeitsaufgaben hinaus für die Informationssicherheit.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	legen ein Verhalten an den Tag, das bei Bedarf über die Erfüllung der eigenen Aufgaben hinausgeht.			
D (4)	Es werden regelmäßige Schulungen zu allen für die Informationssicherheit IT-Sicherung relevanten Themen/Aspekten durchgeführt. Dies umfasst u.a. die folgenden Themen: • Behandlung von Sicherheitsvorfällen (Hackerangriffe, Phishing • Erkennung von riskantem/gefährlichem Verhalten • forensische Beweissicherung • Dokumentation, Führen von Logs, Archivierung • Sensibilität von Informationen/Schutz von sensiblen Daten • Sicheres Ablegen, Speicher, Löschen, Vernichten, Verschlüsselung von Daten/Informationen	Mitarbeitende	In den vergangenen [Monaten/Jahren] habe ich an ___ verschiedenen Schulungen zur Informationssicherheit teilgenommen	Zahlenwert

Kriterium		Zielgruppe	Item	Art der Beantwortung
	• sicherer Umgang mit Informationen auf Dienstreisen • Zugangs-/Zutrittsberechtigungen • Passwort- und Schlüsselmanagement (digital und physisch) • Erkennung nicht vertrauenswürdiger Dateien/Datenträger • Informationsaustausch/Umgang mit Informationen • Verhalten auf Dienstreisen • besondere Aufgaben/Verantwortlichkeiten/Verhaltensweisen als Führungskraft • Einsatz/Verteilung von Ressourcen (materiell, finanziell, personell) • Rollen und Verantwortlichkeiten/Übernahme von Verantwortung/Verantwortliches Handeln • Wissenserhalt/Übergabe bei Personalwechseln • Schulungen für Administratoren			

Kriterium		Zielgruppe	Item	Art der Beantwortung
	• Authentisierungsverfahren und -prozesse • Überzeugungen, Einstellungen, Professionalität • Führungsverhalten • Änderungsmanagement			
D (5)	Die interne und externe Betriebserfahrung fließt in die Inhalte und Schwerpunkte von Schulungsmaßnahmen ein.	Personen, die Schulungen durchführen	Die Inhalte und Schwerpunkte der Schulungen werden bei neuer interner Betriebserfahrung überarbeitet.	Ja/Nein
		Personen, die Schulungen durchführen	Die Inhalte und Schwerpunkte der Schulungen werden bei neuer externer Betriebserfahrung überarbeitet.	Ja/Nein
D (6)	Das Personal (Mitarbeiter und Führungskräfte) nimmt an allen für ihren Fachbereich relevanten Schulungen teil.	Mitarbeitende	Die Schulungen, an denen ich in den vergangenen [Monaten/Jahren] teilgenommen habe, behandelten die folgenden Themen: ___	Freitext
D (7)	Die Teilnahme an Schulungsmaßnahmen wird dokumentiert und überprüft.	Personen, die Schulungen durchführen	Die Teilnahme an Schulungsmaßnahmen wird dokumentiert und überprüft.	Ja/Nein
D (8)	Es finden Nachholtermine bei Verhinderung statt.	Personen, die Schulungen durchführen	Es finden Nachholtermine bei Verhinderung statt.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
D (9)	Bei Änderungen an Arbeits- und Vorgehensweisen finden Sonderschulungen statt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Durchführung von Sonderschulungen bei Änderungen an Arbeitsweisen.	Ja/Nein
		Führungskräfte	Bei Änderungen an Arbeitsweisen nehmen die betroffenen Angestellten an einer Sonderschulung teil.	Ja/Nein
D (10)	Personen, die Schulungen durchführen, haben ausreichend Zeit zur Vorbereitung und Durchführung.	Personen, die Schulungen durchführen	Die mir zur Verfügung gestellte Zeit zur Vorbereitung von Schulungen ist ausreichend.	Bewertungsskala
D (11)	Das Personal wird auch für den Umgang mit unerwarteten Situationen/Entwicklungen geschult.	Personen, die Schulungen durchführen	In Schulungen wird der Umgang mit unerwarteten Situationen/Entwicklungen behandelt.	Ja/Nein
		Mitarbeitende	In Schulungen wird der Umgang mit unerwarteten Situationen/Entwicklungen behandelt.	Ja/Nein
D (12)	Das Personal sollte IT-Systeme als Unterstützung wahrnehmen und im Umgang mit ihnen geschult sein. Zudem sollten sie bei einem Ausfall wissen, was zu tun ist, um weiterhin arbeitsfähig zu bleiben und Sicherheitsvorfälle zu vermeiden.	Mitarbeitende	Ich muss manchmal IT-Systeme verwenden, mit deren Umgang ich mich nicht vertraut fühle und die in meinen Augen die Arbeitsabläufe verkomplizieren.	Ja/Nein
		Mitarbeitende	Beim Ausfall eines IT-Systems weiß ich, an wen ich mich wenden muss, damit eine Lösung für das Problem gefunden werden kann.	Multiple Choice oder Freitext

Kriterium		Zielgruppe	Item	Art der Beantwortung
		IT-Fachpersonal	Beim Ausfall eines IT-Systems kenne ich die Maßnahmen, die zu ergreifen sind, um das Problem zu beheben	Multiple Choice oder Freitext
		Personen, die Schulungen durchführen	Es werden Schulungen zum Umgang mit IT-Systemen durchgeführt.	Ja/Nein
		Mitarbeitende	Es werden Schulungen zum Umgang mit IT-Systemen durchgeführt.	Ja/Nein
		Personen, die Schulungen durchführen	Es werden Schulungen zum Umgang mit dem Ausfall von IT-Systemen durchgeführt.	Ja/Nein
		Mitarbeitende	Es werden Schulungen zum Umgang mit dem Ausfall von IT-Systemen durchgeführt.	Ja/Nein
D (13)	Es existiert ein Prozess zur Überprüfung der Wirksamkeit von Schulungen und Übungen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Wirksamkeit von Schulungen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Wirksamkeit von Übungen.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Personen mit Beteiligung an internen Prüfungen	Überprüfungen der Wirksamkeit von Schulungen werden alle ___ [Wochen/Monate/Jahre] durchgeführt.	Zahlenwert
		Personen mit Beteiligung an internen Prüfungen	Überprüfungen der Wirksamkeit von Übungen werden alle ___ [Wochen/Monate/Jahre] durchgeführt.	Zahlenwert
D (14)	Als Grundlage der Überprüfung der Wirksamkeit von Schulungen und Übungen gibt es klar definierte Zielvorgaben.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Für die Überprüfung der Wirksamkeit von Schulungen gibt es definierte Zielvorgaben.	Ja/Nein oder Bewertungsskala
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Für die Überprüfung der Wirksamkeit von Übungen gibt es definierte Zielvorgaben.	Ja/Nein oder Bewertungsskala
		Personen mit Beteiligung an internen Prüfungen	Für die Überprüfung der Wirksamkeit von Schulungen gibt es definierte Zielvorgaben.	Ja/Nein oder Bewertungsskala
		Personen mit Beteiligung an internen Prüfungen	Für die Überprüfung der Wirksamkeit von Übungen gibt es definierte Zielvorgaben.	Ja/Nein oder Bewertungsskala
D (15)	Führungskräfte messen, inwieweit Schulungsprogramme zu einer Verbesserung der		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung)	

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Einstellung zur Sicherungskultur beitragen.			
D (16)	Das Personal erkennt an, dass Lernen ein kontinuierlicher und fortlaufender Prozess in der gesamten Organisation ist.	Mitarbeitende	Lernen ist: a) etwas, dass vor allem im Studium/in der Ausbildung stattfindet b) ein kontinuierlicher und fortlaufender Prozess in der gesamten Organisation c) mit hohem Zeitaufwand verbunden und daher möglichst zu vermeiden	Multiple Choice
D (17)	Der Inhalt von Schulungen wird regelmäßig überprüft und ggf. an die Weiterentwicklung von W&T angepasst.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren Vorgaben zur Überprüfung des Inhalts von Schulungen mind. alle ___ [Monate/Jahre]	Zahlenwert
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren Vorgaben zur Anpassung des Inhalts von Schulungen an den Stand von W&T.	Ja/Nein
		Personen, die Schulungen durchführen	Eine Überprüfung des Inhalts von Schulungen findet alle ___ [Wochen/Monate/Jahre] statt.	Zahlenwert
		Personen, die Schulungen durchführen	Der Inhalt von Schulungen wird an den Stand von W&T angepasst.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
D (18)	Der Feedback- und Verbesserungsprozess berücksichtigt den Input der Schulungsteilnehmer.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es gibt einen schriftlich festgelegten Feedback- und Verbesserungsprozess für Schulungen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Der Feedback- und Verbesserungsprozess für Schulungen berücksichtigt den Input der Schulungsteilnehmer.	Bewertungsskala
		Mitarbeitende	Ich habe den Eindruck, dass mein Feedback zu den von mir besuchten Schulungen bei der Überarbeitung/Verbesserung dieser Schulungen berücksichtigt wurde.	Bewertungsskala
D (19)	Es existiert ein Prozess zur Einarbeitung von Neueinstellungen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Einarbeitung von Neueinstellungen.	Ja/Nein
		Führungskräfte	Es existiert ein schriftlich festgelegter Prozess zur Einarbeitung von Neueinstellungen.	Ja/Nein
		Mitarbeitende	Nach meiner Anstellung wurde ich systematisch in meine Aufgaben eingearbeitet.	Bewertungsskala
D (20)	Der Qualifikationsstand des Personals wird dokumentiert und ist für diejenigen, die es	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Dokumentation des Qualifikationsstandes des Personals.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	wissen müssen, leicht zugänglich.	Führungskräfte	Die Dokumentation zum Qualifikationsstand der Angestellten in meinem Verantwortungsbereich ist für mich leicht zugänglich.	Bewertungsskala
D (21)	Personal mit administrativen Aufgaben wird in die für sie relevanten technischen Details (IT-Systeme, Anwendungen, IT-Architektur, IT-Umgebung) eingewiesen.	Personal mit administrativen Aufgaben	Ich wurde in alle für mich/meine Arbeit relevanten technischen Details der verwendeten IT-Systeme eingewiesen.	Bewertungsskala
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Einweisung von Personal mit administrativen Aufgaben in die technischen Details der für deren Arbeit verwendeten IT-Systeme.	Ja/Nein
D (22)	Arbeitsaufgaben mit Bedeutung für die Informationssicherheit werden ausschließlich an Personen übertragen, die entsprechend geschult wurden.	Führungskräfte	Bei der Übertragung von Arbeitsaufgaben mit Bedeutung für die Informationssicherheit stellt die Qualifikation der Angestellten einen wesentlichen Entscheidungsfaktor dar.	Bewertungsskala
D (23)	Das Personal führt keine Tätigkeiten aus, für die ihm die erforderlichen Kenntnisse und Fähigkeiten fehlen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess, der sicherstellt, dass Tätigkeiten ausschließlich von hinreichend qualifiziertem Personal ausgeführt werden.	Ja/Nein
		Führungskräfte	Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	

Kriterium		Zielgruppe	Item	Art der Beantwortung
E (1)	Es gibt eine Leitlinie zur Informationssicherheit und zum Notfallmanagement.	Personen mit Kenntnis der internen Regelwerke und Prozesse	In der Organisation existiert eine Leitlinie für das Notfallmanagement in der Informationssicherheit.	Ja/Nein
E (2)	Es existiert eine geeignete Organisationsstruktur für das Notfallmanagement.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
E (3)	Das Notfallmanagement wird als zentraler Bestandteil angesehen. Die Mitglieder des Notfallmanagementteams werden in die Behandlung von Sicherheitsvorfällen eingebunden und über Störungs- und Fehlerbehebungen informiert wird.		Teilaspekte dieses Merkmals sind eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
		Mitglieder des Notfallmanagementteams	Ich wurde in ___ [Wochen/Monate/Jahre] in die Behandlung von ___ Sicherheitsvorfällen einbezogen.	Zahlenwert
E (4)	Sofortmaßnahmen und Notfallpläne werden regemäßig und anlassbezogen getestet und geübt, damit alle teilnehmenden Personen mit den Plänen und ihren Aufgaben vertraut sind. Zudem ist mit den Tests	Personen mit Kenntnis der internen Regelwerke und Prozesse	Notfallpläne werden durch Übungen getestet/geübt.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Übungen der Notfallpläne finden alle ___ [Wochen/Monate/Jahre] statt.	Zahlenwert

Kriterium		Zielgruppe	Item	Art der Beantwortung
	sicherzustellen, dass sie effektiv, aktuell sind und im zeitlichen Rahmen durchführbar sind.	Personen mit Beteiligung an internen Prüfungen	Notfallübungen werden ausgewertet, um deren Effektivität zu prüfen.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Notfallübungen werden ausgewertet, um deren Aktualität zu prüfen.	Ja/Nein
E (5)	Vorfälle werden der Aufsichtsbehörde gemeldet. • Das Personal und die Auftragnehmer sehen die Präsenz der Aufsichtsbehörde auf dem Betriebsgelände positiv. Der Betreiber informiert die Aufsichtsbehörde (oder eine andere einschlägige zuständige Behörde) auf der Grundlage der Ergebnisse der Selbstbewertung über den aktuellen Stand der Informationssicherheitskultur	Zuständige Personen bei der Aufsichtsbehörde	Die Organisation hat uns in ___ [Wochen/Monate/Jahre] ___ Sicherheitsvorfälle gemeldet.	Zahlenwert
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur regelmäßigen Information der Aufsichtsbehörde über die Ergebnisse der Selbstbewertung zur Informationssicherheitskultur.	Ja/Nein
		Führungskräfte	Es findet ein regelmäßiger Austausch mit der Aufsichtsbehörde über die Ergebnisse der Selbstbewertung zur Informationssicherheitskultur statt.	Ja/Nein oder Bewertungsskala
		Mitarbeitende	Die Präsenz der Aufsichtsbehörde auf dem Betriebsgelände empfinde ich als störend.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
E (6)	Es gibt eine festgelegte Vorgehensweise, nach der bei einer forensischen Untersuchung Datenquellen identifiziert und gesichert werden.	direkt an forensischen Untersuchungen Beteiligte	Es gibt eine festgelegte Vorgehensweise, nach der bei einer forensischen Untersuchung Datenquellen identifiziert und gesichert werden.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es gibt eine festgelegte Vorgehensweise, nach der bei einer forensischen Untersuchung Datenquellen identifiziert und gesichert werden.	Ja/Nein
		direkt an forensischen Untersuchungen Beteiligte	Bei forensischen Untersuchungen werden Daten nach folgenden Regeln identifiziert und gesichert:	Freitext oder Multiple Choice
E (7)	Datenträger werden dupliziert und voneinander getrennt aufbewahrt.	direkt an forensischen Untersuchungen Beteiligte	Datenträger werden dupliziert und voneinander getrennt aufbewahrt.	Ja/Nein
E (8)	Für die Beweissicherung wird ausschließlich geschultes und zuverlässiges Personal eingesetzt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Qualifikationsanforderungen an das für die Beweissicherung eingesetzte Personal.	Ja/Nein
		Führungskräfte	Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
E (9)	Es existieren Prozesse und Richtlinien, die die maximalen Verzögerungszeiten bei der	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Prozesse und Richtlinien, die die maximalen Verzögerungszeiten bei der Reparatur von IT-Systemen definieren.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Reparatur von IT-Systemen definieren und kontrollieren.			
E (10)	Das Personal leitet relevante Meldungen an die richtige Stelle weiter.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
E (11)	Ein Sicherheitsvorfall wird analysiert, um festzustellen, ob die Prozesse und Abläufe bei der Behandlung von Sicherheitsvorfällen korrigiert oder weiterentwickelt werden müssen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Analyse und Bewertung der Abläufe bei der Behandlung von Sicherheitsvorfällen.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Die Abläufe bei der Behandlung von Sicherheitsvorfällen werden regelmäßig analysiert und ggf. verbessert.	Ja/Nein oder Bewertungsskala
E (12)	Kleinere Vorfälle im Bereich der Informationssicherheit werden umgehend adressiert und Schutzmaßnahmen umgesetzt.	Personen mit Beteiligung an internen Prüfungen	Auch kleinere Sicherheitsvorfälle werden mit der gleichen Ernsthaftigkeit wie größere Vorfälle analysiert.	Ja/Nein oder Bewertungsskala
		Personen mit Beteiligung an internen Prüfungen	Abgeleitete Vorkehrungen gegen Wiederholung für kleinere Sicherheitsvorfälle werden zeitnah umgesetzt.	Ja/Nein oder Bewertungsskala
E (13)	Grundsätzlich sind Informationen aus zuverlässigen Quellen auszuwerten. Relevante	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Zuverlässigkeit von Quellen, die für	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Informationen sind entsprechend der Sicherheitsvorfallbehandlung zu bearbeiten.		die Behandlung von Sicherheitsvorfällen ausgewertet werden.	
		Personen mit Beteiligung an internen Prüfungen	Für die Behandlung von Sicherheitsvorfällen verwendete Quellen werden auf ihre Zuverlässigkeit geprüft.	Ja/Nein oder Bewertungsskala
E (14)	Der Erkenntnisgewinn über sicherheitsrelevante Ereignisse sollte auch (zuverlässige) externe Quellen miteinschließen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess, der die Einbeziehung verlässlicher externer Quellen zum Erkenntnisgewinn zu sicherheitsrelevanten Ereignissen festlegt.	Ja/Nein
E (15)	Alle beteiligen Personen bringen ihre Erfahrungen mit ein.	Führungskräfte	Die Angestellten in (Abteilung/Bereich) werden durch folgende Maßnahmen ermutigt, ihre Erfahrungen aktiv einzubringen:	Freitext oder Multiple Choice
		Mitarbeitende	Ich fühle mich ermutigt, meine Erfahrungen aktiv einzubringen.	Ja/Nein oder Bewertungsskala
E (16)	Wenn es neue Entwicklungen nach dem Stand von W&T gibt, sind diese in die Abläufe einzubringen (Hilfsmittel und Checklisten etc.).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Prozesse zur Integration neuer Entwicklungen des Standes von W&T in die Prozesse.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
F (1)	Es gibt schriftlich festgelegte Bewertungsprozesse (z.B. QS-Plan, Revisionen) für alle relevanten Aspekte der Informationssicherheit IT-Sicherung.	Personen mit Kenntnis der internen Regelwerke und Prozesse	In der Organisation existieren schriftlich festgelegte Bewertungsprozesse (z.B. QS-Plan, Revisionen) für alle relevanten Aspekte der Informationssicherheit	Ja/Nein oder Bewertungsskala
F (2)	Der Inhalt von QS-Plänen und Bewertungsprozessen ist dem Personal zugänglich und verständlich.	Mitarbeitende	Mir ist der Ablageort von QS-Plänen bekannt.	Ja/Nein oder Bewertungsskala
		Mitarbeitende	Die mir zugänglichen QS-Pläne sind für mich nachvollziehbar.	Ja/Nein oder Bewertungsskala
F (3)	Für Bewertungsprozesse wird geeignetes und ausreichend viel Personal ausgewählt.	Personal mit Beteiligung an internen Prüfungen	Die Arbeit bei der Durchführung von Bewertungsprozessen ist für mich bewältigbar.	Bewertungsskala
F (4)	Personen, die interne Bewertungen, Revisionen etc. durchführen, arbeiten unabhängig und objektiv.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Unabhängigkeit von Personen, die interne Prüfungen durchführen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Eine Überprüfung der Unabhängigkeit von Personen, die interne Prüfungen durchführen, findet alle ___ [Monate/Jahre] statt	Zahlenwert
		Personen mit Beteiligung an internen Prüfungen	Objektivität ist bei der Durchführung von internen Prüfungen von hoher Bedeutung.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
F (5)	Die Rollenverteilung im Bewertungsprozess ist eindeutig.	Personen mit Beteiligung an internen Prüfungen	Die Rollenverteilung bei der Durchführung von internen Prüfungen ist eindeutig.	Bewertungsskala
		Führungskräfte	Die Rollenverteilung bei der Durchführung von internen Prüfungen ist eindeutig.	Bewertungsskala
		Mitarbeitende	Die Rollenverteilung bei der Durchführung von internen Prüfungen ist eindeutig.	Bewertungsskala
F (6)	Die Bewertungsprozesse werden eingehalten.	Personen mit Beteiligung an internen Prüfungen	Bei Überprüfungen der Einhaltung der schriftlich festgelegten Bewertungsprozesse werden im Schnitt ___ Verstöße pro Überprüfung festgestellt.	Zahlenwert
F (7)	Die Einhaltung der Bewertungsprozesse wird regelmäßig und fortlaufend überprüft.	Personen mit Beteiligung an internen Prüfungen	Eine Überprüfung der Einhaltung der schriftlich festgelegten Bewertungsprozesse findet alle ___ [Monate/Jahre] statt.	Zahlenwert
F (8)	Es gibt einen Revisionsplan (d.h. eine Zeitplanung, wann welche Revisionen durchzuführen sind), der fortlaufend gepflegt wird.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein Revisionsplan (d.h. eine Zeitplanung, wann welche Revisionen durchzuführen sind), der fortlaufend gepflegt wird.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Es existiert ein Revisionsplan (d.h. eine Zeitplanung, wann welche Revisionen durchzuführen sind), der fortlaufend gepflegt wird.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
F (9)	Bei der Durchführung von internen Bewertungsprozessen wird Wert auf offene und transparente Kommunikation gelegt.	Personen mit Beteiligung an internen Prüfungen	Eine offene und transparente Kommunikation ist bei der Durchführung von internen Bewertungsprozessen von großer Bedeutung.	Bewertungsskala
		Führungskräfte	Eine offene und transparente Kommunikation ist bei der Durchführung von internen Bewertungsprozessen von großer Bedeutung.	Bewertungsskala
		Mitarbeitende	Eine offene und transparente Kommunikation ist bei der Durchführung von internen Bewertungsprozessen von großer Bedeutung.	Bewertungsskala
F (10)	Es steht ausreichend viel Zeit zur Vor- und Nachbereitung von Bewertungsprozessen (Revisionen, Interviews, …) zur Verfügung.	Personen mit Beteiligung an internen Prüfungen	Für die Vorbereitung von Bewertungsprozessen steht ausreichend viel Zeit zur Verfügung.	Bewertungsskala
F (11)	Zwischen Revisionsteam und zu prüfender Institution/Abteilung/etc. findet im Vorfeld eine Kommunikationsabsprache statt.	Personen mit Beteiligung an internen Prüfungen	Vor der Durchführung einer internen Bewertung findet eine Kommunikationsabsprache mit allen Beteiligten statt.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Vor der Durchführung einer internen Bewertung findet eine Kommunikationsabsprache mit allen Beteiligten statt.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Mitarbeitende	Vor der Durchführung einer internen Bewertung findet eine Kommunikationsabsprache mit allen Beteiligten statt.	Ja/Nein oder Bewertungsskala
F (12)	Die Durchführung von Interviews zu Bewertungszwecken folgt einem festen Schema und wird aufgezeichnet.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert eine schriftlich festgelegte Vorgehensweise für die Durchführung von Interviews zu Bewertungszwecken.	Ja/Nein
F (13)	In regelmäßig durchgeführten Besprechungen des Managements werden auch Aspekte der Informationssicherheit adressiert. Hierbei werden auch regulatorische und unabhängige externe Bewertungen diskutiert.	Führungskräfte	In regelmäßig durchgeführten Besprechungen des Managements werden auch Aspekte der Informationssicherheit adressiert.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Bei der Besprechung des Managements zu Aspekten der Informationssicherheit werden auch regulatorische Aspekte diskutiert.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Bei der Besprechung des Managements zu Aspekten der Informationssicherheit werden auch unabhängige externe Bewertungen diskutiert.	Ja/Nein oder Bewertungsskala
F (14)	Es erfolgen Vergleiche mit bewährten Praktiken im nationalen und internationalen Umfeld,	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zum Vergleich der eigenen Prozesse und Prüfmethoden mit dem nationalen/internationalen Stand von W&T	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	um die eigenen Prozesse und Prüfmethoden an dem Stand von Wissenschaft und Technik auszurichten und zu aktualisieren.	Personen mit Beteiligung an internen Prüfungen	Die bei der Durchführung von internen Prüfungen angewendeten Methoden wurden zuletzt ___ an den Stand von W&T angepasst.	Zahlenwert
F (15)	Wird eine sich systematisch verschlechternde Qualität festgestellt, werden Ursachen und Strategien zur Verbesserung ermittelt.	Personen mit Beteiligung an internen Prüfungen	Es existiert ein schriftlich festgelegter Prozess zur Ursachenermittlung von Qualitätsverlusten.	Ja/Nein
G (1)	Es existiert ein Änderungsmanagementprozess, der in die Geschäftsprozesse der Organisation integriert ist und die Auswirkungen von Änderungen auf die Geschäftsprozesse berücksichtigt. Vor der Änderung oder Beschaffung von Hardware oder Software werden insbesondere die menschlichen Faktoren berücksichtigt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Änderungsmanagementprozess.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Der schriftlich festgelegte Änderungsmanagementprozess berücksichtigt Auswirkungen von Änderungen auf die Geschäftsprozesse der Organisation.	Ja/Nein oder Bewertungsskala
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Berücksichtigung menschlicher Faktoren vor der Beschaffung von Hardware/Software.	Ja/Nein
G (2)	Für die Werkzeuge des Patch- und Änderungsmanagements	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert eine schriftlich festgelegte Sicherheitsrichtlinie für die Werkzeuge des Patch- und Änderungsmanagements.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	existiert eine Sicherheitsrichtlinie.	IT-Fachpersonal	Es existiert eine schriftlich festgelegte Sicherheitsrichtlinie für die Werkzeuge des Patch- und Änderungsmanagements.	Ja/Nein
G (3)	Es gibt feste Anforderungen und Rahmenbedingungen, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt werden.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Anforderungen für die Auswahl der Werkzeuge für das Patch- und Änderungsmanagement.	Ja/Nein
		IT-Fachpersonal	Die Auswahl der Werkzeuge für das Patch- und Änderungsmanagement erfolgt nach festen Regeln.	Ja/Nein oder Bewertungsskala
G (4)	Es gibt ein standardisiertes Verfahren, durch das Änderungsanforderungen hoher Wichtigkeit beschleunigt werden.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Beschleunigung von Änderungsanforderung hoher Wichtigkeit.	Ja/Nein
		IT-Fachpersonal	Änderungsanforderungen von hoher Wichtigkeit werden als solche gekennzeichnet.	Ja/Nein
		IT-Fachpersonal	Änderungsanforderungen von hoher Wichtigkeit werden priorisiert bearbeitet.	Ja/Nein oder Bewertungsskala
G (5)	Alle Änderungsanforderungen werden zentral erfasst und dokumentiert.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die zentrale Erfassung von Änderungsanforderungen.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Dokumentation von Änderungsanforderungen.	Ja/Nein
		IT-Fachpersonal	Alle Änderungsanforderungen werden zentral erfasst.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Alle Änderungsanforderungen werden dokumentiert.	Ja/Nein oder Bewertungsskala
G (6)	Änderungsanforderungen werden vom Fachverantwortlichen für das Patch- und Änderungsmanagement darauf kontrolliert, ob die Aspekte der Informationssicherheit IT-Sicherung ausreichend berücksichtigt wurden.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Berücksichtigung von Aspekten der Informationssicherheit bei Änderungsanforderungen.	Ja/Nein
		IT-Fachpersonal	Änderungsanforderungen werden darauf kontrolliert, ob sie Aspekte der Informationssicherheit berücksichtigen.	Ja/Nein oder Bewertungsskala
G (7)	Änderungsanforderungen werden mit allen relevanten Zielgruppen abgestimmt und potenzielle Auswirkungen auf die Informationssicherheit IT-Sicherung berücksichtigt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Abstimmung von Änderungsanforderungen und deren potenziellen Auswirkungen auf die Informationssicherheit mit allen relevanten Zielgruppen.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Änderungsanforderungen werden mit allen relevanten Zielgruppen abgestimmt.	Ja/Nein, Bewertungsskala,

