Leistungsschein QSEC Version 8.0

Dieses Dokument beschreibt die Software QSEC und gibt eine Übersicht über verfügbare Software-Editionen und deren Beschränkungen. Basisfunktionen werden vorgestellt und von den Funktionalitäten der kostenpflichtigen optionalen Zusatzmodule abgegrenzt. Außerdem wird eine Übersicht über diejenigen Standards gegeben, deren Umsetzung mit QSEC unterstützt wird. Aus dieser Liste können Kunden je nach lizenzierter QSEC-Edition Standards auswählen, nach denen in Ihrer konkreten Implementierung gearbeitet werden soll.

Definitionen und Vorwort

- Die Software QSEC wird in Form von **verschiedenen Editionen (siehe Kapitel 1)** und **optionalen Zusatzmodulen (siehe Kapitel 3)** angeboten. Die maßgebliche Berechnungsgrundlage jeder Lizenzierung von QSEC ergibt sich aus den Allgemeinen Geschäftsbedingungen für QSEC - Software as a Service Solution.
- Die einzelnen QSEC-Editionen enthalten **unterschiedliche Funktionalitäten** und unterliegen **vorgegebenen Nutzungsbeschränkungen** (z.B. die Anzahl der erlaubten Nutzer nach Nutzertyp und die Anzahl der Standards, nach denen gearbeitet werden kann).
- QSEC unterscheidet zwei Arten von Nutzertypen: **Experten-User** (alle Funktionalitäten können ausgeübt werden, inklusive Administratorenrechte) und **Action-User** (nur zugewiesene Interviews, Maßnahmen und Dokumente können bearbeitet werden). Jede QSEC-Edition definiert eine maximale Anzahl der beiden Nutzertypen.
- QSEC arbeitet auf Basis von **Geltungsbereichen**. Ein Geltungsbereich („Scope“) ist jeder definierte organisatorische Bereich von Unternehmen und Behörden, für welchen ein Standard angewandt und separat untersucht bzw. auditiert wird. Im Geltungsbereich wird festgelegt, wonach die Bearbeitung (Bewertung, Standards, etc.) für die zugeordneten Geschäftseinheiten erfolgen soll. Innerhalb eines Geltungsbereichs kann grundsätzlich auch nach unterschiedlichen Standards gearbeitet werden, in diesem Fall erfolgt jedoch keine Trennung der einzelnen Standards. Sollen Standards getrennt betrachtet werden, müssen unterschiedliche Geltungsbereiche angelegt werden. Es ist grundsätzlich empfohlen, vor der Inbetriebnahme von QSEC ein Geltungsbereich-Konzept zu erstellen. Je nach lizenzierter Edition ist eine maximale Anzahl von Geltungsbereichen verfügbar.
- Die ISO/IEC- und DIN/ISO-Normen, nach welchen in QSEC methodisch gearbeitet werden kann, müssen von Kunden selbst lizenziert bzw. bereitgestellt werden.

Stand: Q2 2025 Status: Freigegeben

1. Editionen der Software QSEC

Für die Nutzung der Software QSEC werden drei verschiedene Editionen angeboten. Die folgende Tabelle gibt einen Überblick über die Lizenzbegrenzungen der einzelnen QSEC-Editionen. Jede Edition enthält verschiedene Grundfunktionen, die in Kapitel 2 dieses Dokuments vorgestellt werden.

Software-Edition	Experten-User	Action-User	Geltungsbereiche	Zusatz-module	Connectivity
QSEC Core	2	unbegrenzt	3	nach Bedarf	-
QSEC Professional	5	unbegrenzt	6	nach Bedarf	+
QSEC Enterprise	unbegrenzt	unbegrenzt	unbegrenzt	nach Bedarf	+

Die ab QSEC Professional integrierten Connectivity-Pakete enthalten Funktionen zur Einbindung von QSEC in die Unternehmenslandschaft. Das Connectivity-Paket beinhaltet Funktionen zum Microsoft (Azure) Active Directory / Entra ID Import, die Nutzung der QSEC-API und die erweiterte Administration in QSEC (Anpassung von Funktionalitäten und User Interface). Außerdem ist standardmäßig die Erfassung/Verwaltung von Projekten möglich. Des Weiteren bietet das Connectivity Paket Funktionen zur Ereignis- und Vorfallserfassung (EVA: Sicherheitsvorfälle können ohne Anmeldung in QSEC gemeldet und in die Datenbank von QSEC weitergeleitet werden).