Kriterium		Zielgruppe	Item	Art der Beantwortung
				Multiple Choice oder Freitext
		IT-Fachpersonal	Bei der Abstimmung von Änderungsanforderungen mit den relevanten Zielgruppen werden potenzielle Auswirkungen auf die Informationssicherheit berücksichtigt.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
G (8)	Bevorstehende Änderungen werden in Umfang und Art proaktiv und offen kommuniziert. Dabei werden sowohl unmittelbar als auch mittelbar Betroffene einbezogen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Kommunikation bevorstehender Änderungen (Hardware/Software) an das Personal.	Ja/Nein
		Führungskräfte	Bevorstehende Änderungen von Hardware oder Software werden den unmittelbar Betroffenen frühzeitig mitgeteilt.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Bevorstehende Änderungen von Hardware oder Software werden den mittelbar Betroffenen frühzeitig mitgeteilt.	Ja/Nein oder Bewertungsskala
		Mitarbeitende	Bevorstehende Änderungen von Hardware oder Software werden mir im Vorfeld mitgeteilt, sodass ich genug Zeit habe, mich darauf einzustellen.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Bevorstehende Änderungen von Hardware oder Software werden den unmittelbar Betroffenen frühzeitig mitgeteilt.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
		IT-Fachpersonal	Bevorstehende Änderungen von Hardware oder Software werden den mittelbar Betroffenen frühzeitig mitgeteilt.	Ja/Nein oder Bewertungsskala
G (9)	Neue Hardware inkl. Der zugehörigen Treibersoftware wird vor dem Einsatz auf Kompatibilität mit der eingesetzten Software und den relevanten Betriebssystemen geprüft.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Kompatibilität neuer Hardware (einschließlich Treibersoftware) mit der verwendeten Software.	Ja/Nein
		IT-Fachpersonal	Neue Hardware (einschließlich Treibersoftware) wird vor der Verwendung auf Kompatibilität mit der verwendeten Software überprüft.	Ja/Nein oder Bewertungsskala
G (10)	Neue Hard- und Software wird vor dem Einsatz nach einem standardisierten Abnahme- und Freigabeverfahren getestet.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Abnahme und Freigabe neuer Hardware vor dem Einsatz.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Abnahme und Freigabe neuer Software vor dem Einsatz.	Ja/Nein
		IT-Fachpersonal	Neue Hardware durchläuft vor dem Einsatz einen standardisierten Abnahme- und Freigabeprozess.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Neue Software durchläuft vor dem Einsatz einen standardisierten Abnahme- und Freigabeprozess.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
G (11)	Die Authentizität und Integrität von Softwarepaketen wird während des gesamten Patch- und Änderungsprozesses anhand von Prüfsummen oder digitalen Signaturen überprüft.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Authentizität von Softwarepaketen während des gesamten Patch- und Änderungsprozesse anhand von Prüfsummen oder digitalen Signaturen.	Ja/Nein oder Bewertungsskala
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Überprüfung der Integrität von Softwarepaketen während des gesamten Patch- und Änderungsprozesse anhand von Prüfsummen oder digitalen Signaturen.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Die Authentizität von Softwarepaketen wird während des gesamten Patch- und Änderungsprozesses anhand von Prüfsummen oder digitalen Signaturen überprüft.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Die Integrität von Softwarepaketen wird während des gesamten Patch- und Änderungsprozesses anhand von Prüfsummen oder digitalen Signaturen überprüft.	Ja/Nein oder Bewertungsskala
H (1)	Die Email-basierte Kommunikation erfolgt gemäß den internen Regelungen (kein Zugriff von öffentlich zugänglichen IT-Systemen auf Emails etc.).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegtes Regelwerk für die Kommunikation per E-Mail.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Die Einhaltung der Kommunikationsregeln für E-Mails wird alle ___ [Wochen/Monate/Jahre] geprüft.	Zahlenwert

Kriterium		Zielgruppe	Item	Art der Beantwortung
H (2)	Die Regelungen für die Email-basierte Kommunikation orientieren sich am Stand von W&T (Verwendung kryptographischer Verfahren, Sicherheitsmechanismen beim Provider von Email-Diensten etc.).	Personen mit Beteiligung an internen Prüfungen	Die Regelungen zur E-Mail-basierten Kommunikation werden alle ___ [Wochen/Monate/Jahre] mit dem Stand von W&T abgeglichen.	Zahlenwert
H (3)	Für den sicheren Umgang mit Informationen (auf Dienstreisen) existieren feste Vorgehensweisen und Regelungen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegtes Regelwerk für den Umgang mit Informationen innerhalb der Organisation.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegtes Regelwerk für den Umgang mit Informationen auf Dienstreisen.	Ja/Nein
H (4)	Dem Personal sind alle relevanten Vorgehensweisen und Regelungen zum sicheren Umgang mit Informationen (auf Dienstreisen) bekannt.	Mitarbeitende	Für den sicheren Umgang mit Informationen innerhalb der Organisation sind folgende wesentliche Grundsätze zu beachten:	Multiple Choice oder Freitext
		Mitarbeitende	Für den sicheren Umgang mit Informationen auf Dienstreisen sind folgende wesentliche Grundsätze zu beachten:	Multiple Choice oder Freitext
H (5)	Das Personal hält die Regeln zum sicheren Umgang mit	Mitarbeitende	Die Einhaltung der Regeln für den sicheren Umgang mit Informationen hat für mich auf Dienstreisen stets höchste Priorität.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Informationen auf Dienstreisen eigenverantwortlich ein.	Führungskräfte	Mitarbeiter werden vor jeder Dienstreise auf die Einhaltung der Regeln für den sicheren Umgang mit Informationen auf Dienstreisen aufmerksam gemacht.	Ja/Nein oder Bewertungsskala
H (6)	Vor Auslandsreisen werden mögliche länderspezifische Regelungen identifiziert.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Identifikation von länderspezifischen Regelungen bei Auslandsreisen.	Ja/Nein
		Mitarbeitende	Vor jeder Dienstreise ins Ausland spreche ich mit meinem Vorgesetzten ab, ob es zu beachtende länderspezifische Regelungen gibt.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
		Führungskräfte	Vor jeder Dienstreise ins Ausland frage ich beim betreffenden Mitarbeiter/in ab, ob es zu beachtende länderspezifische Regelungen zu beachten gilt.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
H (7)	Das Personal teilt bevorstehende (Auslands-) Reisen rechtzeitig dem Vorgesetzten sowie Verantwortlichen Personen bzgl. Informationssicherheit mit.	Mitarbeitende	Eine bevorstehende Dienstreise teile ich meinem Vorgesetzten in der Regel ___ [Wochen/Monate] vorher mit.	Zahlenwert
		Mitarbeitende	Bei Bedarf teile ich eine bevorstehende Dienstreise dem IT-Fachpersonal ___ [Wochen/Monate] vorher mit.	Zahlenwert

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Führungskräfte	Dienstreisen in [Abteilung, Bereich] müssen mir mindestens ___ [Wochen/Monate] vorher mitgeteilt werden.	Zahlenwert
		IT-Fachpersonal	Angestellte, die vor einer Dienstreise Bedarf für Unterstützung durch das IT-Fachpersonal haben, teilen dies ausreichend lange vorher mit.	Ja/Nein oder Bewertungsskala
H (8)	Der sichere Umgang mit Informationen auf (Auslands-)Reisen wird von Führungskräften regelmäßig betont und überprüft. Dies beinhaltet: • Sicherer Umgang mit mobilen Datenträgern • Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten • Verwendung von Sichtschutzfolien • Sicherstellung der Abstrahlsicherheit • Verwendung von Diebstahlsicherungen • Verschlüsselung tragbarer IT-Systeme und Datenträger	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Regelungen, die Führungskräfte dazu verpflichten, die Wichtigkeit des sicheren Umgangs mit Informationen auf Reisen zu betonen.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Führungskräfte werden alle ___ [Wochen/Monate] darauf überprüft, ob sie ihrer Verpflichtung, die Wichtigkeit des sicheren Umgangs mit Informationen auf Reisen zu betonen, nachkommen.	Zahlenwert
		Führungskräfte	Ich betone die Wichtigkeit des sicheren Umgangs mit Informationen auf Reisen auf folgende Weise(n):	Multiple Choice oder Freitext

Kriterium		Zielgruppe	Item	Art der Beantwortung
	• Umgehendes Melden von Diebstahl oder Verlust von Informationen, IT-Systemen oder Datenträgern			
H (9)	Der Zugang zu Informationen ist auf diejenigen beschränkt, die diesen Zugang zur Erfüllung ihrer Aufgaben benötigen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Regelungen für die Zugangsberechtigungen zu Informationen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Die schriftlich festgelegten Regelungen für die Zugangsberechtigungen zu Informationen sehen vor, dass Informationen nur denen zugänglich sind, die diese für die Erfüllung ihrer Aufgaben benötigen (Need-to-know-Prinzip).	Ja/Nein
		Führungskräfte	Zugangsberechtigungen zu Informationen werden nach dem folgenden Prinzip vergeben:	Multiple Choice oder Freitext
H (10)	Der Zugang zu Informationen ist durch Zugriffskontroll- und Authentisierungsmechanismen und Identifikation zu verifizieren.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess, der den Zugriff auf Informationen durch Zugriffskontroll-Authentisierungs- und Identifikationsmechanismen regelt.	Ja/Nein
		Führungskräfte	Der Zugriff zu sensiblen Daten ist durch folgende Mechanismen geschützt:	Multiple Choice oder Freitext

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Mitarbeitende	Der Zugriff zu sensiblen Daten ist durch folgende Mechanismen geschützt:	Multiple Choice oder Freitext
H (11)	Die Qualität dieser Zugriffs-, Authentisierungs- und Identifikationsmechanismen ist festzulegen. (Mehr-Faktor Authentifizierung bei weitreichenden Berechtigungen, Zurücksetzen von Passwörtern, Änderung von Passwörtern nach Sicherheitsvorfällen etc.).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Qualitätsanforderungen an die Mechanismen zur Einschränkung des Zugangs zu Informationen.	Ja/Nein
		IT-Fachpersonal	Für die Einschränkung des Zugangs zu Informationen genutzten Mechanismen gelten folgende Qualitätsanforderungen:	Multiple Choice oder Freitext
H (12)	Der Passwortgebrauch ist genau festgelegt und das Personal kennt alle Regeln im Umgang mit Passwörtern.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Regeln für den Passwortgebrauch.	Ja/Nein
		IT-Fachpersonal	Für den Passwortgebrauch gelten folgende Grundregeln:	Multiple Choice oder Freitext
		Mitarbeitende	Für den Passwortgebrauch gelten folgende Grundregeln:	Multiple Choice oder Freitext
H (13)	Es gibt (dokumentierte) Zutrittsberechtigungen (z.B. mit Chipkarten), die auf diejenigen	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Dokumentation von Zutrittsberechtigungen.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	beschränkt sind, die Zutritt benötigen.	IT-Fachpersonal	Die Dokumentation von Zutrittsberechtigungen wird alle ___ [Wochen/Monate] aktualisiert.	Zahlenwert
H (14)	Es gibt klare und wirksame Verfahren und Protokolle für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Der Prozess für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation wird alle ___ [Wochen/Monate] auf seine Wirksamkeit überprüft.	Zahlenwert
		IT-Fachpersonal	Für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation werden folgende Verfahren verwendet:	Multiple Choice oder Freitext
H (15)	Verschlusssachen werden sicher abgetrennt, gespeichert und verwaltet.		Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	
H (16)	Unternehmen und Organisationen sollten über Systeme, Prozesse und Kompetenz haben, um allen Mitarbeitern Informationen über Bedrohungen auf ihre Sicherheitsfreigabe und ihre Rolle zugeschnitten sind.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Information der Angestellten über Bedrohungen und Risiken in Bezug auf IT-Systeme.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Die den Angestellten bereitgestellten Informationen über Bedrohungen und Risiken sind auf deren Rolle und Sicherheitsfreigabe zugeschnitten.	Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Sie sollten auch über ein ein effektives Sicherheitsrisikoregister und ein System zur Kommunikation von Risiken haben; Diese Risiken sollten auch in die Ausbildung und Entwicklung einfließen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Die Informationen zu Bedrohungen und Risiken fließen in die Ausbildung und Entwicklung von Angestellten mit ein.	Ja/Nein oder Bewertungsskala
		IT-Fachpersonal	Angestellte werden auf den folgenden Wegen über Bedrohungen und Risiken in Bezug auf IT-Systeme informiert:	Multiple Choice oder Freitext
H (17)	Die Bedeutung von Vertraulichkeit und Integrität von gesicherten Daten/Informationen ist bekannt und die Daten werden mit technischen Maßnahmen (z.B. Kryptografie) so gesichert, dass ihre Vertraulichkeit und Integrität gewahrt wird.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Sicherung von Daten.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Die zur Sicherung von Daten genutzten technischen Maßnahmen werden alle ___ [Wochen/Monate] auf ihre Wirksamkeit (Vertraulichkeit der Daten) geprüft.	Zahlenwert
		Personen mit Beteiligung an internen Prüfungen	Die zur Sicherung von Daten genutzten technischen Maßnahmen werden alle ___ [Wochen/Monate] auf ihre Wirksamkeit (Integrität der Daten) geprüft.	Zahlenwert
H (18)	Daten/Informationen sind wertvoll und müssen vor Verlust geschützt werden (z.B. Gewährleistung der Wiederherstellbarkeit).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existieren schriftlich festgelegte Anforderungen an die Datensicherung, die die Wiederherstellbarkeit fordern.	Ja/Nein
		Mitarbeitende	Daten/Informationen sind wertvoll und müssen vor Verlust geschützt werden.	Ja/Nein oder Bewertungsskala

Kriterium		Zielgruppe	Item	Art der Beantwortung
		IT-Fachpersonal	Zur Gewährleistung der Wiederherstellbarkeit von Daten/Informationen werden folgende Werkzeuge genutzt:	Multiple Choice oder Freitext
H (19)	Benutzer kennen die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien und wissen, wie man unerwünschte Restinformationen ausschließt (z.B. vor Weitergabe).	Mitarbeitende	Ich kenne das Risiko durch Restinformationen auf Datenträgern.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
		Mitarbeitende	Unerwünschte Restinformationen auf Datenträgern werden durch folgende Maßnahmen vermieden:	Multiple Choice oder Freitext
K (1)	Führungskräfte leben vorbildhaftes, sicherungsbezogenes Verhalten in Worten und Taten vor.	Mitarbeitende	Das Verhalten meines Vorgesetzten/meiner Vorgesetzten nehme ich als vorbildlich wahr.	Ja/Nein oder Bewertungsskala
K (2)	Führungskräfte machen das Personal für ihr Verhalten verantwortlich.	Mitarbeitende	Mein Vorgesetzter/meine Vorgesetzte betonen die Eigenverantwortung jedes Einzelnen für sein Handeln.	Ja/Nein oder Bewertungsskala
K (3)	Fehler können auch gegenüber höherrangigem Personal benannt werden.	Mitarbeitende	Auch gegenüber Vorgesetzten können Fehler angesprochen werden.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Dieses Merkmal ist eher über andere Methoden als Befragung zu ermitteln (z.B. Beobachtung).	

Kriterium		Zielgruppe	Item	Art der Beantwortung
K (4)	Vorbildliches Verhalten wird hervorgehoben und honoriert. Vorsätzliche Nichteinhaltungen von Regeln werden in angemessener Weise sanktioniert. Dabei sind die unterschiedliche Wirkung von Sanktionen und Belohnung auf verschiedene Charaktere sowie die Vor- und Nachteile der verwendeten Methoden zu beachten (z.B. Verschlechterung der Beziehung und Kommunikation zum Vorgesetzten bei Anwendung von Sanktionsmethoden).	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Sanktionierung der vorsätzlichen Nichteinhaltung von Regeln.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Belohnung vorbildlichen Verhaltens.	Ja/Nein
		Führungskräfte	Bei der Sanktionierung vorsätzlicher Nichteinhaltungen der Regeln wird mir ein angemessener Entscheidungsspielraum gewährt.	Bewertungsskala
		Führungskräfte	Bei der Sanktionierung vorsätzlicher Nichteinhaltungen der Regeln berücksichtige ich die unterschiedliche Wirkung auf unterschiedliche Charaktere.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
		Mitarbeitende	Ich fühle mich durch Belohnungen zu vorbildlichem Verhalten motiviert.	Ja/Nein oder Bewertungsskala
		Mitarbeitende	Ich fühle mich durch Schulungen und kontinuierliche Anreize motiviert	Ja/Nein oder Bewertungsskala
L (1)	Die Organisation verfügt über schriftliche Richtlinien, Regeln	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess für die Einstellung neuer Mitarbeiter/innen.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	und Verfahren für die Einstellung von Mitarbeitern.	Führungskräfte	Die Einstellung neuer Mitarbeiter/innen folgt (den folgenden) festen Regeln.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
L (2)	Es gibt ein wirksames Programm zur Eindämmung von Innentäter-Bedrohungen, das zwischen allen Bereichen der Sicherheits- und Betriebsorganisationen koordiniert wird.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Eindämmung von Innentäter-Bedrohungen.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Der Prozess zur Eindämmung von Innentäter-Bedrohungen wird zwischen allen Bereichen der Sicherheits- und Betriebsorganisationen koordiniert.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
		Personen mit Beteiligung an internen Prüfungen	Der Prozess zur Eindämmung von Innentäter-Bedrohungen wird alle ___ [Wochen/Monate/Jahre] auf seine Wirksamkeit überprüft.	Zahlenwert
		Führungskräfte	Der Prozess zur Eindämmung von Innentäter-Bedrohungen wird mit den anderen Abteilungen/Bereichen abgestimmt/koordiniert.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
L (3)	Die Vertrauenswürdigkeit des Personals wird bei der Einstellung und danach in	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Prüfung der Vertrauenswürdigkeit des Personals.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	regelmäßigen Abständen nach einem standardisierten Verfahren überprüft. Das Verfahren zur Feststellung der Vertrauenswürdigkeit ist in der Lage, spezifische Risikofaktoren zu erkennen, z. B. psychische Erkrankungen und Drogen-/Alkoholmissbrauch.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Der Prozess zur Prüfung der Vertrauenswürdigkeit des Personals beinhaltet sowohl die Überprüfung von Neueinstellungen als auch die regelmäßige Überprüfung nach der Einstellung.	Ja/Nein, Bewertungsskala, Multiple Choice oder Freitext
		Personen mit Beteiligung an internen Prüfungen	Der Prozess zur Überprüfung der Vertrauenswürdigkeit des Personals ist in der Lage, psychische Erkrankungen zuverlässig festzustellen.	Ja/Nein oder Bewertungsskala
		Personen mit Beteiligung an internen Prüfungen	Der Prozess zur Überprüfung der Vertrauenswürdigkeit des Personals ist in der Lage, Alkohol-/Drogenmissbrauch zuverlässig festzustellen.	Ja/Nein oder Bewertungsskala
		Führungskräfte	Die Vertrauenswürdigkeit der Angestellten wird alle ___ [Monate/Jahre] überprüft.	Zahlenwert
L (4)	Soll einem Mitarbeiter der Zutritt zu Hochsicherheitsbereichen oder der Zugriff zu hochsensiblen Daten gewährt werden, wird eine gesonderte Prüfung der Vertrauenswürdigkeit durchgeführt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur gesonderten Überprüfung der Vertrauenswürdigkeit von Mitarbeitern, denen der Zugang zu Hochsicherheitsbereichen gewährt werden soll.	Ja/Nein
		Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur gesonderten Überprüfung der Vertrauenswürdigkeit von Mitarbeitern, denen der Zugriff auf hochsensible Daten gewährt werden soll.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
		Personen mit Beteiligung an internen Prüfungen	Zugangsschlüssel zu Hochsicherheitsbereichen werden nur denjenigen Angestellten mit einer positiv durchgeführten Sonderprüfung der Vertrauenswürdigkeit zur Verfügung gestellt.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Zugangsschlüssel zu hochsensiblen Daten werden nur denjenigen Angestellten mit einer positiv durchgeführten Sonderprüfung der Vertrauenswürdigkeit zur Verfügung gestellt.	Ja/Nein
		Führungskräfte	Zugangsschlüssel zu Hochsicherheitsbereichen werden nur denjenigen Angestellten mit einer positiv durchgeführten Sonderprüfung der Vertrauenswürdigkeit zur Verfügung gestellt.	Ja/Nein
		Führungskräfte	Zugangsschlüssel zu hochsensiblen Daten werden nur denjenigen Angestellten mit einer positiv durchgeführten Sonderprüfung der Vertrauenswürdigkeit zur Verfügung gestellt.	Ja/Nein
L (5)	Es gibt eine standardisierte Vorgehensweise zur Koordination mit Dienstleistern und Auftragnehmern bezüglich der	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Koordination mit Dienstleistern und Auftragnehmern bezüglich der Vertrauenswürdigkeit von deren Angestellten.	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	Vertrauenswürdigkeit von deren Angestellten.	Personen mit Beteiligung an internen Prüfungen	Die Prüfung der Vertrauenswürdigkeit von Fremdpersonal folgt einer standardisierten Vorgehensweise.	Ja/Nein
		Führungskräfte	Bevor Fremdpersonal zum Einsatz kommt, findet mit dessen Arbeitgeber eine Abstimmung bezüglich seiner Vertrauenswürdigkeit statt.	Ja/Nein
L (6)	Es werden schriftliche Vereinbarungen zur Vertrauenswürdigkeit von Angestellten mit Dienstleistern und Auftragnehmern geschlossen.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Mit Dienstleistern und Auftragnehmern werden schriftliche Vereinbarungen bezüglich der Vertrauenswürdigkeit von deren Personal getroffen.	Ja/Nein
		Führungskräfte	Mit Dienstleistern und Auftragnehmern werden schriftliche Vereinbarungen bezüglich der Vertrauenswürdigkeit von deren Personal getroffen.	Ja/Nein
L (7)	Bei Arbeiten und Tätigkeiten mit Bedeutung für die Informationssicherheit wird stets das 2-Personen-Prinzip angewendet.	Führungskräfte	Arbeiten und Tätigkeiten mit Bedeutung für die Informationssicherheit werden stets nach dem 2-Personen-Prinzip durchgeführt.	Ja/Nein, Multiple Choice oder Freitext
		Mitarbeitende	Arbeiten und Tätigkeiten mit Bedeutung für die Informationssicherheit werden stets nach dem 2-Personen-Prinzip durchgeführt.	Ja/Nein, Multiple Choice oder Freitext
L (8)	Führungspositionen und weitere für die Informationssicherheit bedeutsame Positionen	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur Prüfung der Vertrauenswürdigkeit von Kandidaten auf Führungspositionen und weitere für die	Ja/Nein

Kriterium		Zielgruppe	Item	Art der Beantwortung
	(z.B. Administrator) werden erst nach einer Prüfung der Vertrauenswürdigkeit der Kandidaten besetzt.		Informationssicherheit bedeutsame Positionen (z.B. Administrator).	
		Führungskräfte	Führungspositionen und weitere für die Informationssicherheit bedeutsame Positionen (z.B. Administrator) werden erst nach einer Prüfung der Vertrauenswürdigkeit der Kandidaten besetzt.	Ja/Nein, Multiple Choice oder Freitext
L (9)	Personalbewertungen finden regelmäßig und unabhängig von der Hierarchieebene statt.	Personen mit Kenntnis der internen Regelwerke und Prozesse	Es existiert ein schriftlich festgelegter Prozess zur regelmäßigen Überprüfung aller Angestellten unabhängig von deren Hierarchieebene.	Ja/Nein
		Personen mit Beteiligung an internen Prüfungen	Personalbewertungen finden alle ___ [Monate/Jahre] statt.	Zahlenwert
		Personen mit Beteiligung an internen Prüfungen	Personalbewertungen sind unabhängig von der Hierarchieebene verpflichtend.	Ja/Nein

4 Zusammenfassung und Ausblick

Die Bedeutung der Sicherungskultur für die Wirksamkeit von Sicherungsmaßnahmen wird seit einigen Jahren verstärkt diskutiert. Vor dem Hintergrund des verstärkten Einsatzes von IT-Systemen in deutschen kerntechnischen Anlagen sowie den Erfahrungen aus Angriffen mit Schadsoftware auf IT-Systeme und industrielle Steuerungssysteme von kritischen Infrastrukturen sind die Erstellung und Umsetzung von IT-Sicherheitskonzepten und eine hohe Sicherungskultur auch für die Informationstechnologie entscheidende Einflussfaktoren, die sich auf das Sicherungs- und Sicherheitsniveau von kerntechnischen Anlagen und Einrichtungen auswirken. Neben gezielten Angriffen auf IT-Systeme und industrielle Steuerungsanlagen besteht zudem das Risiko, dass Schadsoftware unbeabsichtigt und unentdeckt durch Mitarbeiter der Organisation eingebracht wird.

In diesem Vorhaben wurde die Fragestellung der Umsetzung von bewährten Vorgehensweisen zur Schaffung einer hohen Sicherungskultur im Hinblick auf die Informationssicherheit vertieft untersucht, wobei auch die Schnittstelle zur Sicherheitskultur betrachtet wurde. Hierfür wurde zunächst der Stand von Wissenschaft und Technik zu nationalen und internationalen Anforderungen an und Merkmalen von Sicherungskultur ermittelt. Aspekte sowie relevante Anforderungen und Merkmale, die die Informationssicherheitskultur betreffen, wurden herausgearbeitet. Basierend darauf wurde eine Liste von Kriterien, anhand derer Verbesserungspotential in der Informationssicherheitskultur aufgedeckt werden können, erarbeitet. Abschließend wurde ein Fragebogen entwickelt, der z.B. im Rahmen von Selbsteinschätzungen oder Audits zur Überprüfung der Informationssicherheitskultur genutzt werden kann.

Zusammen mit den in diesem Vorhaben erarbeiteten Kriterien einer guten Informationssicherheitskultur wurden die Aspekte der Sicherheits- und der Sicherungskultur vergleichend dargestellt. Dieser Vergleich zeigt, dass einige Kriterien in allen Kulturfacetten zum Tragen kommen, jedoch oft unterschiedliche Formulierungen verwendet werden. Auch werden in manchen Kulturfacetten Aspekte adressiert, die in den anderen Kulturfacetten ebenfalls zur Anwendung kommen können, dort, jedoch nicht adressiert werden. Diese uneinheitliche Herangehensweise macht es einem Anwender (Betreiber oder Behörde) schwer, die Anforderungen aller Kulturfacetten zu erfüllen. Aufbauend auf den Ergebnissen dieses Vorhabens könnte eine Zusammenführung und Vereinheitlichung der verschiedenen Kriterien zu einem einzigen Kriterienkatalog mit spezifischen

Aspekten, die nur für jeweils eine der Kulturfacetten relevant ist, zu einer Vereinfachung der Situation führen.

Darüber hinaus hat die Entwicklung des Fragenkatalogs gezeigt, dass es nicht möglich ist, alle Kriterien für eine gute Informationssicherheitskultur ausschließlich über einen Fragenkatalog zu untersuchen. Auch findet man in der KTA 1402 die Empfehlung, dass man zur Beurteilung der Sicherheitskultur, die Nutzung quantitativer (z. B. Mitarbeiterumfragen) und qualitativer Bewertungsmethoden (z.B. Beobachtungen, Einzelgespräche) kombinieren soll. Ziel der Methodenvielfalt bei der Erfassung der Sicherheitskultur ist es, mit den Stärken einer Vorgehensweise die Schwächen einer anderen auszugleichen. Dieser Bedarf an methodischer Vielfalt wurde auch aus der Praxis im Zuge des Behördenseminars zur Sicherheitskultur 2021 von den Teilnehmenden geäußert, um einen aussagekräftigen Eindruck zur Sicherheitskultur im Unternehmen zu erhalten. Aufbauend auf den Ergebnissen dieses Vorhabens wäre es daher zielführend, auch für die Ermittlung der Informationssicherheitskultur verschiedene Methoden anzuwenden.

A Matrix der Charakteristika, Attribute, Indikatoren und Kriterien der Sicherheitskultur und Sicherungskultur nach IAEA sowie der Informationssicherheitskultur nach IT-Grundschutz des BSI und IAEA

In der Sicherheitskultur nach IAEA GS-G-3.5 /IAE 09/ werden folgende Charakteristika verwendet, denen die verschiedenen Attribute zugeordnet werden:

- Sicherheit ist ein klar anerkannter Wert (1)
- Führung für Sicherheit ist klar (2)
- Verantwortung für die Sicherheit ist klar (3)
- Sicherheit ist in alle Aktivitäten integriert (4)
- Sicherheit ist lerngetrieben (5)

Die Sicherungskultur nach IAEA NSS No. 7 /IAE 08/ und 28-T /IAE 17/ unterscheidet drei Charakteristika Managementsysteme, Führungsverhalten und Personalverhalten, denen die folgenden Indikatoren zugeordnet werden:

- Managementsysteme (I)
    a) Sichtbare Richtlinie für die Sicherung
    b) Klare Rollen und Verantwortlichkeiten
    c) Messung der Leistung
    d) Arbeitsumfeld
    e) Training und Qualifikation
    f) Arbeitsmanagement
    g) Informationssicherheit
    h) Betrieb und Instandhaltung
    i) Kontinuierliche Bestimmung der Vertrauenswürdigkeit des Personals
    j) Qualitätssicherung
    k) Änderungsmanagement
    l) Feedback-Prozess
    m) Notfallpläne und -übungen
    n) Selbstbewertung
    o) Schnittstelle zwischen Betreiber und Aufsichtsbehörde
    p) Koordination externer Organisationen
    q) Aufzeichnungen

- Führungsverhalten (II)
    a) Erwartungen
    b) Ausübung von Befugnissen

c) Entscheidungsfindung
d) Managementaufsicht
e) Beteiligung des Personals
f) Effektive Kommunikation
g) Verbesserung der Leistung
h) Motivation

- Personalverhalten (III)
  a) Berufliches Verhalten
  b) Persönliche Verantwortlichkeit
  c) Einhaltung von Prozeduren
  d) Teamarbeit und Kooperation
  e) Wachsamkeit

Die in nachfolgender Tabelle verwendete Nummerierung entspricht IAEA NSS No 28-T.

A.1 A: Ziele und Politik der Organisation – Sicherheitsrichtlinien

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
A (1)	Es existieren Richtlinien und klar definierte Ziele zur Informationssicherheit.	I(a) (1)	Für die Organisation wird eine Sicherungsrichtlinie erstellt.	1c)	Die strategische geschäftliche Bedeutung der Sicherheit spiegelt sich im Geschäftsplan wider: • Ziele, Strategien, Pläne und Zielsetzungen in Bezug auf die Sicherheit sollten klar identifiziert und in den Geschäftsplan integriert werden.
		I(a) (3)	Es existiert ein Verhaltenskodex für das Personal, der die Bedürfnisse der nuklearen Sicherung abdeckt.		
		I(g) (9)	Es existiert eine dokumentierte Richtlinie zur Informationssicherheit, die alle Informationsträger umfasst.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Die Sicherheitspolitik sollte dokumentiert werden.
A (2)	Die Richtlinien zur Informationssicherheit wurden zielgruppen- und bedarfsgerecht erstellt.	I(d) (3)	Die Texte von Leitfäden und Prozessen sind benutzerfreundlich und für das Personal verständlich.		
A (3)	In den Richtlinien zur Informationssicherheit wurden konkrete Maßnahmen festgelegt.				
A (4)	Die Anforderungen der Informationssicherheitsrichtlinien entsprechen den rechtlichen und behördlichen Vorschriften.				

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
A (5)	Die Informationssicherheitsrichtlinien sollten durchsetzbar, erreichbar und überprüfbar sein.	I(b) (6)	Sicherungsprozesse und -verfahren sind klar definiert, so dass sie leicht zu verstehen, zu befolgen und zu bewerten sind.	4c)	Die Qualität der Dokumentation und der Verfahren ist gut: • Verfahren sollten kontrolliert, klar, verständlich und aktuell sowie leicht zu finden, zu verwenden und zu überarbeiten sein. • Die Dokumentation sollte umfassend, leicht verständlich und leicht zugänglich sein.
		III(c)(5)	Die Sicherungsanweisungen der Organisation sind leicht zu befolgen, da sie klar, aktuell, leicht verfügbar und benutzerfreundlich sind.		
A (6)	Richtlinien und klar definierte Ziele zur Informationssicherheit sind für das Personal sichtbar, ihnen bekannt und allgegenwärtig (z.B. über ihnen zugängliche Medien wie Intranet, Newsletter, Poster, etc.).	III(b)(8)	Führungskräfte definieren eine Strategie, um Mitarbeiter und Auftragnehmer auf Informationen über die aktuelle Sicherungspolitik aufmerksam zu machen.		
		III(c)(9)	Prozeduren sind sofort an allen Arbeitsplätzen verfügbar.		
		I(g) (9)	Die Richtlinie zur Informationssicherheit ist allen Mitarbeitern bekannt.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Die Sicherheitspolitik sollte dem Personal mitgeteilt werden.
		III(a)(1)	Mitarbeiter sind mit dem Berufskodex der Organisation vertraut.		
		I(a) (1b)	Die Sicherungs-Richtlinie wird in Einrichtungen und Büros ausgehängt und ist dem Personal bekannt.		
				3c)	Vorschriften und Prozesse werden in hohem Maß eingehalten: • Die Erwartungen des Managements an die Anwendung von Verfahren (d. h. wann Verfahren in den Händen des

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
					Benutzers liegen und angewendet werden sollen) und die Einhaltung der Verfahren (d. h. den erwarteten Grad der Einhaltung) sollten klar und dem Personal bekannt sein.
		I(a) (15)	Leicht zugängliche Medien (Intranet, Newsletter, usw.) werden verwendet, um die Sicherungsrichtlinien an Mitarbeiter und Auftragnehmer zu verbreiten.		
A (7)	Richtlinien zur Informationssicherheit werden eingehalten und gelebt.	I(a) (2)	Die Sicherheitsfunktion hat innerhalb der gesamten Organisation einen angesehenen Status.		
		III(a) (1)	Mitarbeiter halten den Berufskodex der Organisation ein.	3c)	Es besteht ein hohes Maß an Einhaltung von Vorschriften und Verfahren: • Das Personal sollte sich an Vorschriften und Verfahren halten.
		III(c)(1)	Mitarbeiter halten sich an Prozeduren und andere Protokolle, wie z.B. Informationssicherheitskontrollen.	2i	Beziehungen zwischen Managern und Einzelpersonen basieren auf Vertrauen: • Das Personal sollte sich an das Managementsystem halten.
		II(d)(3)	Mitarbeiter und Auftragnehmer sind für die Einhaltung der festgelegten Richtlinien und Prozesse verantwortlich.	2i)	Beziehungen zwischen Managern und Einzelpersonen basieren auf Vertrauen: • Manager sollten sicherstellen, dass das Sicherheitsbewusstsein in der Arbeitsumgebung in der gesamten Organisation vorherrscht.

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
		I(a)(8)	Mitarbeiter und Auftragnehmer verstehen, dass von allen Mitarbeitern die Einhaltung der Richtlinien zur nuklearen Sicherung erwartet wird.		
		III(c)(3)	Mitarbeiter und Auftragnehmer sind sich der möglichen Folgen einer Nichteinhaltung der festgelegten Sicherungsvorschriften bewusst.		
		III(c)(10)	10) Mitarbeiter und Auftragnehmer vermeiden Abkürzungen bei der Implementierung von Sicherungsprozessen.		
				3c)	Es besteht ein hohes Maß an Einhaltung von Vorschriften und Verfahren: • Fälle von Nichteinhaltung sollten vermieden werden.
		III(b) (2)	Verpflichtungen werden erfüllt oder das Management wird vorab über ihre Nichterfüllung informiert.		
		I(f) (3)	Mitarbeiter halten sich an die festgelegten Pläne oder holen die entsprechende Genehmigung ein, um von geplanten Aufgaben und Aktivitäten abzuweichen.	4d)	Die Qualität der Prozesse von der Planung bis zur Umsetzung und Überprüfung ist gut: • Einzelpersonen sollten die genehmigten Pläne befolgen und ordnungsgemäße Genehmigungen einholen, bevor sie von den genehmigten Plänen abweichen.

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
		III(c)(8)	8) Mitarbeiter und Auftragnehmer zeigen angemessenes Vertrauen in und Akzeptanz von Sicherungsprozessen.		
A (8)	Es gibt Prozesse, mit denen die Einhaltung der Informationssicherheitsrichtlinien überprüft wird.	I(a) (7)	Es bestehen Prozesse zur Identifizierung der zwingend notwendigen Anforderungen an die Sicherung.		
		I(a) (5)	Für alle wesentlichen Sicherungsaktivitäten gibt es bewährte Prozesse.		
		III(c)(4)	Führungskräfte überprüfen häufig die Arbeit, um sicherzustellen, dass die Verfahren gemäß den Erwartungen verwendet und befolgt werden.		
		III(c)(6)	Es ist eine bewährte Praxis, Mitarbeiter und Auftragnehmer an die Bedeutung der zu befolgenden Prozesse zu erinnern.		
		III(c)(7)	Mitarbeiter und Auftragnehmer, die Unstimmigkeiten bei der Umsetzung von Sicherungsprozesse entdecken, melden diese umgehend an die Vorgesetzten.		
		I(d) (6)	Sicherungsprozesse werden nicht als übermäßige Belastung angesehen.		
A (9)	Mögliche sich ändernde Anforderungen an Informationssicherheitsrichtlinien werden in Form eines festgelegten Prozesses regelmäßig überprüft und bei Bedarf aktualisiert.	I(a) (6)	Die Richtlinien zur Sicherung werden regelmäßig unter Beteiligung der Geschäftsleitung überprüft und aktualisiert.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Schlüsselentscheidungen in Bezug auf die Sicherheit sollten regelmäßig
		I(d) (10)	Die Prozesse werden regelmäßig auf Grundlage der Beiträge der Mitarbeiter und		

Charakteristika, Attribute, Indikatoren, Kriterien der Informationssicherheitskultur		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherungskultur nach IAEA NSS No 7 + 28-T		Charakteristika, Attribute, Indikatoren, Kriterien der Sicherheitskultur nach IAEA GS-G 3.5	
			der Ergebnisse der Leistungstests überprüft und aktualisiert.		überprüft und Annahmen und Schlussfolgerungen sollten im Lichte neuer Informationen, Betriebserfahrungen oder geänderter Umstände in Frage gestellt werden.
		I(a) (10)	Die Richtlinien zur Sicherung werden bei Bedarf auf dem neusten Stand gehalten.		
		II(d) (10)	Führungskräfte sorgen für regelmäßige Audits und Aktualisierungen der Informationssicherheitsrichtlinien und -verfahren.		
A (10)	Dem Personal ist aufgrund der Richtlinien zur Informationssicherheit klar, wie sie sich im täglichen Umgang mit IT-Systemen, bei sicherheitsrelevanten Ereignissen und bei Notfällen zu verhalten haben.				

A.2 B: Arbeitsbedingungen

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
B (1a)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Vermeidung von Zeitdruck bei der Arbeit	I(d)(12)	Die Sicherungs-Sicherheits-Schnittstelle wird risikobewusst und ausgewogen verwaltet.		
		I(d)(9)	Es gibt einen Mechanismus zur Überwachung und Kontrolle von Überstunden, um nachteilige Auswirkungen auf die Sicherung aufgrund von Ermüdung oder anderen damit verbundenen Umständen zu vermeiden.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Aufzeichnungen über Überstunden sollten geführt, getrendet und darauf reagiert werden. Geplante Überstunden sollten in geregelten Grenzen gehalten werden.
		II(b)(9)	Führungskräfte verhindern nach Möglichkeit sicherungsrelevanten Personalabbau, trotz finanzieller Zwänge.		
		II(d)(8)	Führungskräfte überwachen die Bewältigungsfähigkeiten sowie das Stress- und Ermüdungsniveau des Personals.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Die Planung von Arbeiten an sicherheitskritischen Aufgaben in der Nacht sollte vermieden werden. • Schichtpläne sollten auf aktuellem Wissen über die besten Lösungen in Bezug auf die menschliche Leistung und Fähigkeiten basieren. • Manager sollten sensibel auf Stress reagieren, der Personen unter ihrer Kontrolle betrifft, indem sie beispielsweise Stressbewusstseinsschulungen durchführen.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(f) (4)	Die Arbeiten werden so detailliert geplant, dass die Mitarbeiter effektiv und effizient arbeiten können (z.B. werden Ressourcen an den Bedarf angepasst, Ersatzteile und Werkzeuge sind bei Bedarf verfügbar).	4d)	Die Qualität der Prozesse von der Planung bis zur Umsetzung und Überprüfung ist gut: Die Arbeiten sollten ausreichend detailliert geplant werden, damit das Personal effektiv und effizient arbeiten kann (z. B. sollten die Ressourcen den Anforderungen angepasst und bei Bedarf Ersatzteile und Werkzeuge verfügbar sein).
		II(e)(7)	Es gibt Pläne, um zu verhindern, dass Arbeitskämpfe unannehmbare Auswirkungen auf die nukleare Sicherung haben.		
B (1b)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Förderung von Teamwork	I(d)(8)	Das Arbeitsklima unterstützt Teamarbeit und Wissensaustausch.		
		III(d)(4)	Teamwork und Kooperation werden auf allen Ebenen und über organisatorische und bürokratische Grenzen hinweg gefördert.		
		III(d)(7)	Es gibt Möglichkeiten, sicherungsrelevante Informationen innerhalb und zwischen Einheiten auszutauschen.	2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen: • Vorgesetzte sollten Sicherheitsfragen häufig mit ihren Teams oder Arbeitsgruppen besprechen.
		II(d)(9)	Führungskräfte helfen, Vertrauen aufzubauen und die Teamarbeit innerhalb der Organisation zu fördern.	4a)	Vertrauen durchdringt die Organisation.
		III(d)(1)	Teams werden für ihren Beitrag zur nuklearen Sicherung anerkannt.	4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					• Personen und ihre beruflichen Fähigkeiten, Werte und Erfahrungen sollten als das wertvollste strategische Gut der Organisation für die Sicherheit betrachtet werden.
B (1c)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Schaffung eines vertrauensvollen Umfelds (Belohnung vs. Bestrafung, offene Fehlerkultur)	III(d)(2)	Mitarbeiter gehen offen und vertrauensvoll miteinander um und unterstützen sich regelmäßig.	4h)	Es gibt eine funktions- und interdisziplinäre Zusammenarbeit und Teamarbeit: • Der Einzelne sollte offen und vertrauensvoll miteinander umgehen und sich regelmäßig gegenseitig unterstützen.
		III(d)(6)	Berufsgruppen schätzen die Kompetenzen und Rollen des anderen im Umgang mit Sicherungsfragen.		
		II(b)(10)	Führungskräfte sorgen für eine faire Behandlung von Untergebenen und verstehen, dass Fehler unvermeidlich sind, aber dass Sicherungsverletzungen analysiert und Korrekturmaßnahmen ergriffen werden müssen.		
		III(d)(10)	Es gibt nur wenige Anzeichen von Frustration, Groll oder anderen Symptomen einer schlechten Moral innerhalb der Organisation, die die Zusammenarbeit zwischen verschiedenen Einheiten, insbesondere denen, die für Sicherheit und Sicherung zuständig sind, behindern könnten.		
B (1d)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a.	III(d)(3)	Probleme werden von mehrstufigen und multidisziplinären Teams gelöst.	4h)	Es gibt eine funktions- und interdisziplinäre Zusammenarbeit und Teamarbeit: Gegebenenfalls sollten multidisziplinäre Teams (aus verschiedenen Arbeitsgruppen und