QSEC Core

QSEC Core ist die Einstiegsedition mit dem kompaktesten Funktionsumfang und beinhaltet alle Grundfunktionalitäten der Software. Die Nutzung erfolgt durch Experten-User (z.B. ein administrativer Nutzer, der Pflegearbeiten in QSEC durchführt ohne Fachbereiche einzubeziehen) und Action Usern. Das Arbeiten nach den Vorgaben der DSGVO und der ISO 27001/27002/27005, sowie weiteren Standards ist enthalten. Der Kunde kann darüber hinaus weitere Standards aus der Liste am Ende dieses Dokuments auswählen. Eine Erweiterung um das Connectivity-Paket ist nicht möglich.

QSEC Professional

QSEC Professional beinhaltet den gesamten Umfang der Core-Edition und erweitert diese um das Connectivity-Paket. Die Lizenzierung von optional kostenpflichtigen Zusatzmodulen ist analog zur Core-Edition möglich. Außerdem ist eine erhöhte Anzahl an Experten-Usern und Geltungsbereichen verfügbar.

QSEC Enterprise

QSEC Enterprise beinhaltet den gesamten Umfang der QSEC Professional-Edition und hebt bestehende Limitationen der Anzahl der Geltungsbereiche, der Experten-User und Action-User auf. Sie wird typischerweise in Unternehmen mit einer hohen Anzahl an verschiedenen Benutzern (Action-User und Experten-User) und Geltungsbereichen eingesetzt. Die optionale Buchung von Zusatzfunktionen ist wie bei der QSEC Core und der QSEC Professional-Edition möglich.

2. Grundfunktionen aller QSEC-Editionen

QSEC bietet folgende, inhaltlich gruppiert dargestellten Grundfunktionalitäten in allen Editionen. Funktionalitäten, die nur in bestimmten Editionen verfügbar sind, sind entsprechend gekennzeichnet.

Bezeichnung	Beschreibung
Suchfunktion und Datenfilterung	Zentralisierte Suche nach verwalteten Elementen (z.B. Maßnahmen, Verantwortlichkeiten, ...) und konfigurierbare Datenfilterung.
Wiedervorlagen und Mailing	Automatische Erinnerungen für anstehende Aufgaben, Assessments, Freigaben etc.; Mailversand über QSEC (angepasst auf die gewünschte CI) über einen durch den Kunden bereitgestellten SMTP-Server
Workflowfunktionen	Wizard-basierte Technologien; individuelle Workflows ab QSEC Core.
Vertretungen	Verantwortlichkeiten können während der Abwesenheit der Verantwortlichen über eine Vertretungsfunktion an Kollegen weitergegeben werden.
Kopieren, Sperren, Freeze	Duplizieren von Elementen, Sperren von gleichzeitiger Bearbeitung und Einfrieren (Freeze, verhindert nachträgliches Manipulieren) von Elementen.
Historisierung	QSEC historisiert die Daten, sodass nachträglich Änderungen und Neuerungen nachvollzogen werden können.
Import	Excellisten mit Informationen zu den Stammdaten (Geschäftsprozesse, Mitarbeiter, Assets etc.) können in QSEC eingelesen werden.
Geschäfts- und Organisationseinheiten	Abbildung von Unternehmensstrukturen und Mitarbeiterzuordnung zur Begrenzung der Sichten auf die Daten (z.B. eigene Abteilung).
KPI-Abbildung	Abbildung von Key Performance Indikatoren (ISO FTE je Geschäfts/Organisationseinheit, Anzahl Mitarbeiter je ISO).
Benutzeradministration	Erstellung und Verwaltung von Benutzeraccounts. Definition und Vergabe (optional über eine AD-Anbindung automatisiert) von Rollenberechtigungen.
Berechtigungssteuerung	Rollenberechtigungen können definiert und vergeben werden. Die Zuweisung der Mitarbeiter kann z.B. über eine AD-Anbindung automatisiert werden.
Allgemeine Administration	Zurücksetzen von persistierten Daten, Cache-Löschung, Überblick über Logs. Einstellbare Corporate Identity und Sprache (Deutsch, Englisch).
Berichtserstellung	Erstellen von Berichten und Berichtsvorlagen. Export in unterschiedlichen Formaten, z.B. .docx, .xlsx, .pdf.
Standardberichte	Arbeits- und Managementberichte mit administrierbarer Zugriffskontrolle, z.B. Status des Compliance Managements, Risikomatrix-Bericht, ...

Maßnahmenverwaltung

Die QSEC-Maßnahmenverwaltung ermöglicht eine zentrale Pflege, Auswertung und Ausleitung von Maßnahmen.

Bezeichnung	Beschreibung
Verbesserung von Reifegraden/Risiken	Angabe von Reifegradverbesserungen für verbundene Controls.
Maßnahmenkatalog/individuelle Anzeigen	Zusammenfassender Überblick über alle gepflegten Maßnahmen inklusive Einsicht in relevante Attribute (z.B. Status, Verantwortlichkeiten, Typ, ...).
Maßnahmenbewertung	Maßnahmen können auf ihre Wirtschaftlichkeit und rechtliche Relevanz überprüft werden und ggf. zusammenhängende Risiken akzeptiert werden.
Maßnahmenvorschläge	Best Practice-Ansätze für die Behandlung von Risiken/Umsetzung von Controls in Form von Maßnahmenvorschlägen.
Maßnahmen-Dashboard	Abbildung von Performance Indikatoren (Anzahl Maßnahmen je Mitarbeiter, nach Status, nach Kosten, nach Wiedervorlage) in Form eines Dashboards.

Compliance-Verwaltung

In der QSEC-Compliance-Verwaltung können eine Vielzahl von verschiedenen Compliance-Anforderungen wie Gesetze, Richtlinien, Normen etc. hinterlegt und nach verschiedenen Reifegradmodellen bewertet werden.

Bezeichnung	Beschreibung
Compliance-Bewertung	Bewertung von Compliance-Anforderungen nach dem PDCA-Zyklus sowie einer individuell gewählten Reifegradmethodik.
Self-Assessment	Planung von Self-Assessments für Scopes, Geltungsbereiche, Untersuchungsbereiche und Compliance-Anforderungen.
Zusatzfragen	Zusatzfragenkataloge, die die Inhalte von ausgewählten Normen auf einzelne Fragen herunterbrechen und so die Reifegradbewertung unterstützen.
Compliance Wizard	Gesonderter Anwenderbereich, in welchem die Bewertung von Normen und Standards in vereinfachter Weise stattfinden kann.
Erweiterte Normen, Richtlinien, Gesetze	Zu bewertende Inhalte können ab QSEC Professional frei erweitert und bearbeitet werden.

Information Asset-Verwaltung

Die Information Asset-Verwaltung ermöglicht das Hinterlegen von Geschäftsprozessen, IT-Assets und Informationswerten. Es wird der Grundstein für die relevanten Bewertungen für das ISMS (Schutzbedarfe, IT-Risiko, BIA/BCM etc.) und den Datenschutz (Identifizierung von Datenarten, Empfängern etc.) gelegt.

Bezeichnung	Beschreibung
Strukturanalyse	Übersichtliche Verwaltung von Geschäftsprozessen, Informationen und Assetgruppen (= IT-Assets)
Kritikalitätsbewertung und Schutzbedarfsfeststellung	Kritikalitätsbewertung von Geschäftsprozessen auf Basis der verknüpften Informationen und deren Einstufung nach Vertraulichkeit, Verfügbarkeit, Integrität, Datenschutzrelevanz etc.

Aufbau eines Asset-Registers	Einzelassets können den jeweiligen Assetgruppen zugewiesen und mit individuellen Feldern (Seriennummer, Lizenz etc.) angepasst werden.

Datenschutzmanagement

Die QSEC-Datenschutzfunktionalitäten bieten eine Ansicht auf Verarbeitungen und die dort verarbeiteten Daten. Außerdem können weitere Themen wie bspw. Dienstleister und Verträge bearbeitet werden. QSEC enthält eine elektronische Berichtserstellung zur Auswertung, z.B. zur Erstellung des „Verzeichnis von Verarbeitungstätigkeiten".

Bezeichnung	Beschreibung
Verzeichnis von Verarbeitungstätigkeiten	QSEC verfügt über die Möglichkeit, das VVT I sowie VVT II elektronisch auszuleiten.
Bewertungsformularseite	Formular, in welchem die datenschutzrechtlichen Anforderungen gesichtet, bearbeitet und verifiziert werden können.
Datenschutzfolgeabschätzung	Durchführung der Datenschutzfolgeabschätzungen direkt an den Prozessen.
Dienstleister & AV-Verträge	Dienstleister, die personenbezogene Daten verarbeiten, können an den Verarbeitungen referenziert und verknüpfte Verträge geprüft werden.

Incidentmanagement

Die Incident-Verwaltung ermöglicht die Dokumentation und Bearbeitung von Sicherheitsvorfällen. Sicherheitsvorfälle können mit anderen Funktionen in Verbindung gebracht werden (IT-Risiko, Datenschutz, IT-Assets, Prozessen etc.).