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
	• Multidisziplinäre Teams zur Lösung von Problemen				verschiedenen Ebenen) eingesetzt werden, um Problemlösungen zu entwickeln.
		III(d)(8)	Teammitglieder werden regelmäßig anderen Teams zugewiesen, um die Kommunikation zwischen den Teams zu verbessern.		
		III(d)(9)	Cross-Training wird zwischen verschiedenen Berufsfeldern und Gruppen durchgeführt, um Teamarbeit und Zusammenarbeit zu erleichtern.		
B (1e)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Einbindung der Mitarbeitenden in den Entscheidungsprozess	II(c) (1)	Führungskräfte treffen Entscheidungen, wenn es die Situation erfordert.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Mehrere Methoden sollten verwendet werden, um die Bedeutung der Sicherheit in der gesamten Organisation zu kommunizieren. • Entscheidungen, die die Sicherheit betreffen, sollten rechtzeitig getroffen werden.
				1e)	Ein proaktiver und langfristiger Ansatz für Sicherheitsfragen wird bei der Entscheidungsfindung gezeigt: • Bei der strategischen und langfristigen Planung sollten bekannte und potenzielle Sicherheitsprobleme berücksichtigt werden. • Die Prioritäten und Anreize für die Geschäftsleitung sollten sich nicht ausschließlich auf kurzfristige Ziele, Strategien, Pläne und Ziele beziehen.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(a) (4)	Die meisten Mitarbeiter und Auftragnehmer auf allen Ebenen der Organisation sind aktiv und routinemäßig an der Verbesserung der Sicherung beteiligt.		
		I(i) (6)	Abweichende Ansichten, unterschiedliche Perspektiven und eine solide Diskussion anstehender sicherungsbezogener Fragen und Änderungen sind erwünscht.	2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern: • Manager sollten aktiv nach abweichenden Ansichten und unterschiedlichen Perspektiven suchen und sollten offene Diskussionen fördern, um unabhängiges Denken zu unterstützen.
		II(c) (3)	Führungskräfte fordern ggf. abweichende Ansichten und unterschiedliche Perspektiven ein, um die getroffene Entscheidung zu stärken.		
		II(c) (4)	Führungskräfte verkürzen oder umgehen die Entscheidungsprozesse nicht.		
		II(d) (4)	Mitarbeiter und Auftragnehmer sind befugt, technische Entscheidungen in Bezug auf Fragen der nuklearen Sicherung zu treffen.		
		II(c) (5)	Entscheidungen werden von qualifizierten und befugten Personen getroffen.		
		II(c) (6)	Sicherungsrelevante Entscheidungen von Führungskräften werden als vernünftig angesehen.		
		II(c) (7)	Manager sind aktiv daran beteiligt, Prioritäten abzuwägen, um zeitnahe Lösungen zu erreichen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(c) (8)	Führungskräfte unterstützen und stärken die konservative Entscheidungsfindung in Bezug auf Sicherung.		
		II(c)(2)	Führungskräfte erläutern ihre Entscheidungen, wenn möglich.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Die Gründe für wichtige Sicherheitsentscheidungen sollten dem Personal regelmäßig mitgeteilt werden.
				2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation: • Manager sollten Mitarbeiter an ihren Arbeitsplätzen besuchen und, wenn möglich, offene Sitzungen abhalten, um Fragen und Entscheidungen im Kontext zu erläutern.
		II(e)(1)	Führungskräfte beziehen die Mitarbeiter in die Risikobewertungs- und Entscheidungsprozesse und andere Aktivitäten ein, die sie betreffen.	2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern: • Soweit durchführbar, sollten Führungskräfte ihre Mitarbeiter in Entscheidungen und Aktivitäten, die sie betreffen, einbeziehen, beispielsweise indem sie Einzelpersonen in ihre eigenen Verfahren und Anweisungen einbeziehen. • Der Einzelne sollte das Gefühl haben, dass seine Meinung wichtig ist, und sollte in der Lage sein, Beispiele zu nennen, in denen sein Beitrag zu positiven Veränderungen geführt hat.
		II(e)(3)	Die Mitarbeiter sind aktiv an der Identifizierung, Planung und Verbesserung von sicherungsrelevanten Arbeiten und Arbeitspraktiken beteiligt.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
B (1f)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Es gibt einen Feedback- und Verbesserungsprozess	II(b) (6)	Es gibt Korrektur- und Verbesserungsprogramme, die von Führungskräften, Managern und der Aufsichtsbehörde überwacht werden.		
		I(i) (1)	Es gibt Prozesse zur Beschaffung, Überprüfung und Anwendung verfügbarer nationaler und internationaler Informationen, die sich auf die Sicherungsfunktion und das nukleare Sicherungssystem beziehen.		
		I(i) (2)	Es gibt Prozesse, die es der Öffentlichkeit und allen Mitarbeitern ermöglichen und sie ermuntern, ungewöhnliche Zustände, Bedenken, tatsächliche oder Beinahe-Ereignisse zu melden und sie ggf. dafür zu belohnen.		
		I(d) (7)	Feedback von Mitarbeitern und Auftragnehmern wird angefordert und analysiert.	2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation: • Vorgesetzte sollten offen und ehrlich auf die Fragen von Einzelpersonen antworten und gute Beziehungen zum Personal pflegen. • Manager sollten sicherstellen, dass offene Kommunikation geschätzt und bewahrt wird. • Das Management hat die Fähigkeit, Konflikte nach Bedarf zu lösen. • Bei Bedarf sollten faire und unparteiische Methoden zur Konfliktlösung und Streitbeilegung verwendet werden.
		I(i) (5)	Feedback wird geschätzt und gefördert.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(f) (8)	Manager reagieren auf Feedback, um negativen Sicherungstrends entgegenzuwirken.		
		II(d) (2)	Konstruktives Feedback wird verwendet, um das von den Mitarbeitern erwartete Verhalten zu verstärken.		
		II(a) (11)	Konstruktives Feedback wird verwendet, um das von den Mitarbeitern erwartete Verhalten zu verstärken.		
B(1g)	Als zugrundeliegende Basis wird beim Personal eine kritisch hinterfragende Grundhaltung gefördert. Dies beinhaltet auch den Schutz der Personen, die Probleme melden (z.B. durch die Möglichkeit der anonymen Meldung).	II(e)(4)	Mitarbeiter und Auftragnehmer melden jedes Problem vertraulich, weil sie wissen, dass hinterfragende Einstellungen gefördert werden.	2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation: • Führungskräfte und andere Personen, die das Verhalten des Personals beeinflussen können, sollten eine hinterfragende Haltung fördern.
		I(l) (7)	Mitarbeiter und Auftragnehmer werden aufgefordert, Verfahren und Anweisungen während ihrer Verwendung kritisch zu überprüfen und ggf. Verbesserungen vorzuschlagen.	5a)	Auf allen Organisationsebenen herrscht eine hinterfragende Haltung: • Einzelpersonen sollten ungewöhnliche Anzeichen und Ereignisse bemerken und in der Lage sein, diese zu hinterfragen und im Zweifelsfall Rat einholen.
B(1h)	Wenn ein Fehler oder Ereignis auftritt, lautet die Frage "Was ist schiefgelaufen?" und nicht "Wer hat sich geirrt?", wobei der Schwerpunkt auf Verbesserung und nicht auf Schuldzuweisung liegt.	I(f) (8)	Manager reagieren auf Feedback, um negativen Sicherungstrends entgegenzuwirken.		
		III(d) (5)	Die Teammitglieder unterstützen sich gegenseitig, indem sie sich der Handlungen		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			des anderen bewusst sind und bei Bedarf konstruktives Feedback geben.		
B (1i)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Ermutigung zu Verbesserungsvorschlägen	II(e)(2)	Die Mitarbeiter werden ermutigt, Vorschläge zu machen und werden für ihre Beiträge angemessen gewürdigt.		
		II(h) (11)	Mitarbeiter und Auftragnehmer können Beispiele dafür nennen, wann Personen, die sicherungsbezogene Bedenken oder potenzielle Verbesserungen übermittelt haben, öffentlich anerkannt wurden.		
		I(i) (7)	Mitarbeiter und Auftragnehmer werden aufgefordert, Verfahren und Anweisungen während ihrer Verwendung kritisch zu überprüfen und ggf. Verbesserungen vorzuschlagen.	3c)	Es besteht ein hohes Maß an Einhaltung von Vorschriften und Verfahren: Das Personal sollte ermutigt werden, Verfahren und Anweisungen im Einsatz kritisch zu überprüfen und gegebenenfalls Verbesserungen vorzuschlagen.
		II(e)(6)	Mitarbeiter und Auftragnehmer können ihre Erkenntnisse und Ideen zu praktischen Problemen einbringen, und es gibt Mechanismen zur Unterstützung ihrer Beiträge.		
				5a)	Auf allen Organisationsebenen herrscht eine hinterfragende Haltung: • Einzelpersonen auf allen Ebenen sollten ermutigt werden, in den Sitzungen detaillierte Fragen zu stellen. • Das Management sollte seine eigenen Einstellungen und Ansichten hinterfragen und

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					aktiv nach unabhängigen Ansichten suchen.
				2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern: • Führungskräfte sollten das Vorbringen von Bedenken durch das Personal fördern und Maßnahmen ergreifen oder erklären, warum keine Maßnahmen ergriffen wurden.
		II(e)(5)	Es sind Systeme vorhanden, die sicherstellen, dass es für Mitarbeiter einfach, unkompliziert und willkommen ist, Probleme im Zusammenhang mit potenziellen oder erwarteten sicherungsbezogenen Schwächen und Bedrohungen anzusprechen.		
		III(d)(11)	Management und Mitarbeiter fördern und implementieren Maßnahmen zur gegenseitigen Inspiration von Ideen und zur Aufrechterhaltung der Sicherungskooperation zwischen Organisationseinheiten.		
		II(b) (7)	Manager leiten bei Bedarf Verfahren ein, um Sicherungsprobleme zu untersuchen, sich zu deren Ursachen und zu implementierenden Verbesserungen beraten zu lassen.		
		I(f)(7)	Das Sicherungspersonal wird durch das Schulungssystem und durch Anreize kontinuierlich motiviert.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(h)(10)	Die Führungskräfte haben Maßnahmen ergriffen, um die Karriere im Management der nuklearen Sicherung zu verbessern.		
		II(h)(12)	Eine sicherungsbewusste Einstellung ist einer der Faktoren bei der Genehmigung einer Beförderung in die Führungsebene.		
		I(d)(1)	Die Arbeitsumgebung ist für hohe Leistungsstandards förderlich (z.B. Standards für die Hausverwaltung, rechtzeitige Bereitstellung von Ausrüstung und Werkzeugen).	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Die physische Arbeitsumgebung sollte hohen Sicherheits- und Leistungsstandards förderlich sein (z. B. Standards für die Haushaltsführung, Bereitstellung von Ausrüstung und Werkzeugen, einschließlich Reaktionsausrüstung sowie Bewachung und Beschilderung von Gefahren).
				4i)	Die Hausverwaltung und die materiellen Bedingungen spiegeln das Engagement für Exzellenz wider: • Manager sollten langjährige Probleme mit Ausrüstung, Systemen oder Prozessen nicht als „so wie die Dinge sind“ akzeptieren. Manager sollten der Lösung solcher Probleme besondere Aufmerksamkeit schenken, auch wenn die Lösungen schwierig und teuer sind. • Es sollte einen Prozess geben, um seit langem bestehende Probleme in Bezug auf Ausrüstung oder Prozesse zu identifizieren. Z. B. könnte jedes Problem einen Aktionsplan für seine Lösung haben.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(d) (2)	Die Mitarbeiter werden zur Ergonomie und Effektivität ihrer Arbeitsumgebung befragt.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Einzelpersonen sollten über die Ergonomie und die Effektivität ihrer Arbeitsumgebung konsultiert werden.
		I(d) (11)	Konstrukteure und Betreiber von Sicherungssystemen sorgen dafür, dass Sicherungsmaßnahmen keine Sicherheitsfunktionen beeinträchtigen.		
		I(f)(1)	Es sind Arbeiten geplant, um sicherzustellen, dass die Integrität des nuklearen Sicherungssystems jederzeit wirksam gewahrt wird.	4d)	Die Qualität der Prozesse von der Planung bis zur Umsetzung und Überprüfung ist gut: • Die Arbeiten sollten im Voraus geplant werden (einschließlich Notfallplänen), um sicherzustellen, dass alle Sicherheitsfunktionen jederzeit wirksam sind und die Sicherheit nicht beeinträchtigt wird.
		I(h) (2)	Es werden Checklisten und detaillierte Prozesse verwendet.		
		I(d)(12)	Die Sicherungs-Sicherheits-Schnittstelle wird risikobewusst und ausgewogen verwaltet.		
		I(f) (5)	Die Schnittstellen zwischen den Arbeitsgruppen werden bei der Planung berücksichtigt und adressiert.		
		I(f) (6)	IT-Sicherheitssysteme werden entwickelt und instandgehalten, um sicherzustellen, dass sie sicher sind, dass sie von einer geeigneten Behörde akkreditiert sind und in		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			Übereinstimmung mit den Prozeduren betrieben werden.		
		I(f) (9)	Kleine Sicherungsprobleme werden umgehend behoben.		
		I(f) (11)	Die Organisation verfügt über schriftliche Richtlinien, Regeln und Prozesse für die Einstellung, Beurteilung und Beendigung des Arbeitsverhältnisses in Bezug auf Sicherung.		
Informationssicherheitskultur		**Sicherungskultur nach IAEA NSS No 7 + 28-T**		**Sicherheitskultur nach IAEA GS-G 3.5**	
B (1a)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Vermeidung von Zeitdruck bei der Arbeit	I(d)(4)	Top-Manager besuchen regelmäßig besetzte Sicherungsposten. Besonderes Augenmerk wird auf Zeiten geringer Aktivität wie Nachtschichten und Wochenenden gelegt.		
		I(d)(9)	Es gibt einen Mechanismus zur Überwachung und Kontrolle von Überstunden, um nachteilige Auswirkungen auf die Sicherung aufgrund von Ermüdung oder anderen damit verbundenen Umständen zu vermeiden.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Aufzeichnungen über Überstunden sollten geführt, getrendet und darauf reagiert werden. Geplante Überstunden sollten in geregelten Grenzen gehalten werden.
		II(b)(9)	Führungskräfte verhindern nach Möglichkeit sicherungsrelevanten Personalabbau, trotz finanzieller Zwänge.		
		II(d)(8)	Führungskräfte überwachen die Bewältigungsfähigkeiten sowie das Stress- und Ermüdungsniveau des Personals.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					• Die Planung von Arbeiten an sicherheitskritischen Aufgaben in der Nacht sollte vermieden werden. • Schichtpläne sollten auf aktuellem Wissen über die besten Lösungen in Bezug auf die menschliche Leistung und Fähigkeiten basieren. • Manager sollten sensibel auf Stress reagieren, der Personen unter ihrer Kontrolle betrifft, indem sie beispielsweise Stressbewusstseinsschulungen durchführen.
		I(f) (4)	Die Arbeiten werden so detailliert geplant, dass die Mitarbeiter effektiv und effizient arbeiten können (z.B. werden Ressourcen an den Bedarf angepasst, Ersatzteile und Werkzeuge sind bei Bedarf verfügbar).	4d)	Die Qualität der Prozesse von der Planung bis zur Umsetzung und Überprüfung ist gut: Arbeiten sollten ausreichend detailliert geplant werden, damit das Personal effektiv und effizient arbeiten kann (z. B. sollten die Ressourcen den Anforderungen angepasst und bei Bedarf Ersatzteile und Werkzeuge verfügbar sein).
		II(e)(7)	Es gibt Pläne, um zu verhindern, dass Arbeitskämpfe unannehmbare Auswirkungen auf die nukleare Sicherung haben.		
B (1b)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Förderung von Teamwork	I(d)(8)	Das Arbeitsklima unterstützt Teamarbeit und Wissensaustausch.		
		III(d)(4)	Teamwork und Kooperation werden auf allen Ebenen und über organisatorische und bürokratische Grenzen hinweg gefördert.		
		III(d)(7)	Es gibt Möglichkeiten, sicherungsrelevante Informationen innerhalb und zwischen Einheiten auszutauschen.	2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					• Vorgesetzte sollten Sicherheitsfragen häufig mit ihren Teams oder Arbeitsgruppen besprechen.
		II(d)(9)	Führungskräfte helfen, Vertrauen aufzubauen und die Teamarbeit innerhalb der Organisation zu fördern.	4a)	Vertrauen durchdringt die Organisation.
		III(d)(1)	Teams werden für ihren Beitrag zur nuklearen Sicherung anerkannt.	4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt: • Personen und ihre beruflichen Fähigkeiten, Werte und Erfahrungen sollten als das wertvollste strategische Gut der Organisation für die Sicherheit betrachtet werden.
B (1c)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Schaffung eines vertrauensvollen Umfelds (Belohnung vs. Bestrafung, offene Fehlerkultur)	III(d)(2)	Mitarbeiter gehen offen und vertrauensvoll miteinander um und unterstützen sich regelmäßig.	4h)	Es gibt eine funktions- und interdisziplinäre Zusammenarbeit und Teamarbeit: • Der Einzelne sollte offen und vertrauensvoll miteinander umgehen und sich regelmäßig gegenseitig unterstützen.
		III(d)(6)	Berufsgruppen schätzen die Kompetenzen und Rollen des anderen im Umgang mit Sicherungsfragen.		
		II(b)(10)	Führungskräfte sorgen für eine faire Behandlung von Untergebenen und verstehen, dass Fehler unvermeidlich sind, aber dass Sicherungsverletzungen analysiert und Korrekturmaßnahmen ergriffen werden müssen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(d)(10)	Es gibt nur wenige Anzeichen von Frustration, Groll oder anderen Symptomen einer schlechten Moral innerhalb der Organisation, die die Zusammenarbeit zwischen verschiedenen Einheiten, insbesondere denen, die für Sicherheit und Sicherung zuständig sind, behindern könnten.		
B (1d)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Multidisziplinäre Teams zur Lösung von Problemen	III(d)(3)	Probleme werden von mehrstufigen und multidisziplinären Teams gelöst.	4h)	Es gibt eine funktions- und interdisziplinäre Zusammenarbeit und Teamarbeit: Gegebenenfalls sollten multidisziplinäre Teams (aus verschiedenen Arbeitsgruppen und verschiedenen Ebenen) eingesetzt werden, um Problemlösungen zu entwickeln.
		III(d)(8)	Teammitglieder werden regelmäßig anderen Teams zugewiesen, um die Kommunikation zwischen den Teams zu verbessern.		
		III(d)(9)	Cross-Training wird zwischen verschiedenen Berufsfeldern und Gruppen durchgeführt, um Teamarbeit und Zusammenarbeit zu erleichtern.		
B (1e)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Einbindung der Mitarbeitenden in den Entscheidungsprozess	II(c) (1)	Führungskräfte treffen Entscheidungen, wenn es die Situation erfordert.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Mehrere Methoden sollten verwendet werden, um die Bedeutung der Sicherheit in der gesamten Organisation zu kommunizieren. • Entscheidungen, die die Sicherheit betreffen, sollten rechtzeitig getroffen werden.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
				1e)	Ein proaktiver und langfristiger Ansatz für Sicherheitsfragen wird bei der Entscheidungsfindung gezeigt: • Bei der strategischen und langfristigen Planung sollten bekannte und potenzielle Sicherheitsprobleme berücksichtigt werden. • Die Prioritäten und Anreize für die Geschäftsleitung sollten sich nicht ausschließlich auf kurzfristige Ziele, Strategien, Pläne und Ziele beziehen.
		III(a) (4)	Die meisten Mitarbeiter und Auftragnehmer auf allen Ebenen der Organisation sind aktiv und routinemäßig an der Verbesserung der Sicherung beteiligt.		
		I(i) (6)	Abweichende Ansichten, unterschiedliche Perspektiven und eine solide Diskussion anstehender sicherungsbezogener Fragen und Änderungen sind erwünscht.	2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern: • Manager sollten aktiv nach abweichenden Ansichten und unterschiedlichen Perspektiven suchen und sollten offene Diskussionen fördern, um unabhängiges Denken zu unterstützen.
		II(c) (3)	Führungskräfte fordern ggf. abweichende Ansichten und unterschiedliche Perspektiven ein, um die getroffene Entscheidung zu stärken.		
		II(c) (4)	Führungskräfte verkürzen oder umgehen die Entscheidungsprozesse nicht.		
		II(d) (4)	Mitarbeiter und Auftragnehmer sind befugt, technische Entscheidungen in Bezug auf Fragen der nuklearen Sicherung zu treffen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(c) (5)	Entscheidungen werden von qualifizierten und befugten Personen getroffen.		
		II(c) (6)	Sicherungsrelevante Entscheidungen von Führungskräften werden als vernünftig angesehen.		
		II(c) (7)	Manager sind aktiv daran beteiligt, Prioritäten abzuwägen, um zeitnahe Lösungen zu erreichen.		
		II(c) (8)	Führungskräfte unterstützen und stärken die konservative Entscheidungsfindung in Bezug auf Sicherung.		
		II(c)(2)	Führungskräfte erläutern ihre Entscheidungen, wenn möglich.	1a)	Die hohe Priorität, die der Sicherheit eingeräumt wird, zeigt sich in der Dokumentation, Kommunikation und Entscheidungsfindung: • Die Gründe für wichtige Sicherheitsentscheidungen sollten dem Personal regelmäßig mitgeteilt werden.
				2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation: • Manager sollten Mitarbeiter an ihren Arbeitsplätzen besuchen und, wenn möglich, offene Sitzungen abhalten, um Fragen und Entscheidungen im Kontext zu erläutern.
		II(e)(1)	Führungskräfte beziehen die Mitarbeiter in die Risikobewertungs- und Entscheidungsprozesse und andere Aktivitäten ein, die sie betreffen.	2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(e)(3)	Die Mitarbeiter sind aktiv an der Identifizierung, Planung und Verbesserung von sicherungsrelevanten Arbeiten und Arbeitspraktiken beteiligt.		• Soweit durchführbar, sollten Führungskräfte ihre Mitarbeiter in Entscheidungen und Aktivitäten, die sie betreffen, einbeziehen, beispielsweise indem sie Einzelpersonen in ihre eigenen Verfahren und Anweisungen einbeziehen. • Der Einzelne sollte das Gefühl haben, dass seine Meinung wichtig ist, und sollte in der Lage sein, Beispiele zu nennen, in denen sein Beitrag zu positiven Veränderungen geführt hat.
B (1f)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Es gibt einen Feedback- und Verbesserungsprozess	II(b) (6)	Es gibt Korrektur- und Verbesserungsprogramme, die von Führungskräften, Managern und der Aufsichtsbehörde überwacht werden.		
		I(i) (1)	Es gibt Prozesse zur Beschaffung, Überprüfung und Anwendung verfügbarer nationaler und internationaler Informationen, die sich auf die Sicherungsfunktion und das nukleare Sicherungssystem beziehen.		
		I(i) (2)	Es gibt Prozesse, die es der Öffentlichkeit und allen Mitarbeitern ermöglichen und sie ermuntern, ungewöhnliche Zustände, Bedenken, tatsächliche oder Beinahe-Ereignisse zu melden und sie ggf. dafür zu belohnen.		
				2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					• Vorgesetzte sollten offen und ehrlich auf die Fragen von Einzelpersonen antworten und gute Beziehungen zum Personal pflegen. • Manager sollten sicherstellen, dass offene Kommunikation geschätzt und bewahrt wird. • Das Management hat die Fähigkeit, Konflikte nach Bedarf zu lösen. • Bei Bedarf sollten faire und unparteiische Methoden zur Konfliktlösung und Streitbeilegung verwendet werden.
		I(i) (5)	Feedback wird geschätzt und gefördert.		
		I(f) (8)	Manager reagieren auf Feedback, um negativen Sicherungstrends entgegenzuwirken.		
		II(d) (2)	Konstruktives Feedback wird verwendet, um das von den Mitarbeitern erwartete Verhalten zu verstärken.		
B(1g)	Als zugrundeliegende Basis wird beim Personal eine kritisch hinterfragende Grundhaltung gefördert. Dies beinhaltet auch den Schutz der Personen, die Probleme melden (z.B. durch die Möglichkeit der anonymen Meldung).	II(e)(4)	Mitarbeiter und Auftragnehmer melden jedes Problem vertraulich, weil sie wissen, dass hinterfragende Einstellungen gefördert werden.	2h)	Das Management bemüht sich kontinuierlich um Offenheit und gute Kommunikation in der gesamten Organisation: • Führungskräfte und andere Personen, die das Verhalten des Personals beeinflussen können, sollten eine hinterfragende Haltung fördern.
				5a)	Auf allen Organisationsebenen herrscht eine hinterfragende Haltung: • Einzelpersonen sollten ungewöhnliche Anzeichen und Ereignisse bemerken und in

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					der Lage sein, diese zu hinterfragen und im Zweifelsfall Rat einholen.
B(1h)	Wenn ein Fehler oder ein Ereignis auftritt, lautet die Frage "Was ist schiefgelaufen?" und nicht "Wer hat sich geirrt?", wobei der Schwerpunkt auf Verbesserung und nicht auf Schuldzuweisung liegt.	I(f) (8)	Manager reagieren auf Feedback, um negativen Sicherungstrends entgegenzuwirken.		
		III(d) (5)	Die Teammitglieder unterstützen sich gegenseitig, indem sie sich der Handlungen des anderen bewusst sind und bei Bedarf konstruktives Feedback geben.		
B (1i)	Führungskräfte schaffen bestmögliche Voraussetzungen für die sichere und zuverlässige Erfüllung von Aufgaben. Hierzu zählt u.a. • Ermutigung zu Verbesserungsvorschlägen	II(e)(2)	Die Mitarbeiter werden ermutigt, Vorschläge zu machen und werden für ihre Beiträge angemessen gewürdigt.		
		II(h) (11)	Mitarbeiter und Auftragnehmer können Beispiele dafür nennen, wann Personen, die sicherungsbezogene Bedenken oder potenzielle Verbesserungen übermittelt haben, öffentlich anerkannt wurden.		
		I(i) (7)	Mitarbeiter und Auftragnehmer werden aufgefordert, Verfahren und Anweisungen während ihrer Verwendung kritisch zu überprüfen und ggf. Verbesserungen vorzuschlagen.	3c)	Es besteht ein hohes Maß an Einhaltung von Vorschriften und Verfahren: Das Personal sollte ermutigt werden, Verfahren und Anweisungen im Einsatz kritisch zu überprüfen und gegebenenfalls Verbesserungen vorzuschlagen.
		II(e)(6)	Mitarbeiter und Auftragnehmer können ihre Erkenntnisse und Ideen zu praktischen Problemen einbringen, und es gibt		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			Mechanismen zur Unterstützung ihrer Beiträge.		
				5a)	Auf allen Organisationsebenen herrscht eine hinterfragende Haltung: • Einzelpersonen auf allen Ebenen sollten ermutigt werden, in den Sitzungen detaillierte Fragen zu stellen. • Das Management sollte seine eigenen Einstellungen und Ansichten hinterfragen und aktiv nach unabhängigen Ansichten suchen.
				2f)	Das Management strebt die aktive Beteiligung von Einzelpersonen an, um die Sicherheit zu verbessern: • Führungskräfte sollten das Vorbringen von Bedenken durch das Personal fördern und Maßnahmen ergreifen oder erklären, warum keine Maßnahmen ergriffen wurden.
		II(e)(5)	Es sind Systeme vorhanden, die sicherstellen, dass es für Mitarbeiter einfach, unkompliziert und willkommen ist, Probleme im Zusammenhang mit potenziellen oder erwarteten sicherungsbezogenen Schwächen und Bedrohungen anzusprechen.		
		III(d)(11)	Management und Mitarbeiter fördern und implementieren Maßnahmen zur gegenseitigen Inspiration von Ideen und zur Aufrechterhaltung der Sicherungskooperation zwischen Organisationseinheiten.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(b) (7)	Manager leiten bei Bedarf Verfahren ein, um Sicherungsprobleme zu untersuchen, sich zu deren Ursachen und zu implementierenden Verbesserungen beraten zu lassen.		
		I(f)(7)	Das Sicherungspersonal wird durch das Schulungssystem und durch Anreize kontinuierlich motiviert.		
		II(h)(10)	Die Führungskräfte haben Maßnahmen ergriffen, um die Karriere im Management der nuklearen Sicherung zu verbessern.		
		II(h)(12)	Eine sicherungsbewusste Einstellung ist einer der Faktoren bei der Genehmigung einer Beförderung in die Führungsebene.		
		I(d)(1)	Die Arbeitsumgebung ist für hohe Leistungsstandards förderlich (z.B. Standards für die Hausverwaltung, rechtzeitige Bereitstellung von Ausrüstung und Werkzeugen).	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Die physische Arbeitsumgebung sollte hohen Sicherheits- und Leistungsstandards förderlich sein (z. B. Standards für die Haushaltsführung, Bereitstellung von Ausrüstung und Werkzeugen, einschließlich Reaktionsausrüstung sowie Bewachung und Beschilderung von Gefahren).
				4i)	Die Hausverwaltung und die materiellen Bedingungen spiegeln das Engagement für Exzellenz wider: • Manager sollten langjährige Probleme mit Ausrüstungsgegenständen, Systemen oder Prozessen nicht als „so wie die Dinge sind“

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					akzeptieren. Manager sollten der Lösung solcher Probleme besondere Aufmerksamkeit schenken, auch wenn die Lösungen schwierig und teuer sind. • Es sollte einen Prozess geben, um seit langem bestehende Probleme in Bezug auf Ausrüstung oder Prozesse zu identifizieren. Zum Beispiel könnte jedes Problem einen Aktionsplan für seine Lösung haben.
		I(d) (2)	Die Mitarbeiter werden zur Ergonomie und Effektivität ihrer Arbeitsumgebung befragt.	4g)	Es bestehen gute Arbeitsbedingungen in Bezug auf Zeitdruck, Arbeitsbelastung und Stress: • Einzelpersonen sollten über die Ergonomie und die Effektivität ihrer Arbeitsumgebung konsultiert werden.
		I(d) (11)	Konstrukteure und Betreiber von Sicherungssystemen sorgen dafür, dass Sicherungsmaßnahmen keine Sicherheitsfunktionen beeinträchtigen.		
		I(f)(1)	Es sind Arbeiten geplant, um sicherzustellen, dass die Integrität des nuklearen Sicherungssystems jederzeit wirksam gewahrt wird.	4d)	Die Qualität der Prozesse von der Planung bis zur Umsetzung und Überprüfung ist gut: • Die Arbeiten sollten im Voraus geplant werden (einschließlich Notfallplänen), um sicherzustellen, dass alle Sicherheitsfunktionen jederzeit wirksam sind und die Sicherheit nicht beeinträchtigt wird.
		I(h) (2)	Es werden Checklisten und detaillierte Prozesse verwendet.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(d)(12)	Die Sicherungs-Sicherheits-Schnittstelle wird risikobewusst und ausgewogen verwaltet.		
		I(f) (5)	Die Schnittstellen zwischen den Arbeitsgruppen werden bei der Planung berücksichtigt und adressiert.		
		I(f) (6)	IT-Sicherheitssysteme werden entwickelt und instandgehalten, um sicherzustellen, dass sie sicher sind, dass sie von einer geeigneten Behörde akkreditiert sind und in Übereinstimmung mit den Prozeduren betrieben werden.		
		I(f) (9)	Kleine Sicherungsprobleme werden umgehend behoben.		
		I(f) (11)	Die Organisation verfügt über schriftliche Richtlinien, Regeln und Prozesse für die Einstellung, Beurteilung und Beendigung des Arbeitsverhältnisses in Bezug auf Sicherung.		

A.3 C: Personelle Organisation – Rollen, Verantwortlichkeiten, Ressourcen, Fremdpersonal

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Rollen und Verantwortlichkeiten					
C (1)	Die Organisation hat klar definierte und dokumentierte Rollen und Verantwortlichkeiten für alle Positionen im Bereich der Informationssicherheit.	III(b) (6)	Die persönliche Verantwortlichkeit ist in entsprechenden Richtlinien und Verfahren klar definiert.	3b)	Rollen und Verantwortlichkeiten sind klar definiert und verstanden: • Die Organisation muss Funktionen und Verantwortlichkeiten für alle Aspekte der Sicherheit, die unter ihrer Kontrolle stehen, definieren und dokumentieren
		I(b) (1)	Die Organisation hat klar definierte und dokumentierte Rollen und Verantwortlichkeiten für alle Positionen im Bereich der nuklearen Sicherung.	4c)	Die Qualität der Dokumentation und der Verfahren ist gut: • Die Verantwortlichkeiten für die Erstellung der Dokumentation und der Umfang der Überprüfungen sollten klar definiert und verstanden werden.
C (2)	Die Institutionsleitung übernimmt die Gesamtverantwortung.	I(b) (10)	Die Gesamtverantwortung des Managements für die Sicherung ist offensichtlich.	4b)	Die Berücksichtigung aller Arten von Sicherheit, einschließlich Arbeitsschutz und Umweltschutz, und der Sicherung ist offensichtlich.
C (3)	Für das Personal ist offensichtlich, dass die Gesamtverantwortung für die Informationssicherheit beim Management der Geschäftsführung angesiedelt ist.				
C (4)	Alle Mitglieder der Organisation sind sich sowohl ihrer individuellen als auch der gemeinsamen Verantwortung in Bezug auf die Informationssicherheit bewusst.	I(b) (4)	Die Verantwortung für die Sicherung wird einem leitenden Mitglied des Managementteams übertragen, aber alle Mitarbeiter und Auftragnehmer sind sich bewusst, dass die Sicherung eine gemeinsame		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			Verantwortung für die gesamte Organisation ist.		
		III(b) (4)	Mitarbeiter übernehmen Verantwortung für die Lösung von Problemen.		
		III(b) (5)	Mitarbeiter und Auftragnehmer fühlen sich für die Sicherheit der Organisation verantwortlich.		
C (5)	Das Personal versteht seine Rollen und Verantwortlichkeiten für die Informationssicherheit, fühlt sich dafür verantwortlich und kommt diesen vollumfänglich nach.	II(b) (1)	Designierte Manager zeigen gute Kenntnisse über die an sie gestellten Anforderungen, erkennen und übernehmen alle widrigen Sicherungssituationen oder Situationen, in denen die Verwundbarkeit erhöht ist, z.B. wenn das Sicherungssystem beeinträchtigt oder die Bedrohungsstufe erhöht wird.		
		I(b) (5)	Alle Mitarbeiter und Auftragnehmer kennen potenzielle Bedrohungen und das Sicherungssystem gut genug, um ihre Rolle und Verantwortung in Bezug auf die nukleare Sicherung zu übernehmen.	3b)	Rollen und Verantwortlichkeiten sind klar definiert und verstanden: • Personen sollten ihre Funktionen und Verantwortlichkeiten für die Sicherheit verstehen und wissen, wie sich ihre Arbeit auf die Sicherheit auswirken kann.
		I(b) (7)	Alle Mitarbeiter und Auftragnehmer wissen, warum ihnen sicherungsrelevante Funktionen zugewiesen werden, wie diese Funktionen in das Gesamtbild passen und welche Auswirkungen sie auf die Organisation haben können.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(b) (1)	Mitarbeiter verstehen, wie ihre spezifischen Aufgaben die nukleare Sicherheit unterstützen.		
		I(b) (2)	Die Mitarbeiter verstehen ihre Rollen und Verantwortlichkeiten für die nukleare Sicherung und werden ermutigt, bei Bedarf um Klärung zu bitten.	3b)	Rollen und Verantwortlichkeiten sind klar definiert und verstanden: • Einzelpersonen sollten wissen, wo sie Hilfe bei sicherheitsrelevanten Fragen erhalten, und sollten bei Bedarf um Klärung bitten.
		I(b) (3)	Rollen und Verantwortlichkeiten werden neuen Mitarbeitern bei ersten Briefings, Schulungen oder beidem angemessen erklärt.		
C (6)	Hierarchische Lücken, die durch Abgänge von Personal entstehen, werden schnellstmöglich geschlossen.				
C (7)	Es existieren Vertretungs- und Nachfolgeregelungen, falls einzelne Personen ausfallen (Krankheit, Abwesenheit, Abgang).				
		I(b) (9)	Innerhalb der Organisation gibt es ein klares Verständnis der sicherheitsbezogenen Autoritätsebenen und Kommunikationswege.		
		II(f) (9)	Klare, eindeutige und dokumentierte Definitionen der Verantwortlichkeiten der Mitarbeiter wurden über etablierte Kanäle kommuniziert.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(b) (7)	Verfahren und Prozesse gewährleisten eine klare zentrale Rechenschaftspflicht vor der Ausführung.		
Ressourcen					
		II(a) (5)	Sicherung ist ein klar anerkannter Wert in der Organisation und das Management investiert angemessene Ressourcen in Sicherungsvorkehrungen.	1b)	Sicherheit ist ein vorrangiger Aspekt bei der Zuweisung von Ressourcen: • Die Ressourcenzuweisung sollte im Einklang mit den angegebenen Prioritäten, Strategien, Plänen und Zielen der Organisation stehen.
		I(h) (11)	Die Ressourcen werden dem Bedarf angepasst, so dass kritische Ersatzteile und Werkzeuge bei Bedarf verfügbar sind.		
		II(a) (2)	Führungskräfte stellen sicher, dass Ressourcen zur Verfügung stehen, um eine wirksame nukleare Sicherung zu gewährleisten.		
Einsatz von Fremdpersonal					
C (8)	Es existieren Absprachen, vertragliche Festlegungen zu Rollen und Verantwortlichkeiten sowie Vertretungsregelungen im Umgang mit externen Dienstleistern/Unterauftragnehmern etc.	I(b) (8)	In Vertragsdokumenten sind die Rollen und Verantwortlichkeiten der Auftragnehmer im Bereich der nuklearen Sicherung klar definiert.	3b)	Rollen und Verantwortlichkeiten sind klar definiert und verstanden: • Wenn Auftragnehmer beauftragt werden, sollten ihre Funktionen und ihre Verantwortung für die Sicherheit normalerweise in Vertragsdokumenten festgelegt werden. Die betroffenen Personen in der Organisation und in der Auftragnehmer-Organisation sollten auf diese

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					Regelungen aufmerksam gemacht werden.
C (9)	Fremdpersonal kennt die für sie relevanten Gesetze, Vorschriften und internen Regelungen. Sie werden dem Fremdpersonal über ihnen zugängliche Medien (z.B. Poster, Hinweisschilder) allgegenwärtig und sichtbar gemacht.	I(p) (4)	Auftragnehmer kennen die einschlägigen Sicherungsverfahren, nachdem sie vor Beginn der Arbeiten eine entsprechende Schulung absolviert haben.		
C (10)	Es ist dafür Sorge zu tragen, dass Fremdpersonal, das kurzfristig/einmalig in sicherheitsrelevanten Bereichen eingesetzt wird, überwacht und in dem für die auszuführenden Arbeiten notwendigen (ggf. reduzierten) Umfang eingewiesen wird.				
C (11)	Fremdpersonal hält die geltenden Gesetze, Vorschriften und internen Regelungen ein.				
C (12)	Bei längerfristiger Beschäftigung muss Fremdpersonal in die Aufgaben eingewiesen werden. Schulungen werden vertraglich festgelegt und durchgeführt.				
C (13)	Beim ausscheidenden Fremdpersonal bestehen vergleichbare Prozesse wie für eigenes Personal.				
		III(d) (12)	Mitarbeiter und Auftragnehmer verwenden ein gemeinsames technisches Vokabular, um eine einfache Interaktion zu erreichen.		

A.4 D: Schulungs- und Sensibilisierungsmaßnahmen

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Bewusstsein schaffen					
		I(h) (2)	Manager helfen bei der Umsetzung des Programms zur Innentäter-Minimierung, indem sie die Verantwortung betonen, auf ungewöhnliche Vorkommnisse zu achten und diese zu melden.		
D (1)	Die Bedrohung, gegen die IT-Systeme geschützt werden sollten, ist festgelegt und wird von allen an der Konzeption, Anwendung und Bewertung der Sicherheitsmaßnahmen beteiligten Parteien gut verstanden.	I(b) (11)	Die Bedrohung, gegen die nukleares und radioaktives Material geschützt werden sollte, wird von allen Parteien, die an der Planung, Anwendung und Bewertung der Sicherungsmaßnahmen beteiligt sind, bestimmt und verstanden.		
D (2)	Allen Parteien sind die Synergien, die sich durch die verschiedenen Systeme der Sicherheit und Sicherung ergeben, bekannt.	I(b) (12)	Es gibt Systeme, um Synergien zwischen Sicherheit und Sicherung zu erkennen und zu nutzen.		
		I(f) (10)	Synergien und Konflikte zwischen Sicherung, Sicherheit und Betrieb werden berücksichtigt, um negative Auswirkungen auf den Betrieb zu vermeiden.		
		III(a) (9)	Mitarbeiter und Auftragnehmer benachrichtigen ihre Mitarbeiter, wenn diese Mitarbeiter etwas tun, das die Sicherung beeinträchtigen könnte, auch wenn dies nicht zu ihrer Tätigkeit gehört.		
D (3)	Personal und Führungskräfte engagieren sich für die Ziele der Informationssicherheit und legen ein Verhalten an den Tag, das bei Bedarf über die Erfüllung der eigenen Aufgaben hinausgeht.	I(a) (9)	Führungskräfte haben ein sichtbares Interesse an Sicherung und integrieren sie in ihre tägliche Arbeit.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(a) (11)	Regelmäßig abgehaltene Management-Meetings in der Organisation behandeln wichtige Sicherungsthemen.		
		I(a) (12)	Ereignisse im Zusammenhang mit der Bedrohungsumgebung und ihren möglichen Auswirkungen auf die nukleare Sicherung und die Richtlinien der nuklearen Sicherung werden allen Mitarbeitern angemessen mitgeteilt.		
		I(a) (14)	Mitarbeiter und Auftragnehmer können Beispiele aus den Anforderungen der Sicherungsrichtlinien anführen, die ihre Bedeutung veranschaulichen.		
		III(e) (1)	Mitarbeiter bemerken und hinterfragen ungewöhnliche Hinweise und Vorkommnisse und melden sie so schnell wie möglich der Geschäftsleitung unter Verwendung der etablierten Prozesse.		
		III(e) (2)	Mitarbeiter achten auf Details.		
		III(e) (3)	Mitarbeiter suchen Rat, wenn sie sich der Sicherungsbedeutung ungewöhnlicher Ereignisse, Beobachtungen oder Vorkommnissen nicht sicher sind.		
		III(e) (5)	Mitarbeiter und Auftragnehmer werden in Beobachtungstechniken geschult, um Unregelmäßigkeiten bei der Umsetzung von Sicherungsverfahren zu erkennen.		
		III(e) (9)	Mitarbeiter und Auftragnehmer fühlen sich bei der Meldung von Fehlern und Vorfällen vor Repressalien sicher.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(e) (10)	Eine Politik, die Belästigung und Vergeltungsmaßnahmen verbietet, wenn Bedenken hinsichtlich der nuklearen Sicherung geäußert werden, wird durchgesetzt.		
		III(e) (11)	Mitarbeiter und Auftragnehmer treffen Entscheidungen und ergreifen Maßnahmen im Einklang mit ihren Verantwortlichkeiten, wenn eine Entscheidung getroffen werden muss, bevor die Manager am Einsatzort eintreffen.		
		III(e) (12)	Mitarbeiter und Auftragnehmer benachrichtigen das Management über alle Vorfälle oder mögliche Vorfälle, die eine Gefährdung der Informationssicherheit beinhalten.		
Schulungen - Durchführung					
		I(e) (1)	Es existiert ein umfassendes Schulungsprogramm für nukleare Sicherung, in dem Anforderungen und Qualifikationsstandards festgelegt und dokumentiert sind und dem Personal mitgeteilt werden.		
				2e)	Die Geschäftsführung stellt sicher, dass es genügend kompetente Personen gibt: • Bei der Ausbildung und Qualifizierung sollte systematisch vorgegangen werden.
D (4)	Es werden regelmäßige Schulungen zu allen für die Informationssicherheit IT-Sicherung relevanten Themen/Aspekten durchgeführt. Dies umfasst u.a. die folgenden Themen:	I(a) (4)	Mitarbeiter sind mit dem Verhaltenskodex durchlaufende Schulungen und Sensibilisierungsmaßnahmen vertraut.	2d)	Führungsfähigkeiten werden systematisch entwickelt: • Fähigkeiten im Change Management sollten Personen in Führungspositionen vermittelt werden.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
	• Behandlung von Sicherheitsvorfällen (Hackerangriffe, Phishing,) • Erkennung von riskantem/gefährlichem Verhalten • forensische Beweissicherung • Dokumentation, Führen von Logs, Archivierung • Sensibilität von Informationen/Schutz von sensiblen Daten • Sicheres Ablegen, Speicher, Löschen, Vernichten, Verschlüsselung von Daten/Informationen • sicherer Umgang mit Informationen auf Dienstreisen • Zugangs-/Zutrittsberechtigungen • Passwort- und Schlüsselmanagement (digital und physisch) • Erkennung nicht vertrauenswürdiger Dateien/Datenträger • Informationsaustausch/Umgang mit Informationen • Verhalten auf Dienstreisen • besondere Aufgaben/Verantwortlichkeiten/Verhaltensweisen als Führungskraft • Einsatz/Verteilung von Ressourcen (materiell, finanziell, personell) • Rollen und Verantwortlichkeiten/Übernahme von Verantwortung/Verantwortliches Handeln • Wissenserhalt/Übergabe bei Personalwechseln • Schulungen für Administratoren • Authentisierungsverfahren und -prozesse			4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt: • Führungskräfte sollten geschult sein und über angemessene Kenntnisse der Faktoren verfügen, die die menschliche Leistung beeinflussen.
		I(e) (8)	Grundlegende Schulungen zum Sicherungsbewusstsein weisen die Mitarbeiter auf die angemessene Sicherung am Arbeitsplatz sowie die Anforderungen zur Meldung von Sicherheitsverletzungen hin.		
		I(e) (10)	Führungskompetenzen und bewährte Sicherungspraktiken sind Bestandteil von Schulungsprogrammen für Manager und Vorgesetzte.		
		I(e) (13)	Überzeugungen und Einstellungen werden in den Schulungen zur Sicherung berücksichtigt.		
		I(e) (18)	Schulungsprogramme der Organisation befassen sich mit sicherungsbewusstem Verhalten als Schlüsselelement der Professionalität.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
	• Überzeugungen, Einstellungen, Professionalität • Führungsverhalten • Änderungsmanagement				
D (5)	Die interne und externe Betriebserfahrung fließt in die Inhalte und Schwerpunkte von Schulungsmaßnahmen ein.	I(e) (16)	Die Schulungsmaterialien umfassen bewährte Verfahren und Erkenntnisse aus Sicherungsverletzungen sowohl in der Einrichtung als auch anderswo.		
D (6)	Das Personal (Mitarbeiter und Führungskräfte) nimmt an allen für ihren Fachbereich relevanten Schulungen teil.	I(e) (7)	Top-Manager besuchen regelmäßig Schulungen.		
		I(e) (15)	Die Manager verpflichten sich, an Schulungen zur nuklearen Sicherung teilzunehmen.		
		I(e) (12)	Unternehmenswerte und -praktiken erfordern die Teilnahme von Sicherungs- und Nicht-Sicherungs-Personal an Auffrischungsschulungen, um sicherungsbezogene Kenntnisse und Fähigkeiten zu verbessern.		
D (7)	Die Teilnahme an Schulungsmaßnahmen wird dokumentiert und überprüft.				
D (8)	Es finden Nachholtermine bei Verhinderung statt.	I(e) (21)	Es wurden Vorkehrungen getroffen, die es Mitarbeitern und Auftragnehmern ermöglichen, Lücken in ihrer Ausbildung zu vermeiden, wenn sie relevante Module verpassen müssen.		
		I(e) (2)	Die Teilnahme an Schulungen zur Sicherung hat einen hohen Stellenwert und wird nicht durch nicht-dringende Aktivitäten gestört.	2e)	Die Geschäftsführung stellt sicher, dass es genügend kompetente Personen gibt:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
					• Der Teilnahme an Schulungen durch das Personal sollte hohe Priorität eingeräumt werden.
		I(e) (20)	Die Abwesenheitsquote bei Schulungen zur nuklearen Sicherung ist gering.		
D (9)	Bei Änderungen an Arbeits- und Vorgehensweisen finden Sonderschulungen statt.				
D (10)	Personen, die Schulungen durchführen, haben ausreichend Zeit zur Vorbereitung und Durchführung.				
D (11)	Das Personal wird auch für den Umgang mit unerwarteten Situationen/Entwicklungen geschult.				
D (12)	Das Personal sollte IT-Systeme als Unterstützung wahrnehmen und im Umgang mit ihnen geschult sein. Zudem sollten sie bei einem Ausfall wissen, was zu tun ist, um weiterhin arbeitsfähig zu bleiben und Sicherheitsvorfälle zu vermeiden.				
		I(e) (4)	Informationen über den Status der Qualifikationen des Personals sind für diejenigen, die es wissen müssen, leicht zugänglich.		
		I(e) (5)	Mitarbeiter führen keine Tätigkeiten aus, für die ihnen die erforderlichen Kenntnisse und Fähigkeiten fehlen.	2e)	Die Geschäftsführung stellt sicher, dass es genügend kompetente Personen gibt: • Personal sollte nur Arbeiten ausführen, für die es geschult und qualifiziert ist.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
		I(e) (6)	Angemessene Kriterien für die körperliche Fitness werden festgelegt und überwacht.		
		I(e) (9)	Es existieren Systeme, die sicherstellen, dass die in der Ausbildung erlernten Prozeduren und Praktiken in der Praxis angewandt werden.		
		I(e) (14)	Mitarbeiter und Auftragnehmer erkennen an, dass Lernen ein kontinuierlicher und fortlaufender Prozess in der gesamten Organisation ist.		
				5e)	Das Lernen wird erleichtert durch die Fähigkeit, Abweichungen zu erkennen und zu diagnostizieren, Lösungen zu formulieren und umzusetzen und die Auswirkungen von Korrekturmaßnahmen zu überwachen: • Das Personal sollte Vertrauen in den Korrekturmaßnahmenprozess haben und in der Lage sein, auf Beispiele von Problemen hinzuweisen, die es gemeldet und die gelöst wurden. • Es sollten Überprüfungen durchgeführt werden, um sicherzustellen, dass ergriffene Korrekturmaßnahmen die tatsächlichen und zugrunde liegenden Ursachen angehen und das Problem lösen. • Es sollte eine geringe Häufigkeit von Wiederholungsereignissen und Fehlern geben.
					(g) Es gibt eine systematische Entwicklung der individuellen Kompetenzen:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
					• Individuelle Entwicklungsprogramme, einschließlich Nachfolgeplanung, sollten eingeführt werden. • Manager und Vorgesetzte sollten auf der Grundlage ihrer nachgewiesenen Fähigkeit zur Förderung einer starken Sicherheitskultur ausgewählt und bewertet werden. • Beurteilungen der individuellen Entwicklung sollten durchgeführt werden, um den Schulungsbedarf und den Entwicklungsbedarf des Einzelnen zu ermitteln.
					(d) Führungsfähigkeiten werden systematisch entwickelt: • Manager und Vorgesetzte sollten unter gebührender Berücksichtigung ihrer nachgewiesenen Fähigkeit, eine starke Sicherheitskultur zu fördern, ausgewählt und bewertet werden. • Für die Entwicklung zukünftiger Führungskräfte sollte ein Nachfolgeplan eingeführt werden, der Aspekte der Sicherheitskultur beinhaltet.
					(e) Personen verfügen über die erforderlichen Kenntnisse und das Verständnis der Arbeitsabläufe: • Der Einzelne sollte nicht nur seine eigenen Arbeitsprozesse gut verstehen, sondern auch, wie diese Prozesse mit anderen Prozessen interagieren.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
Schulungen - Wirksamkeit					
D (13)	Es existiert ein Prozess zur Überprüfung der Wirksamkeit von Schulungen und Übungen.				
D (14)	Als Grundlage der Überprüfung der Wirksamkeit von Schulungen und Übungen gibt es klar definierte Zielvorgaben.				
D (15)	Führungskräfte messen, inwieweit Schulungsprogramme zu einer Verbesserung der Einstellung zur Sicherungskultur beitragen.				
Schulungen - Ressourcen					
		I(e) (11)	Führungskräfte sind verpflichtet, angemessene Ressourcen für eine effektive Schulung bereitzustellen.		
Schulungen - Einstellungen					
D (16)	Das Personal erkennt an, dass Lernen ein kontinuierlicher und fortlaufender Prozess in der gesamten Organisation ist.				
Schulungen - Qualitätssicherung von Schulungsmaßnahmen					
D (17)	Der Inhalt von Schulungen wird regelmäßig überprüft und ggf. an die Weiterentwicklung von W&T angepasst.	I(e) (3)	Das Schulungsprogramm wird regelmäßig evaluiert und bei Bedarf überarbeitet.		
D (18)	Der Feedback- und Verbesserungsprozess berücksichtigt den Input der Schulungsteilnehmer.	I(e) (17)	Mitarbeiter können Feedback zu Sicherungsschulungen geben.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T			Sicherheitskultur nach IAEA GS-G 3.5
		III(a) (6)	Mitarbeiter und Auftragnehmer tragen zur Verbesserung des Ausbildungsprogramms bei.		
Schulungen - Qualifikationsanforderungen					
		III(a) (6)	Mitarbeiter und Auftragnehmer verfügen über die erforderlichen Qualifikationen, Fähigkeiten und Kenntnisse, um alle Aspekte ihrer sicherungsrelevanten Tätigkeiten effektiv zu erfüllen, und erhalten Gelegenheiten, diese zu verbessern.		
D (19)	Es existiert ein Prozess zur Einarbeitung von Neueinstellungen.				
D (20)	Der Qualifikationsstand des Personals wird dokumentiert und ist für diejenigen, die es wissen müssen, leicht zugänglich.				
D (21)	Personal mit administrativen Aufgaben wird in die für sie relevanten technischen Details (IT-Systeme, Anwendungen, IT-Architektur, IT-Umgebung) eingewiesen.				
D (22)	Arbeitsaufgaben mit Bedeutung für die Informationssicherheit werden ausschließlich an Personen übertragen, die entsprechend geschult wurden.				
D (23)	Das Personal führt keine Tätigkeiten aus, für die ihm die erforderlichen Kenntnisse und Fähigkeiten fehlen.				

A.5 E: Ereignis- und Notfallmanagement

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
Notfallmanagement					
E (1)	Es gibt eine Leitlinie zur Informationssicherheit und zum Notfallmanagement.				
E (2)	Es existiert eine geeignete Organisationsstruktur für das Notfallmanagement.				
E (3)	Das Notfallmanagement wird als zentraler Bestandteil angesehen. Die Mitglieder des Notfallmanagementteams werden in die Behandlung von Sicherheitsvorfällen eingebunden und über Störungs- und Fehlerbehebungen informiert wird.				
		I(f) (2)	Notfallpläne werden erstellt, um auf vorhersehbare Ereignisse zu reagieren.		
		I(m) (1)	Es gibt Notfallpläne, um den definierten Bedrohungen und Reaktionen zu begegnen.		
		I(m) (9)	Notfallpläne basieren auf soliden menschlichen Leistungsprinzipien.		
		I(m) (10)	Die Organisation informiert öffentliche Einrichtungen wie Ersthelfer, Polizei, Militär, medizinische Einrichtungen und Umweltbehörden angemessen über potenzielle Risiken.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
E (4)	Sofortmaßnahmen und Notfallpläne werden regemäßig und anlassbezogen getestet und geübt, damit alle teilnehmenden Personen mit den Plänen und ihren Aufgaben vertraut sind. Zudem ist mit den Tests sicherzustellen, dass sie effektiv, aktuell sind und im zeitlichen Rahmen durchführbar sind.	I(m)(2)	Die Pläne werden regelmäßig durch Übungen und andere Mittel getestet, um sicherzustellen, dass sie effektiv und aktuell sind und dass die beteiligten Personen mit den Plänen und ihren Rollen vertraut sind.		
		I(m)(3)	Alle Sicherungssysteme werden regelmäßig getestet, um sicherzustellen, dass sie funktionsfähig und bei Bedarf verfügbar sind. Besonderes Augenmerk wird auf Systeme gelegt, die im Normalbetrieb nicht aktiviert sind.		
		I(m)(4)	Der Faktor Mensch in Sicherungssystemen wird regelmäßig bewertet, um sicherzustellen, dass das Personal wachsam und bei Bedarf verfügbar ist. Besondere Aufmerksamkeit sollte dem menschlichen Faktor in Zeiten reduzierter Aktivität wir Nachtschicht oder Wochenende gewidmet werden.		
		I(m)(5)	Notfallpläne werden mit einer entsprechenden nationalen Strategie koordiniert und verknüpft.		
		I(m)(6)	Notfallpläne werden nicht nur mit Einsatzkräften vor Ort, sondern auch in Abstimmung mit externen Einsatzkräften getestet.		
		I(m)(7)	Führungskräfte werden darin geschult, mit Ausnahmesituationen, für die keine Verfahren entwickelt wurden, effektiv umzugehen.		
		I(m)(8)	Es sind Vorkehrungen getroffen, dass in Zeiten erhöhter Bedrohung (z.B. Einführung zusätzlicher Maßnahmen oder Einschränkung des Zugriffs) die Sicherungsbereitschaft vorübergehend erhöht werden kann.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
Beweissicherung					
E (5)	Vorfälle werden der Aufsichtsbehörde gemeldet. • Das Personal und die Auftragnehmer sehen die Präsenz der Aufsichtsbehörde auf dem Betriebsgelände positiv. • Der Betreiber informiert die Aufsichtsbehörde (oder eine andere einschlägige zuständige Behörde) auf der Grundlage der Ergebnisse der Selbstbewertung über den aktuellen Stand der Informationssicherheitskultur				
E (6)	Es gibt eine festgelegte Vorgehensweise, nach der bei einer forensischen Untersuchung Datenquellen identifiziert und gesichert werden.				
E (7)	Datenträger werden dupliziert und voneinander getrennt aufbewahrt.				
E (8)	Für die Beweissicherung wird ausschließlich geschultes und zuverlässiges Personal eingesetzt.				
Umgang mit Sicherheitsvorfällen					
E (9)	Es existieren Prozesse und Richtlinien, die die maximalen Verzögerungszeiten bei der Reparatur von IT-Systemen definieren und kontrollieren.				

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
E (10)	Das Personal leitet relevante Meldungen an die richtige Stelle weiter.				
E (11)	Ein Sicherheitsvorfall wird analysiert, um festzustellen, ob die Prozesse und Abläufe bei der Behandlung von Sicherheitsvorfällen korrigiert oder weiterentwickelt werden müssen.				
E (12)	Kleinere Vorfälle im Bereich der Informationssicherheit werden umgehend adressiert und Schutzmaßnahmen umgesetzt.				
Auswertung interner und externer Betriebserfahrung (national, international) zur ständigen Verbesserung					
E (13)	Grundsätzlich sind Informationen aus zuverlässigen Quellen auszuwerten. Relevante Informationen sind entsprechend der Sicherheitsvorfallbehandlung zu bearbeiten.				
E (14)	Der Erkenntnisgewinn über sicherheitsrelevante Ereignisse sollte auch (zuverlässige) externe Quellen miteinschließen.				
E (15)	Alle beteiligen Personen bringen ihre Erfahrungen mit ein.				
E (16)	Wenn es neue Entwicklungen nach dem Stand von W&T gibt, sind diese in die Abläufe einzubringen (Hilfsmittel und Checklisten etc.).				

A.6 F: Qualitätssicherung

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
F (1)	Es gibt schriftlich festgelegte Bewertungsprozesse (z.B. QS-Plan, Revisionen) für alle relevanten Aspekte der Informationssicherheit IT-Sicherung.	I(j)(1)	Es gibt Bewertungsprozesse für die Sicherungsfunktion.		
		I(l)(4)	4) Es gibt dokumentierte und etablierte Überprüfungssysteme für Prozesse und Verfahren, um Kommentare und Beiträge von allen Stellen innerhalb der Organisation einzuholen.		
F (2)	Der Inhalt von QS-Plänen und Bewertungsprozessen ist dem Personal zugänglich und verständlich.				
F (3)	Für Bewertungsprozesse wird geeignetes und ausreichend viel Personal ausgewählt.				
F (4)	Personen, die interne Bewertungen, Revisionen etc. durchführen, arbeiten unabhängig und objektiv.				
F (5)	Die Rollenverteilung im Bewertungsprozess ist eindeutig.				
		I(j)(3)	Sicherungsprozesse werden gemäß den empfohlenen Qualitätssicherungsstandards vorbereitet, dokumentiert und gepflegt.		
F (6)	Die Bewertungsprozesse werden eingehalten.	I(j)(4)	Qualitätssicherungsmaßnahmen werden durchgesetzt.		
F (7)	Die Einhaltung der Bewertungsprozesse wird regelmäßig und fortlaufend überprüft.				
F (8)	Es gibt einen Revisionsplan (d.h. eine Zeitplanung, wann welche Revisionen durchzuführen sind), der fortlaufend gepflegt wird.				

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
F (9)	Bei der Durchführung von internen Bewertungsprozessen wird Wert auf offene und transparente Kommunikation gelegt.				
F (10)	Es steht ausreichend viel Zeit zur Vor- und Nachbereitung von Bewertungsprozessen (Revisionen, Interviews, …) zur Verfügung.				
F (11)	Zwischen Revisionsteam und zu prüfender Institution/Abteilung/etc. findet im Vorfeld eine Kommunikationsabsprache statt.				
F (12)	Die Durchführung von Interviews zu Bewertungszwecken folgt einem festen Schema und wird aufgezeichnet.				
F (13)	In regelmäßig durchgeführten Besprechungen des Managements werden auch Aspekte der Informationssicherheit adressiert. Hierbei werden auch regulatorische und unabhängige externe Bewertungen diskutiert.				
F (14)	Es erfolgen Vergleiche mit bewährten Praktiken im nationalen und internationalen Umfeld, um die eigenen Prozesse und Prüfmethoden an dem Stand von Wissenschaft und Technik auszurichten und zu aktualisieren.	I(j)(5)	Qualitätssicherungsprozesse werden regelmäßig anhand guter Praktiken für die Industrie bewertet.		
F (15)	Wird eine sich systematisch verschlechternde Qualität festgestellt, werden Ursachen und Strategien zur Verbesserung ermittelt.				

A.7 G: Änderungsmanagement

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
G (1)	Es existiert ein Änderungsmanagementprozess, der in die Geschäftsprozesse der Organisation integriert ist und die Auswirkungen von Änderungen auf die Geschäftsprozesse berücksichtigt. Vor der Änderung oder Beschaffung von Hardware oder Software werden insbesondere die menschlichen Faktoren berücksichtigt.	I(k)(1)	Es gibt Änderungsmanagementprozesse für Änderungen, die sich direkt und indirekt auf die Sicherheitsfunktion auswirken könnten.	3g)	Sicherheitsauswirkungen werden in Änderungsmanagementprozessen berücksichtigt: • Es sollten Prozesse für Änderungsmanagement und -kontrolle eingeführt werden, um die möglichen Auswirkungen von Änderungen an Verfahren und Ausrüstung und anderen verwalteten Änderungen auf die Sicherheit zu berücksichtigen.
G (2)	Für die Werkzeuge des Patch- und Änderungsmanagements existiert eine Sicherheitsrichtlinie.	I(k)(7)	Es werden grundlegende Standards in Prozessen und Anlagendesign festgelegt, von denen aus Änderungen vorgenommen und dokumentiert werden.		
G (3)	Es gibt feste Anforderungen und Rahmenbedingungen, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt werden.				
G (4)	Es gibt ein standardisiertes Verfahren, durch das Änderungsanforderungen hoher Wichtigkeit beschleunigt werden.				
G (5)	Alle Änderungsanforderungen werden zentral erfasst und dokumentiert.				
G (6)	Änderungsanforderungen werden vom Fachverantwortlichen für Patch- und Änderungsmanagement darauf kontrolliert, ob die	I(k)(4)	Während der Planung des Änderungsprozesses werden Bewertungen durchgeführt, um		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
	Aspekte der Informationssicherheit IT-Sicherung ausreichend berücksichtigt wurden.		festzustellen, ob die Änderung etablierte Sicherungsprozesse beeinträchtigen würde.		
G (7)	Änderungsanforderungen werden mit allen relevanten Zielgruppen abgestimmt und potenzielle Auswirkungen auf die Informationssicherheit IT-Sicherung berücksichtigt.	I(k)(8)	Vor der Änderung oder Anschaffung von Hardware, Software und Geräten werden Aufgabenanalysen durchgeführt, die menschliche Faktoren berücksichtigen.		
		I(k)(3)	Änderungen werden bewertet, um zu bestätigen, dass die gewünschten Ergebnisse erzielt wurden.		
G (8)	Bevorstehende Änderungen werden in Umfang und Art proaktiv und offen kommuniziert. Dabei werden sowohl unmittelbar als auch mittelbar Betroffene einbezogen.	I(k)(2)	Änderungen in Bereichen wie Betrieb, Sicherheit und Sicherung werden mit allen potenziell betroffenen Organisationen abgestimmt.	3g)	Sicherheitsauswirkungen werden in Änderungsmanagementprozessen berücksichtigt: • Das Personal sollte über bevorstehende Veränderungen in einer Weise informiert werden, die das Vertrauen innerhalb der Organisation aufrechterhält.
		I(k)(10)	Vor der Umsetzung von Änderungen an Prozessen, Einrichtungen oder Organisationsstrukturen, die die Sicherheit und Sicherung beeinträchtigen können, wird ein Kommunikationsprozess eingerichtet, um zu informieren und deren Einhaltung zu fördern.		
		I(k)(5)	Alle Mitarbeiter und Auftragnehmer, deren sicherheitsrelevante Aufgaben von Änderungen betroffen sind, erhalten die notwendige Schulung, um mit der Änderung umzugehen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(k)(6)	Es besteht Klarheit darüber, wer für die Durchführung sicherungsbezogener Arbeiten verantwortlich und rechenschaftspflichtig ist.		
G (9)	Neue Hardware inkl. Der zugehörigen Treibersoftware wird vor dem Einsatz auf Kompatibilität mit der eingesetzten Software und den relevanten Betriebssystemen geprüft.				
G (10)	Neue Hard- und Software wird vor dem Einsatz nach einem standardisierten Abnahme- und Freigabeverfahren getestet.	I(k)(9)	Tests werden durchgeführt, um sicherzustellen, dass ersetzte oder modifizierte Geräte wie erwartet funktionieren.		
G (11)	Die Authentizität und Integrität von Softwarepaketen wird während des gesamten Patch- und Änderungsprozesses anhand von Prüfsummen oder digitalen Signaturen überprüft.				

A.8 H: Sicherer Umgang mit Informationen

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
Sichere Email-Kommunikation					
H (1)	Die Email-basierte Kommunikation erfolgt gemäß den internen Regelungen (kein Zugriff von öffentlich zugänglichen IT-Systemen auf Emails etc.).				
H (2)	Die Regelungen für die Email-basierte Kommunikation orientieren sich am Stand von W&T (Verwendung kryptographischer Verfahren, Sicherheitsmechanismen beim Provider von Email-Diensten etc.).				
Sicherer Umgang mit Informationen im Unternehmen					
H (3)	Für den sicheren Umgang mit Informationen (auf Dienstreisen) existieren feste Vorgehensweisen und Regelungen.	I(g)(2)	Es gibt klare und wirksame Prozesse und Protokolle für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation.		
		I(g)(3)	Klassifizierte Informationen werden sicher getrennt, gespeichert und verwaltet.		
H (4)	Dem Personal sind alle relevanten Vorgehensweisen und Regelungen zum sicheren Umgang mit Informationen (auf Dienstreisen) bekannt.	I(g)(4)	Die Mitarbeiter sind sich der Bedeutung der Einhaltung der Informationskontrollen bewusst und verstehen sie.		
H (5)	Das Personal hält die Regeln zum sicheren Umgang mit Informationen auf Dienstreisen eigenverantwortlich ein.				

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
		I(g)(5)	IT-Systeme werden gewartet, um sicherzustellen, dass sie sicher sind, dass sie von einer geeigneten Behörde akkreditiert sind und gemäß den Verfahren betrieben werden.		
		I(g)(7)	Eine Informations- und Informationssicherheitsfunktion ist eingerichtet, finanziert, personell besetzt und sichtbar.		
		I(g)(8)	Manager engagieren sich voll und ganz für Initiativen zur Informationssicherheit und unterstützen diese.		
		I(g)(10)	Sowohl innerhalb als auch außerhalb der Organisation wurden klare und effektive Prozesse und Protokolle für den Betrieb von IT-Systemen erstellt.		
Sicherer Umgang mit Informationen auf Reisen					
H (6)	Vor Auslandsreisen werden mögliche länderspezifische Regelungen identifiziert.				
H (7)	Das Personal teilt bevorstehende (Auslands-) Reisen rechtzeitig dem Vorgesetzten sowie Verantwortlichen Personen bzgl. Informationssicherheit mit.				

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
H (8)	Der sichere Umgang mit Informationen auf (Auslands-)Reisen wird von Führungskräften regelmäßig betont und überprüft. Dies beinhaltet: • Sicherer Umgang mit mobilen Datenträgern • Sicheres Vernichten von schutzbedürftigen Materialien und Dokumenten • Verwendung von Sichtschutzfolien • Sicherstellung der Abstrahlsicherheit • Verwendung von Diebstahlsicherungen • Verschlüsselung tragbarer IT-Systeme und Datenträger • Umgehendes Melden von Diebstahl oder Verlust von Informationen, IT-Systemen oder Datenträgern				
Zugriffs-, Zugangs- und Zutrittsrechte					
H (9)	Der Zugang zu Informationen ist auf diejenigen beschränkt, die diesen Zugang zur Erfüllung ihrer Aufgaben benötigen.	I(g)(6)	Der Zugang zu Informationen ist auf diejenigen beschränkt, die diesen Zugang zur Erfüllung ihrer Aufgaben benötigen, über die erforderlichen Befugnisse verfügen und einer der Sensibilität der Informationen angemessenen Vertrauenswürdigkeitsprüfung unterzogen wurden.		
H (10)	Der Zugang zu Informationen ist durch Zugriffskontroll- und Authentisierungsmechanismen und Identifikation zu verifizieren.				
		I(g)(1)	Klassifizierungs- und Kontrollanforderungen sind klar dokumentiert und vom Personal gut verstanden.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
H (11)	Die Qualität dieser Zugriffs-, Authentisierungs- und Identifikationsmechanismen ist festzulegen. (Mehr-Faktor Authentifizierung bei weitreichenden Berechtigungen, Zurücksetzen von Passwörtern, Änderung von Passwörtern nach Sicherheitsvorfällen etc.).				
H (12)	Der Passwortgebrauch ist genau festgelegt und das Personal kennt alle Regeln im Umgang mit Passwörtern.				
H (13)	Es gibt (dokumentierte) Zutrittsberechtigungen (z.B. mit Chipkarten), die auf diejenigen beschränkt sind, die Zutritt benötigen.				
Vertraulichkeit von Informationen					
H (14)	Es gibt klare und wirksame Verfahren und Protokolle für die Klassifizierung und den Umgang mit Informationen innerhalb und außerhalb der Organisation.				
H (15)	Verschlusssachen werden sicher abgetrennt, gespeichert und verwaltet.				
H (16)	Unternehmen und Organisationen sollten über Systeme, Prozesse und Kompetenz haben, um allen Mitarbeitern Informationen über Bedrohungen auf ihre Sicherheitsfreigabe und ihre Rolle zugeschnitten sind. Sie sollten auch über ein ein effektives Sicherheitsrisikoregister und ein System zur Kommunikation von Risiken haben; Diese Risiken sollten auch in die Ausbildung und Entwicklung einfließen.				

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
H (17)	Die Bedeutung von Vertraulichkeit und Integrität von gesicherten Daten/Informationen ist bekannt und die Daten werden mit technischen Maßnahmen (z.B. Kryptografie) so gesichert, dass ihre Vertraulichkeit und Integrität gewahrt wird.				
H (18)	Daten/Informationen sind wertvoll und müssen vor Verlust geschützt werden (z.B. Gewährleistung der Wiederherstellbarkeit).				
H (19)	Benutzer kennen die Gefahren von Rest- und Zusatzinformationen in Dokumenten und Dateien und wissen, wie man unerwünschte Restinformationen ausschließt (z.B. vor Weitergabe).				
Aufzeichnungen					
		I(q)(1)	Die Führung von Aufzeichnungen erfüllt die Anforderungen zur Unterstützung des wirksamen Funktionierens des Sicherungssystems und seiner Bewertung.		
		I(q)(2)	Aufzeichnungen und Logbücher sind benutzerfreundlich und leicht zugänglich.		
		I(q)(3)	Aufzeichnungen werden ausgewertet, und es gibt ein Verfahren zur Gewinnung relevanter Informationen aus aktuellen Aufzeichnungen und Logbüchern sowie aus Archiven.		
		I(q)(4)	Es gibt einen Mechanismus zum Schutz vertraulicher Aufzeichnungen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur IAEA GS-G 3.5	
		I(q)(5)	Logbücher werden korrekt verwendet und vom Management überprüft.		

A.9 I: Einstellungen und Erwartungen

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Einstellungen und Überzeugungen					
				1d)	Einzelpersonen sind davon überzeugt, dass Sicherheit und Produktion Hand in Hand gehen: • Manager sollten besonders sensibel auf Entscheidungen reagieren, die die Produktion oder andere Faktoren über die Sicherheit zu stellen scheinen, und sollten darauf achten, solche Entscheidungen dem Personal zu erklären.
		I(j)(2)	Mitarbeiter in der gesamten Organisation wissen, dass das Managementsystem für die Sicherungsfunktion und die Aufrechterhaltung des nuklearen Sicherungssystems relevant ist.	1d)	Einzelpersonen sind davon überzeugt, dass Sicherheit und Produktion Hand in Hand gehen: • Manager und Vorgesetzte sollten regelmäßig kommunizieren, wie wichtig es ist, die Sicherheit zu gewährleisten und gleichzeitig die Produktions- und Leistungsanforderungen zu erfüllen.
		III(e)(4)	Mitarbeiter und Auftragnehmer glauben, dass eine glaubwürdige Bedrohung besteht.		
		III(e)(6)	Mitarbeiter und Auftragnehmer sind sich einer potenziellen Bedrohung durch Innentäter und deren Folgen bewusst.		
		III(e)(7)	Mitarbeiter und Auftragnehmer vermeiden Selbstgefälligkeit und können ihre Manifestationen erkennen.		
		III(e)(8)	Mitarbeiter und Auftragnehmer akzeptieren und verstehen die Notwendigkeit einer		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			wachsamen und aufmerksamen Haltung zu jeder Zeit.		
Erwartungen					
		II(a)(1)	Führungskräfte haben spezifische Erwartungen an die Leistung in Bereichen, die das nukleare Sicherungssystem betreffen, und teilen diese ihren Mitarbeitern und Auftragnehmern mit.	2b)	Die Verpflichtung zur Sicherheit ist auf allen Managementebenen offensichtlich: • Manager sollten klare Leistungserwartungen in sicherheitsrelevanten Bereichen formulieren und diese gegebenenfalls dokumentieren.
		II(a)(3)	Führungskräfte gehen mit gutem Beispiel voran und verhalten sich – wie von allen Mitarbeitern erwartet – in ihrem persönlichen Verhalten an Richtlinien und Prozesse.	2b)	Die Verpflichtung zur Sicherheit ist auf allen Managementebenen offensichtlich: • Manager sollten sich bei ihrem eigenen Verhalten strikt an Richtlinien und Verfahren halten und keine Sonderbehandlung erwarten oder akzeptieren.
		II(a)(4)	Führungskräfte überprüfen persönlich die Leistung vor Ort, indem sie Begehungen durchführen, den Mitarbeitern zuhören und die durchgeführten Arbeiten beobachten und dann Maßnahmen ergreifen, um Mängel zu beheben.	2a)	Die Geschäftsleitung ist eindeutig der Sicherheit verpflichtet • Leitende Unternehmensleiter sollten regelmäßig Betriebsanlagen besuchen, um die Wirksamkeit des Managements aus erster Hand zu beurteilen.
		II(a)(7)	Führungskräfte unterstützen sichtbar das hohe Sicherungsniveau, das in einer Sicherungsrichtlinie oder einem Verhaltenskodex definiert ist.	2a)	Die Geschäftsleitung ist eindeutig der Sicherheit verpflichtet • Führungskräfte sollten Vorgesetzte als wesentlichen Teil des Managementteams bei der Umsetzung der Sicherheitskultur in die Praxis behandeln und ihnen ihre volle Unterstützung zukommen lassen.
		II(a)(8)	Manager machen ihre Sicherungsverpflichtung gegenüber allen Mitarbeitern und Auftragnehmern bekannt und stellen gleichzeitig		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			sicher, dass diese Verpflichtung in die tägliche Routine umgesetzt wird.		
		II(a)(9)	Führungskräfte bieten fortlaufende Überprüfungen der Leistung der zugewiesenen Rollen und Verantwortlichkeiten, um die Erwartungen zu stärken und sicherzustellen, dass die wichtigsten Sicherungsaufgaben erfüllt werden.	2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen. • Manager sollten die Leistung einzeln notieren und die Bedingungen vor Ort inspizieren, indem sie um die Anlage herumgehen und Personen beobachten und ihnen zuhören, und sollten energisch eingreifen, um Sicherheitsprobleme zu beheben („gehen, schauen, zuhören und reparieren“). • Vorgesetzte sollten Zeit damit verbringen, Einzelpersonen an ihren Arbeitsplätzen zu beobachten und zu coachen, und sollten das erwartete Verhalten fördern und verstärken.
		II(a)(10)	Mitarbeiter und Auftragnehmer können beschreiben, wie Manager Baustellen inspizieren, um sicherzustellen, dass Verfahren gemäß den Erwartungen verwendet und befolgt werden.		
		II(a)(12)	Mitarbeiter und Auftragnehmer können Beispiele für hohe Erwartungen von Führungskräften an die Sicherung nennen.		
				2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen: • Manager sollten in der Lage sein, Bedingungen verschlechterter Sicherheit (physisch oder organisatorisch) zu erkennen.
				2b)	Die Verpflichtung zur Sicherheit ist auf allen Managementebenen offensichtlich

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					• Führungskräfte sollten mangelhafte Leistungen in Bezug auf die Sicherheit aus keinem Grund tolerieren oder ignorieren.
		II(a)(5)	Führungskräfte zeigen ein Gefühl der Dringlichkeit, signifikante Sicherungsschwächen oder Sicherungslücken zu beheben.	2b)	Die Verpflichtung zur Sicherheit ist auf allen Managementebenen offensichtlich: • Manager sollten ein Gefühl der Dringlichkeit bei der Behebung erheblicher Schwächen oder Schwachstellen zeigen.
				2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen • Manager sollten sicherstellen, dass sicherheitswidrige Situationen behoben werden.
				2e)	Die Geschäftsführung stellt sicher, dass es genügend kompetente Personen gibt: • Der Personalbestand sollte den Anforderungen zur Gewährleistung von Sicherheit und Zuverlässigkeit entsprechen.
		II(a)(13)	Senior Manager ermutigen die Belegschaft, sich andere Organisationen oder andere Teile ihrer eigenen Organisation anzusehen, um zu sehen, was sie von ihnen lernen können.		

A.10 J: Führungs- und Personalverhalten

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(b)(2)	Führungskräfte machen sich ansprechbar und ermöglichen eine effektive Zwei-Wege-Kommunikation und ermutigen Mitarbeiter, Bedenken oder Verdächtigungen zu melden, ohne befürchten zu müssen, später Disziplinarmaßnahmen zu erleiden.		
		II(b)(3)	Führungskräfte missbrauchen ihre Autorität nicht, um die Sicherung zu umgehen.		
		II(b)(4)	Führungskräfte verbringen regelmäßig Zeit damit, Mitarbeiter und Auftragnehmer an ihren Arbeitsorten zu beobachten und zu schulen.	3c)	Es besteht ein hohes Maß an Einhaltung von Vorschriften und Verfahren: • Manager und Vorgesetzte sollten Arbeitsplätze häufig inspizieren, um sicherzustellen, dass die Verfahren gemäß den Erwartungen angewendet und befolgt werden.
				2i)	Beziehungen zwischen Managern und Einzelpersonen basieren auf Vertrauen: • Manager sollten das tun, wozu sie sich in ihrer Kommunikation verpflichten. • Führungskräfte sollten sich darauf verlassen können, dass sie professionell handeln, wenn Mitarbeiter Sicherheitsbedenken äußern oder Beinahe-Unfälle melden. • Manager sollten sicherstellen, dass die Kommunikation in der Organisation nicht erstickt wird, und unverzüglich Maßnahmen ergreifen, um solchen Auswirkungen entgegenzuwirken.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(b)(5)	Führungskräfte stellen sicher, dass sie die Sicherungsleistung ihrer Organisation verstehen und Maßnahmen ergreifen, um eine angemessene Aufsicht über die Sicherung aufrechtzuerhalten.		
		II(b)(6)	Führungskräfte schätzen die Bedeutung der Sicherungskultur bei der Erfüllung von Sicherungsaufgaben.		
		II(b)(7)	Führungskräfte stellen sicher, dass eine sicherungsbewusste Umgebung das gesamte Unternehmen durchdringt.		
		III(a)(5)	Mitarbeiter und Auftragnehmer halten die sicherungsbezogenen Aspekte ihrer Arbeit für wertvoll und wichtig.		
		III(a)(7)	Mitarbeiter und Auftragnehmer sind bereit, bei Bedarf Situationen anzugehen, denen sie zuvor noch nicht begegnet sind und für die sie keine Anleitung haben.		
		III(a)(8)	Die nukleare Sicherungsarbeit gilt als respektabler und karrierefördernder Beruf für qualifiziertes Personal.		
		III(a)(11)	Sicherungspersonal nimmt an professionellen Organisationen und Gruppen teil, sowohl innerhalb als auch außerhalb der Einrichtung.		
		III(a)(12)	Es werden Papiere veröffentlicht und Präsentationen von Mitarbeitern zu Fragen der nuklearen Sicherung gehalten.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
				3e)	„Eigentum“ für die Sicherheit ist auf allen Organisationsebenen und für alle Mitarbeiter offensichtlich: • Der Einzelne sollte seine eigenen Ziele in Bezug auf die Sicherheit haben und sollte ständig nach Verbesserungen suchen. • Der Einzelne sollte für die Sicherheit in seiner eigenen Arbeitsumgebung sorgen.
		III(b)(3)	Verhalten, das die Sicherungskultur verbessert, wird von Kollegen verstärkt.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflichtiges Verhalten sollte von Managern und Kollegen positiv bestärkt werden.
		III(b)(8)	8) Es können Belege dafür angeführt werden, dass Mitarbeiter und Auftragnehmer ermutigt werden, Rat einzuholen oder weitere Informationen einzuholen, wenn sie Zweifel an der Sicherheit haben.		

A.11 K: Motivation, Fehlerkultur, Selbsteinschätzung, Leistungsmessung

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Motivation					
K (1)	Führungskräfte leben vorbildhaftes, sicherungsbezogenes Verhalten in Worten und Taten vor.				
		II(h)(8)	Das Fachwissen und die speziellen sicherheitsrelevanten Fähigkeiten von Einzelpersonen werden von der Organisation anerkannt, genutzt und belohnt, unabhängig von ihrer formalen Stellung innerhalb der Organisation.		
		II(h)(1)	Führungskräfte ermutigen, erkennen und belohnen lobenswerte Einstellungen und Verhaltensweisen.	4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt: • Anerkennung sollte Einzelpersonen und Teams für vorbildliche Leistungen gegeben werden.
		III(a)(2)	Mitarbeiter sind stolz auf ihre Arbeit.	4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt: • Der Einzelne sollte stolz auf seine Arbeit sein und das Gefühl haben, dass seine Aufgaben und Leistungen einen wichtigen Beitrag zum Erfolg der Organisation leisten.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		III(a)(3)	Mitarbeiter helfen sich gegenseitig und zeigen professionelle Höflichkeit und Respekt im Umgang miteinander.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Einzelpersonen sollten sich gegenseitig helfen, ihre Verantwortlichkeiten zu erfüllen.
Fehlerkultur					
		I(a)(13)	Es gibt eine gut definierte und weithin bekannte Praxis, die Umsetzung der Richtlinien der nuklearen Sicherung zu fördern, wobei Belohnung oder Anerkennung direkt oder indirekt mit der Erreichung ihrer Ziele verbunden sind.		
K (2)	Führungskräfte machen das Personal für ihr Verhalten verantwortlich.	II(b)(5)	Führungskräfte machen Menschen für ihr Verhalten verantwortlich.		
K (3)	Fehler können auch gegenüber höherrangigem Personal benannt werden.			4f)	Faktoren, die die Arbeitsmotivation und Arbeitszufriedenheit beeinflussen, werden berücksichtigt: • Das Belohnungssystem sollte auf Sicherheitsrichtlinien abgestimmt sein und das gewünschte Verhalten und die gewünschten Ergebnisse verstärken.
K (4)	Vorbildliches Verhalten wird hervorgehoben und honoriert. Vorsätzliche Nichteinhaltungen von Regeln werden in angemessener	III(c)(2)	Sichtbare Sanktionen sind vorhanden und werden angewandt, um das Personal zu ermutigen, Prozeduren zu befolgen.	3e)	„Eigentum“ für die Sicherheit ist auf allen Organisationsebenen und für alle Mitarbeiter offensichtlich: • Vorgesetzte sollten gute Sicherheitspraktiken fördern.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
	Weise sanktioniert. Dabei sind die unterschiedliche Wirkung von Sanktionen und Belohnung auf verschiedene Charaktere sowie die Vor- und Nachteile der verwendeten Methoden zu beachten (z.B. Verschlechterung der Beziehung und Kommunikation zum Vorgesetzten bei Anwendung von Sanktionsmethoden).	I(h)(4)	Die Mitarbeiter kennen die Belohnungs- und Sanktionssysteme im Zusammenhang mit der nuklearen Sicherung.		
		I(h)(6)	6) Bei der Anwendung von Disziplinarmaßnahmen bei Verstößen werden die Sanktionen für selbst gemeldete Verstöße gemildert, um die Meldung zukünftiger Verstöße zu fördern.		
		II(h)(3)	Belohnungssysteme erkennen den Beitrag des Personals zur Aufrechterhaltung der nuklearen Sicherung an.		
Selbsteinschätzung					
		I(n)(1)	Ein Selbsteinschätzungsprogramm wird mit einem Plan dokumentiert, der Selbsteinschätzungsprozesse definiert.	5c)	Interne und externe Bewertungen, einschließlich Selbstbewertungen, werden verwendet: • Verschiedene Aufsichtsforen und -prozesse, einschließlich der Selbstbewertung, sollten genutzt werden, um die Sicherheitsleistung der Organisation zu überprüfen, zu bewerten und zu verbessern. • Anzahl und Art der Aufsichtsmechanismen sollten regelmäßig überprüft und angepasst werden. • Aufsicht ist positiv zu sehen und externe oder unabhängige Meinungen sollten konstruktiv genutzt werden.
		I(n)(2)	Erkannte Mängel werden analysiert, um aufkommende Muster und Trends zu erkennen und zu korrigieren.	5c)	Interne und externe Bewertungen, einschließlich Selbstbewertungen, werden verwendet: • Periodische Bewertungen der Sicherheitskultur sollten durchgeführt und als

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					Grundlage für Verbesserungen verwendet werden
		I(n)(3)	Human-Faktor-Methoden werden in Problemanalysetechniken integriert.	5c)	Interne und externe Bewertungen, einschließlich Selbstbewertungen, werden verwendet: • Führungskräfte sollten regelmäßig informiert werden und Maßnahmen auf der Grundlage der Ergebnisse der Aufsichtstätigkeiten einleiten.
		I(n)(4)	Die Leistung wird einem Benchmarking unterzogen, um den Betrieb mit nationalen und internationalen bewährten Verfahren zu vergleichen.		
		I(n)(5)	Die operative Leistung wird beobachtet, um zu bestätigen, dass die Erwartungen erfüllt werden.		
		I(n)(6)	Auf der Grundlage der Ergebnisse der Selbstbewertung werden Korrekturmaßnahmenpläne entwickelt und die Umsetzung dieser Pläne verfolgt.		
		I(n)(7)	Die Bewertung von Sicherungssystemen berücksichtigt die aktuelle DBT-Bewertung und regulatorische Anforderungen.		
		I(n)(8)	Mitarbeiter und Auftragnehmer sind sich ihrer Verantwortung für Verbesserungen bewusst, die als Ergebnis von Sicherungsbewertungen eingeführt wurden.		
		I(n)(9)	Führungskräfte spielen eine sichtbare Rolle bei der Förderung, Vorbereitung und Durchführung der Selbstbewertung.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(n)(10)	Die Mitglieder der Organisation betrachten Assessments, Reviews und Audits als Chance und nicht als Belastung.		
		I(n)(11)	Es gibt ein etabliertes Verfahren zur kontinuierlichen Überwachung der Sicherheitskultur durch den Einsatz von Indikatoren, um Verbesserungen umzusetzen und eine Verschlechterung der nuklearen Sicherheitskultur zu verhindern.		
		I(n)(12)	Führungskräfte messen, inwieweit Schulungsprogramme zu einer Verbesserung der Einstellung zur Sicherungskultur beitragen.		
		I(n)(13)	Mitarbeiter und Auftragnehmer können Beispiele für von der Geschäftsleitung eingeleitete Maßnahmen nennen, die auf den Ergebnissen von Bewertungen der Sicherungskultur basieren.		
		I(n)(14)	Die Ergebnisse der Selbstbewertung werden im Rahmen des Austauschs bewährter Verfahren so weit wie möglich branchenweit ausgetauscht.		
Leistungsmessung					
		II(d)(1)	Manager verbringen regelmäßig Zeit damit, die Leistung der Mitarbeiter an ihrem Arbeitsplatz zu beobachten, zu korrigieren und zu verstärken.	2c)	Es gibt sichtbare Führungsqualitäten, die die Beteiligung des Managements an sicherheitsbezogenen Aktivitäten zeigen: • Manager sollten Mitarbeiter an ihren Arbeitsplätzen besuchen.
		II(g)(1)	Mitarbeiter aller Ebenen werden ermutigt, Probleme zu melden und Vorschläge zur Verbesserung der	5b)	Offenes Melden von Abweichungen und Fehlern wird empfohlen:

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			Leistung des nuklearen Sicherungssystems zu machen.		• Die Organisation sollte über eine Vielzahl etablierter Prozesse verfügen, um Einzelpersonen zu ermöglichen und zu ermutigen, ungewöhnliche Zustände, Bedenken und Ereignisse, einschließlich Beinaheunfälle, zu melden. • Anerkennung sollte Einzelpersonen und Teams gegeben werden, die ungewöhnliche Zustände, Bedenken und Ereignisse, einschließlich Beinaheunfälle, melden. • Einzelpersonen sollten sich wohl fühlen, Sicherheitsbedenken zu äußern, ohne Angst vor Vergeltung zu haben. • Manager sollten sicherstellen, dass auf die angesprochenen Angelegenheiten reagiert wird und dass Feedback zu den Ergebnissen gegeben wird.
		II(g)(2)	Die Ursachen von Sicherungsereignissen und negativen Trends werden identifiziert und korrigiert.		
		II(g)(3)	Bei der Analyse und Nachverfolgung von Ereignissen oder ungewöhnlichen Ereignissen werden nicht nur die tatsächlichen, sondern auch die möglichen Folgen jedes Vorfalls berücksichtigt.		
		II(g)(4)	Wenn ein Fehler oder ein Ereignis auftritt, wird die Frage gestellt: Was ist schiefgelaufen? Und nicht Wer lag falsch?, mit dem Fokus auf Verbesserung und nicht auf Schuldzuweisung.		
		II(g)(5)	Es gibt ein Verfahren für alle Mitarbeiter, um Bedenken hinsichtlich der nuklearen Sicherung direkt bei unmittelbar Vorgesetzten, leitenden Angestellten		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
			und Aufsichtsbehörden oder anderen Stellen anzusprechen.		
		II(g)(6)	Relevante Sicherungsindikatoren werden an Mitarbeiter und Auftragnehmer kommuniziert.		
		II(g)(7)	Senior Manager zeigen, dass die beruflichen Fähigkeiten, Werte und Erfahrungen der Mitarbeiter das wertvollste strategische Kapital des Unternehmens für die Sicherung sind.		
		II(g)(8)	Führungskräfte zeigen ein starkes Engagement für den Aufbau einer „lernenden Organisation“, d. h. einer, die das Lernen aus internen und externen Quellen schätzt und sich verpflichtet, die Sicherungsleistungen als Ergebnis dieses Lernens zu verbessern.		
		II(g)(9)	Führungskräfte überprüfen häufig die Arbeit, um sicherzustellen, dass die Verfahren gemäß den Erwartungen verwendet und befolgt werden.		
		II(g)(10)	Die Führungskräfte sorgen für kontinuierliche und umfassende Nachverfolgung von Maßnahmen, die die sicherungsbezogene menschliche Leistung betreffen.		
		II(g)(11)	Senior Manager stellen sicher, dass aus der Analyse von Ereignissen relevante Informationen abgeleitet werden, die zur Verbesserung der Sicherungsleistung verwendet werden können.		
		II(g)(12)	Führungskräfte und zuständige Mitarbeiter kennen bewährte Praktiken in Bezug auf die nationale und internationale Sicherung.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		II(g)(13)	Wenn Abweichungen von einem Verfahren erforderlich sind, gibt es ein effizientes und effektives Mittel, um diese richtig zu verwalten.		
		II(g)(14)	Human Factors Spezialisten und Psychologen sind mit der Organisation beschäftigt.		
		II(g)(9)	Die Grundsätze zur Belohnung guter Leistung im Bereich Sicherung spiegeln die Grundsätze wider, die zur Belohnung guter Leistungen im Bereich Sicherheit und Betrieb verwendet werden.		
		I(l)(3)	Berichte werden vom Management überprüft, wobei Maßnahmen ergriffen werden, um sicherzustellen, dass die Organisation aus den Erfahrungen lernt, um ihre Leistung zu verbessern.		
		II(h)(5)	Jährliche Leistungsbewertungen enthalten einen Abschnitt über Leistung und Bemühungen zur Unterstützung der nuklearen Sicherung.		
		II(h)(7)	Leistungsverbesserungsprozesse ermutigen die Mitarbeiter, innovative Ideen zur Verbesserung der Sicherungsleistung anzubieten und geeignete Lösungen zu finden.	1f)	Sicherheitsbewusstes Verhalten wird gesellschaftlich akzeptiert und unterstützt (sowohl formell als auch informell): • Der Leistungsbewertungsprozess sollte sicherheitsbewusstes Verhalten erkennen und belohnen. • Kollegen sollten sich gegenseitig zu sicherheitsbewusstem Verhalten ermutigen.
		I(c)(1)	Die Organisation verwendet Benchmarks und Ziele, um die Leistung auf allen Ebenen zu verstehen, zu erreichen und zu verbessern.	5f)	Sicherheitsleistungsindikatoren werden verfolgt, verfolgt und bewertet und darauf reagiert: • Die Organisation sollte Maßnahmen und Ziele verwenden, um die Sicherheitsleis-

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
					tung auf allen Ebenen zu erklären, aufrechtzuerhalten und zu verbessern.
		I(c)(2)	Leistungsergebnisse im Vergleich zu den Zielen werden regelmäßig an die Mitarbeiter kommuniziert.	5f)	Sicherheitsleistungsindikatoren werden verfolgt, verfolgt und bewertet und darauf reagiert: • Ergebnisse in Bezug auf die Sicherheitsleistung sollten regelmäßig mit Zielen verglichen und die Ergebnisse des Vergleichs sollten dem Personal mitgeteilt werden.
		I(c)(3)	Maßnahmen werden ergriffen, wenn die Leistung der nuklearen Sicherung nicht vollständig ihren Zielen entspricht.	5f)	Sicherheitsleistungsindikatoren werden verfolgt, verfolgt und bewertet und darauf reagiert: • Es sollten Maßnahmen ergriffen werden, wenn die Sicherheitsleistung nicht mit ihren Zielen, Strategien, Plänen und Zielen übereinstimmt.
		I(c)(4)	Effiziente Leistung, die zu mehr Sicherung führt, wird belohnt.	5f)	Sicherheitsleistungsindikatoren werden verfolgt, verfolgt und bewertet und darauf reagiert: • Die Ursachen sicherheitsrelevanter Ereignisse und nachteiliger Trends sollten identifiziert und in Übereinstimmung mit einem festgelegten Zeitrahmen behandelt werden. • Die Fallstricke bei der Konzentration auf eine zu enge Reihe von Sicherheitsleistungsindikatoren sollten erkannt werden. • Die Organisation sollte wachsam sein, um mögliche Anzeichen einer nachlassenden Sicherheitsleistung zu erkennen und darauf zu reagieren.
		I(c)(5)	Aufsichtliche und unabhängige Bewertungen der Sicherungsleistung werden bei Management- und anderen Sitzungen erörtert.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(c)(6)	Die Organisation überwacht die Leistung aktiv und systematisch auf vielfältige Weise, z.B. durch Management-Rundgänge, Meldung von Problemen, Indikatoren, Trendanalysen, Benchmarking, Überprüfungen von Branchenerfahrungen, Selbstbewertungen und Leistungsbewertungen.		

A.12 L: Zuverlässigkeit

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur, IAEA GS-G 3.5	
L (1)	Die Organisation verfügt über schriftliche Richtlinien, Regeln und Verfahren für die Einstellung von Mitarbeitern.				
		I(i)(1)	Dokumentierte Personal-und-Auftragnehmer-Screening-Prozesse werden auf die Risiken und Bedrohungen abgestimmt, die mit den spezifischen Beschäftigungsrollen und Verantwortlichkeiten verbunden sind. Gegebenenfalls muss das Screening regelmäßig durchgeführt werden.		
		I(i)(3)	Screening-Prozesse werden streng befolgt, unterliegen der Aufsicht und Auditierung, sind für alle Ebenen der Organisation erforderlich und werden auf alle Ebenen angewandt, einschließlich Zeitarbeitskräfte, Auftragnehmer und Besucher.		
		I(i)(4)	Echte oder offensichtliche Fehler der Screening-Prozesse werden angemessen untersucht und beurteilt.		
L (2)	Es gibt ein wirksames Programm zur Eindämmung von Innentäter-Bedrohungen, das zwischen allen Bereichen der Sicherheits- und Betriebsorganisationen koordiniert wird.	I(i)(8)	Es gibt ein wirksames Programm zur Eindämmung von Insider-Bedrohungen, das zwischen allen Aspekten der Sicherung und des Betriebs koordiniert wird.		
L (3)	Die Vertrauenswürdigkeit des Personals wird bei der Einstellung und danach in regelmäßigen Abständen nach einem standardisierten Verfahren überprüft. Das Verfahren zur Feststellung der Vertrauenswürdigkeit ist in der Lage, spezifische Risikofaktoren zu	I(i)(2)	Der Prozess der Vertrauenswürdigkeitsbestimmung ist in der Lage, spezifische Sicherheitsrisikofaktoren zu identifizieren, z.B. psychische Erkrankungen und Drogen-/ Alkoholmissbrauch.		

	erkennen, z. B. psychische Erkrankungen und Drogen-/Alkoholmissbrauch.				
		I(i)(7)	Der Screening-Prozess sollte Faktoren berücksichtigen, die zu einer Verschlechterung der Vertrauenswürdigkeit führen können, wie Drogenmissbrauch, Gewalt am Arbeitsplatz oder kriminelles und abweichendes Verhalten.		
L (4)	Soll einem Mitarbeiter der Zutritt zu Hochsicherheitsbereichen oder der Zugriff zu hochsensiblen Daten gewährt werden, wird eine gesonderte Prüfung der Vertrauenswürdigkeit durchgeführt.				
L (5)	Es gibt eine standardisierte Vorgehensweise zur Koordination mit Dienstleistern und Auftragnehmern bezüglich der Vertrauenswürdigkeit von deren Angestellten.				
L (6)	Es werden schriftliche Vereinbarungen zur Vertrauenswürdigkeit von Angestellten mit Dienstleistern und Auftragnehmern geschlossen.				
L (7)	Bei Arbeiten und Tätigkeiten mit Bedeutung für die Informationssicherheit wird stets das 2-Personen-Prinzip angewendet.				
L (8)	Führungspositionen und weitere für die Informationssicherheit bedeutsame Positionen (z.B. Administrator) werden erst nach einer Prüfung der Vertrauenswürdigkeit der Kandidaten besetzt.				

L (9)	Personalbewertungen finden regelmäßig und unabhängig von der Hierarchieebene statt.				
		I(i)(5)	Mitarbeiter sind sich der Bedeutung der Vertrauenswürdigkeitsbestimmung bewusst und verstehen sie.		
		I(i)(6)	Das Management und andere geeignete Mitarbeiter werden geschult, um sie bei der Identifizierung offensichtlicher Hochrisiko-Verhaltenssymptome und bei der Anwendung anderer ähnlicher Beobachtungs- und Analysefähigkeiten anzuleiten.		
		I(i)(9)	Der Prozess der Hintergrundüberprüfungen wird regelmäßig überprüft.		

A.13 M: Betrieb und Instandhaltung

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
		I(h)(1)	Betrieb und Instandhaltung werden gemäß genehmigten Prozessen und Lieferantenplänen durchgeführt, um sicherzustellen, dass die Konstruktionsanforderungen nicht beeinträchtigt werden.	5d)	Organisationserfahrung und Betriebserfahrung (sowohl innerhalb als auch außerhalb der Anlage) werden verwendet: • Es sollten Prozesse vorhanden sein, um verfügbare interne und externe sicherheitsrelevante Informationen, einschließlich Informationen über Erfahrungen aus anderen Branchen, zu erhalten, zu überprüfen und anzuwenden. • Berichte über Betriebserfahrungen sollten überprüft und Maßnahmen ergriffen werden, um sicherzustellen, dass die Organisation die relevanten Erkenntnisse lernt und anwendet. • Es sollte keine Anzeichen für eine Haltung von „hier kann es nicht passieren“ geben.
		I(h)(3)	Es werden Maßnahmen ergriffen, wenn Sicherungseinrichtungen zu Wartungszwecken außer Betrieb genommen werden oder wenn Ausfälle auftreten, um die betroffenen Einrichtungen zu kompensieren.		
		I(h)(4)	Betriebserfahrung mit Sicherungseinrichtung wird bei der Wartung und bei der Planung von Anschaffungen als unerlässlich angesehen.		
		I(h)(5)	Bei Entscheidungen über die Betriebszuverlässigkeit von Sicherungssoftware und -hardware		

			werden konservative Entscheidungsprinzipien angewandt.		
		I(h)(6)	Betriebs- und Wartungsverfahren wurden in Übereinstimmung mit den Bedrohungen eingerichtet, von denen die DBT (Design Basis Threat) abgeleitet wurden.		
		I(h)(7)	Reparaturen und Wartungen von Sicherungseinrichtungen und Hardware werden umgehend durchgeführt.		
		I(h)(8)	Prozesse werden effektiv und ohne die Tendenz verwendet, Abkürzungen zu nehmen, selbst wenn die Wartung hinter dem Zeitplan läuft.		
		I(h)(9)	Es gibt ein System zur Dokumentation historischer Daten zu Geräten und Wartungsmaßnahmen, die bei der Analyse der Zuverlässigkeit und des Wartungsbedarfs verwendet werden.		
		I(h)(10)	Es gibt Regeln, die maximale Verzögerungszeiten für die Reparatur von Sicherheitsausrüstung definieren und kontrollieren.		
		I(h)(12)	Es gibt Regeln für Ausgleichsmaßnahmen, wenn Sicherheitseinrichtungen außer Betrieb sind oder repariert werden.		
		I(h)(13)	Dem Betriebs- und Wartungspersonal wird die Möglichkeit geboten, Besprechungen zur Erörterung von Fragen von gemeinsamem Interesse abzuhalten.		

A.14 N: Kommunikation

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		II(f)(3)	Führungskräfte besuchen Mitarbeiter an ihren Arbeitsplätzen und führen offene Forumssitzungen durch, bei denen Mitarbeiter Fragen stellen können.		
		II(f)(4)	Führungskräfte begrüßen die Beiträge der Mitarbeiter und Auftragnehmern und ergreifen Sie		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
			Maßnahmen oder erklären, warum keine Maßnahmen ergriffen wurden.		
		II(f)(5)	Führungskräfte halten die Mitarbeiter über Änderungen der Politik und der Organisation auf hoher Ebene auf dem Laufenden.		
		II(f)(6)	Mitarbeiter und Auftragnehmer fühlen sich wohl, Fragen oder Bedenken zu äußern und zu diskutieren, da gute und schlechte Nachrichten sowohl geschätzt als auch geteilt werden.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		II(f)(7)	Es gibt Richtlinien, die das Recht und die Verantwortung der Mitarbeiter stärken, Sicherungsfragen mit verfügbaren Mitteln anzusprechen, einschließlich der Wege außerhalb ihrer Befehlskette.		
		II(f)(8)	Führungskräfte kommunizieren ihre Vision des Sicherungsstatus häufig, konsistent und auf unterschiedliche Weise.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		II(f)(10)	Die Sicherungsbedeutung von Regeln und Verfahren wird dem Personal klar kommuniziert und angemessen erklärt.		
		II(f)(11)	Alle Mitarbeiter sind sich einer klaren und ungehinderten Kommunikation innerhalb der Organisation bewusst, sowohl nach oben als auch nach unten.		
		II(f)(12)	Das Kommunikationssystem wird regelmäßig getestet, um zu überprüfen, ob die		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
			Informationen von Führungskräften von den Mitarbeitern aller Ebenen empfangen und verstanden werden.		
		II(f)(13)	Sicherungsrelevante Kommunikation steht im Einklang mit der Vertraulichkeitsrichtlinie.		
		II(f)(14)	In der Organisation werden Maßnahmen ergriffen, um Gruppendenken zu vermeiden und den Austausch gegensätzlicher Ansichten zu fördern.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		II(f)(15)	Es gibt Prozesse, um sicherzustellen, dass die Erfahrungen der leitenden Mitarbeiter mit neuen und jungen Mitarbeitern und Auftragnehmern in der Organisation geteilt werden.		
Kommunikation mit externen Organisationen					
		I(p)(1)	Es findet eine regelmäßige Kommunikation von Mitarbeitern und Managementebene mit lokalen und nationalen Organisationen statt, die sich mit der nuklearen Sicherung befassen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		I(p)(2)	Es bestehen schriftliche Vereinbarungen mit geeigneten Organisationen, um Hilfe, Kommunikation und rechtzeitige Reaktion auf Vorfälle zu erleichtern.		
		I(p)(3)	Es werden regelmäßig Sicherheitsübungen außerhalb und vor Ort durchgeführt, bei denen die gewonnenen Erkenntnisse in Verfahren und Absichtserklärungen einfließen.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		I(p)(5)	Externe Stakeholder werden konsequent in die Problemlösung und Entscheidungsfindung nach dem Need-to-know-Prinzip eingebunden.		
		I(p)(6)	Es gibt ein System für die Kommunikation und Zusammenarbeit mit aktuellen und potenziellen Lieferanten und Auftragnehmern, das sicherheitsrelevante Themen abdeckt.		
		I(p)(7)	Die Teilnahme an anerkannten Kursen und Veranstaltungen (z.B. von der IAEA einberufenen)		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
			wird von der Geschäftsführung gefördert und unterstützt.		
		I(p)(8)	Dem zuständigen Personal stehen internationale Veröffentlichungen und Berichte zur nuklearen Sicherung zur Verfügung.		
		I(p)(9)	Die Organisation beteiligt sich an der internationalen Zusammenarbeit in Fragen der nuklearen Sicherung.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		I(p)(10)	Informationen über die nukleare Sicherung aus internationalen Veröffentlichungen werden, wenn möglich, in einer Sprache zur Verfügung gestellt, die von der Belegschaft verstanden wird.		
Schnittstelle zur Überwachungsbehörde					
		I(o)(1)	Zwischen der Aufsichtsbehörde und der Organisation werden Informationen frei und regelmäßig ausgetauscht.	3a)	Es besteht eine angemessene Beziehung zur Regulierungsbehörde, die gewährleistet, dass die Verantwortung für

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
					die Sicherheit beim Lizenznehmer verbleibt: • Der Regulierungsbehörde sollten vollständige und genaue Informationen zur Verfügung gestellt werden. • Die Regulierungsbehörde sollte konsultiert werden, um alle erforderlichen Klärungen und Anleitungen zu Regulierungsfragen zu erhalten.

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
					• Der Lizenznehmer sollte von der Regulierungsbehörde als offen und zeitnah in seiner Berichterstattung und Interaktion angesehen werden.
		I(o)(2)	Informationen über Schwachstellen und Bedrohungen werden zeitnah gegenseitig weitergegeben.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		I(o)(3)	Die Rollen der regulatorischen Schnittstellen sind klar definiert und die behördenübergreifenden Prozesse werden gestrafft.		
		I(o)(4)	Nukleare Sicherungsvorfälle werden der Aufsichtsbehörde gemeldet.		
		I(o)(5)	Die Mitglieder der Organisation verstehen die Verantwortung der Aufsichtsbehörde vollständig.		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
		I(o)(6)	Die Mitglieder der Organisation zeigen Respekt vor der Aufsichtsbehörde, und ihre Mission genießt sichtbare Unterstützung und Zusammenarbeit von Managern.		
		I(o)(7)	Mitarbeiter und Auftragnehmer bewerten die Anwesenheit der Aufsichtsbehörde auf dem Gelände positiv.		
		I(o)(8)	Der Betreiber stellt der Aufsichtsbehörde (oder einer anderen relevanten zuständigen		

Informationssicherheitskultur		Sicherungskultur nach IAEA NSS No 7 + 28-T		Sicherheitskultur nach IAEA GS-G 3.5	
Interne Kommunikation					
		II(f)(1)	Führungskräfte sorgen dafür, dass Kommunikation wertgeschätzt wird und potenzielle Kommunikationsblockaden behoben werden.	3d)	Das Management delegiert die Verantwortung mit angemessener Befugnis, um die Schaffung klarer Verantwortlichkeiten zu ermöglichen: • Rechenschaftspflicht sollte positiv und nicht negativ als eine Möglichkeit der Schuldzuweisung wahrgenommen werden. • Wenn möglich, sollte die Verantwortlichkeit für jede operative Entscheidung vor ihrer Ausführung klar sein. • Die Art und Weise, wie Autorität ausgeübt wird, sollte Einzelpersonen nicht davon abhalten, eine offene Kommunikation aufrechtzuerhalten oder Bedenken oder ungewöhnliche Beobachtungen zu melden.
		II(f)(2)	Führungskräfte erklären nach Möglichkeit den Kontext für Fragen und Entscheidungen.		
			Behörde) Aktualisierungen bezüglich der Sicherungskultur auf der Grundlage der Ergebnisse der Selbstbewertung zur Verfügung.		

Literaturverzeichnis

/BER 15/ Beris, O; Beautement, A; Sasse, MA; (2015) Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. Somayaji, A and Van Oorschot, P and Böhme, R and Mannan, M, (eds.) NSPW '15: Proceedings of the 2015 New Security Paradigms Workshop. (pp. pp. 73-84). ISBN: 9781450337540, Association for Computing Machinery (ACM): New York, NY, USA., 2015

/BMU 15/ Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMU): Änderung und Neufassung der Bekanntmachung zu den „Sicherheitsanforderungen an Kernkraftwerke“ (BAnz AT 30.03.2015 B2), Bonn, 3. März 2015

/BMU 12/ Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (jetzt BMU): Sicherheitsanforderungen an Kernkraftwerke, vom 22. November 2012 (BAnz AT 24.01.2013 B3).

/BSI 17/ Bundesamt für Sicherheit in der Informationstechnik: Leitfaden zur Basis-Absicherung nach IT-Grundschutz, 20.10.2017, abgerufen unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.html

/BSI 22/ Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, 23.12.2022, abgerufen unter https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

/BUE 10/ Bühner, M.: Einführung in die Test- und Fragebogenkonstruktion, ISBN: 978-3-86894-326-9, 2010

/DHA 18/ Dhakal, R.: Measuring the Effectiveness of an Information Security Training and Awareness Program, Doktorarbeit, Charles Sturt University, März 2018

/DIN 21/ Deutsches Institut für Normung: Kernkraftwerke – Leittechnische und Elektrische Systeme – Anforderungen an die Cybersicherheit. DIN EN IEC 62645:2021-03. März 2021

/GRS 16/ Faßmann, W., Beck, J., Preischl, W.: Erhaltung und Weiterentwicklung der Sicherheitskultur in Kernkraftwerken unter Berücksichtigung der aktuellen Randbedingungen der Kernenergienutzung in Deutschland, GRS-A-3862, September 2016

/GRS 15a/ Faßmann, W., Beck, J.: Stand von Wissenschaft und Technik zur Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur, GRS-A-3795, April 2015

/GRS 15b/ Faßmann, W., Beck, J.: Leitfaden für die Erfassung und Beurteilung wesentlicher Merkmale der Sicherheitskultur deutscher Kernkraftwerke durch die Genehmigungs- und Aufsichtsbehörde, GRS-A-3792, Oktober 2015

/IAE 21/ International Atomic Energy Agency (IAEA): Enhancing Nuclear Security Culture in Organizations Associated with Nuclear and Other Radioactive Material, Technical Guidance, IAEA Nuclear Security Series No 38-T, Wien, März 2021

/IAE 22/ International Atomic Energy Agency (IAEA): IAEA Nuclear Safety and Security Glossary, Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, Wien, 2022

/IAE 20/ International Atomic Energy Agency (IAEA): A Harmonized Safety Culture Model, Wien, 05.05.2020

/IAE 18/ International Atomic Energy Agency (IAEA): Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Technical Guidance, IAEA Nuclear Security Series No 33-T, Mai 2018

/IAE 17/ International Atomic Energy Agency (IAEA): Self-assessment of Nuclear Security Culture in Facilities and Activities, IAEA Nuclear Security Series No. 28-T, Wien, 2017

/IAE 15/ International Atomic Energy Agency (IAEA): Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, Wien, Februar 2015

/IAE 13/ International Atomic Energy Agency (IAEA): Regulatory Oversight of Safety Culture in Nuclear Installations, IAEA TECDOC No. 1707, Wien, 2013

/IAE 11/ International Atomic Energy Agency (IAEA): Computer Security at Nuclear Facilities, Reference Manual, IAEA Nuclear Security Series No. 17, Wien, Dezember 2011

/IAE 10/ International Atomic Energy Agency (IAEA): The Interface Between Safety and Security at Nuclear Power Plants, INSAG-24, Wien, 2010

/IAE 09/ International Atomic Energy Agency (IAEA): The Management System for Nuclear Installations, Safety Guide No. GS-G-3.5, Wien, 2009

/IAE 08/ International Atomic Energy Agency (IAEA): Nuclear Security Culture, Implementing Guide, IAEA Nuclear Security Series No. 7, Wien, 2008

/IAE 07/ International Atomic Energy Agency (IAEA): Safety Glossary, Wien, 2007

/IAE 06/ International Atomic Energy Agency (IAEA): Amendment to the Convention on the Physical Protection of Nuclear Material, IAEA International Law Series No. 2, Wien, 2006

/IAE 06b/ International Atomic Energy Agency (IAEA): Fundamental Safety Principles, Safety Fundamentals No. SF-1, Wien, 2006

/IAE 04/ International Atomic Energy Agency (IAEA): Code of Conduct on the Safety and Security of Radioactive Resources. Wien, 2004

/IAE 91/ International Atomic Energy Agency (IAEA): Safety Culture, IAEA Safety Series No. 75 INSAG-4, Wien, 1991

/KHR 14/ Khripunov, I. et al: The Human Dimension of Security for Radioactive Sources: From Awareness to Culture, 2014

/KIR 14/ Kirlappos, I; Parkin, S; Sasse, MA: Learning from “Shadow Security”: Why understanding non-compliance provides the basis for effective security. In: (Proceedings) Workshop on Usable Security, ISBN: 189156237 1, San Diego, California, 2014

/KIR 15/ Kirlappos, I; Sasse, MA: Fixing Security Together: Leveraging trust relationships to improve security in organizations. In: Proceedings of the NDSS Symposium 2015. Internet Society: San Diego, CA, USA, 2015

/KTA 17/ Kerntechnische Ausschuss (KTA): Sicherheitstechnische Regel des KTA, Integriertes Managementsystem zum sicheren Betrieb von Kernkraftwerken (KTA 1402), Fassung 2017-11, 2017

/KHR 18/ Khripunov, I., Kuykendall, T., Lowe, J.: Harmonizing Safety Culture and Security Culture at Nuclear Facilities, Final report on the Proceedings of the International Workshop in Serpong, Indonesia, 29-31. Januar 2018

/MAR 02/ Martins, A., Elofe, J.: Information Security Culture, Ghonaimy M.A., El-Hadidi M.T., Aslan H.K. (eds) Security in the Information Society. IFIP Advances in Information and Communication Technology, vol 86. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-35586-3_16

/NIS 12/ National Institute of Standards and Technology (NIST): Information Security – Guide for Conducting Risk Assessments, NIST 800-30, U.S. Department of Commerce, September 2012

/NIS 13/ Nuclear Industry Safety Directors’ Forum: Key Attributes of an Excellent Nuclear Security Culture, Juni 2013

/SCH 02/ Schlienger, T., Teufel, S.: Information Security Culture: The Socio-Cultural Dimension in Information Security Management. SEC, 2002

/SCH 03/ Schlienger, T., S. Teufel: Information Security Culture - From Analysis to Change. J. Elofe, H. Venter, L. Labuschagne and M. Eloff, Eds. Information Security South Africa - Proceedings of ISSA 2003, 3rd Annual Information Security South Africa Conference, 9-11 July 2003, Sandton Convention Center, Johannesburg, South Africa, ISSA: 183-195.

/SPE 15/ Speicher, C. Vortrag: The Importance of Security Culture for Computer Security Effectiveness, International Conference on Computer Security in a Nuclear World, IAEA International Conference on Computer Security in a Nuclear World, Österreich, Juni 2015

/SPE 16/ Speicher, C. Vortrag: Effective Regulatory Oversight/Cooperation between Regulatory Authority and Licensees for Promoting Strong Nuclear Security Culture, IAEA International Workshop on Nuclear Security Culture, Spanien, März 2016

/WIN 16a/ World Institute for Nuclear Security: An Integrated Approach to Nuclear Safety and Nuclear Security, ISBN: 978-3-903191-50-1, April 2016

/WIN 16b/ World Institute for Nuclear Security: Nuclear Security Culture, ISBN 978-3-903191-34-1, Januar 2016

Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) gGmbH

Schwertnergasse 1
50667 Köln
Telefon +49 221 2068-0
Telefax +49 221 2068-888

Boltzmannstraße 14
85748 Garching b. München
Telefon +49 89 32004-0
Telefax +49 89 32004-300

Kurfürstendamm 200
10719 Berlin
Telefon +49 30 88589-0
Telefax +49 30 88589-111

Theodor-Heuss-Straße 4
38122 Braunschweig
Telefon +49 531 8012-0
Telefax +49 531 8012-200

www.grs.de

ISBN 978-3-910548-04-6