Bezeichnung	Beschreibung
Incident-Erfassung	Erfassung von Security Incidents, Definition der Sicherheitsziele, Umsetzung gezielter Maßnahmen, sowie die Bestimmung betroffener Systeme.
Dokumentation meldepflichtiger Vorfälle	Formular zur Erfassung und Weiterleitung meldepflichtiger Datenschutz- und Informationssicherheitsvorfälle an zuständige Behörden bei KRITISOrganisationen.
Incident-Auswertung	Überblick über Spitzen-Incidents, ihre Häufigkeit und die betroffenen Systeme.
Incidentzeitraum	Erfassung und Nachverfolgung von Incident-Behandlungszeiträumen.

IT-Risiko-Management

Das QSEC IT-Risiko-Management deckt den Risikomanagementprozess für die IT-Assets nach den Methodiken der ISO 27005 ab. I.d.R. kann die Methodik auch auf bereits feststehende unternehmenseigene Richtlinien angepasst werden.

Bezeichnung	Beschreibung
Schutzbedarfsermittlung	Definition der Schutzbedarfskriterien (standardmäßig mit Vertraulichkeit, Verfügbarkeit, Integrität und Datenschutzrelevanz hinterlegt).
Individuelle Risikokataloge	QSEC verfügt über eine Bandbreite an Risikokatalogen, die individuell und je nach Risikomethodik angewendet werden können.
Risikobewertung	Einzelne oder massenhafte Risikobewertung (Massenbearbeitungen).

Risikobehandlungsplan	Auflistung von Risiken nach Stufen. Konfiguration des Informationsgehalts des Risikobehandlungsplans.
Iterative Bewertungszyklen	Nach der Bewertung und Behandlung können die Rezertifizierungsprozesse in QSEC automatisiert werden.

Dokumenten- und Vertragsmanagement

Mit dem Dokumentenmanagement kann die Verwaltung der Dokumente für IT- und Informationssicherheit durchgeführt und die Dokumentenpflege durch Workflows unterstützt werden (z.B. Dokumentenfreigaben & -Rezertifizierungen, ...).

Bezeichnung	Beschreibung
Dokumentenerfassung	Hinterlegen von Metadaten zu jedem Dokument (z.B. Einstellung eines Wiedervorlagedatums, Dokumentenverantwortlicher, Versionierung etc.)
Vertragsattribute	Vertragskriterien/-bewertungen (Datenschutzanforderung) bei Dokumententyp „Vertrag“ vorhanden und individuell anpassbar.
Vertragsübersicht	Übersicht aller Verträge, deren verantwortlichen Personen und wichtige weitere Informationen (z.B. Vertragslaufzeit etc.).
Zugriffsrechte	Zuweisen von Zugriffsrechten pro Dokument, Mehrfachzuweisung von Zugriffsrechten für mehrere Dokumente.

3. Optionale QSEC-Zusatzmodule

Neben den Basisfunktionalitäten (Kapitel 2) können Kunden folgende weitere kostenpflichtige Zusatzmodule für QSEC lizenzieren.

Modul 1: Business Continuity Management

Das Zusatzmodul BCM (Business Continuity Management) setzt die Anforderungen der ISO 22301 bzw. des BSI ITGrundschutz 200-4 um. Das schließt die Möglichkeiten zur Analyse der Geschäftsprozesse durch eine BIA (Business Impact Analyse), die Fortführung der GAP-Analyse der verbundenen Ressourcen sowie dessen Risikoanalyse, und die Verwaltung der Dokumente zur Notfallplanung mit ein. Die Analysen in QSEC können im Reporting-Bereich ausgewertet und kommuniziert (z.B. an die Geschäftsleitung) werden. Folgende Kernfunktionen sind in dem Zusatzmodul enthalten:

- Anzeige der BIA-relevanten Prozesse
- Durchführung der Business Impact Analyse
- Bewertung von potenziellen Schäden nach Zeithorizonten (Reputationsschäden, finanzielle Schäden, rechtliche Schäden, weitere konfigurierbare Schadensarten)
- Ermittlung des RTO-Soll (Vorgabe der Wiederherstellungszeit)
- Ermittlung des RPO-Soll (Vorgabe des Wiederherstellungs-Zeitpunktes)
- Planung & Bewertung von Ressourcen (Mitarbeiter, Dienstleister, Systeme, Informationen, ...)
- Gap-Analyse
- Ermittlung und Behandlung von Verfügbarkeitsrisiken
- Festlegung der Notfallplanung und Notfalltests für kritische Geschäftsprozesse
- Überprüfung und Bewertung der Dokumentation für kritische Asset-Gruppen (IT-Notfallplan, Betriebshandbuch, Wiederanlaufplan) mit den ggf. durchgeführten Testergebnissen (individuell einstellbar)
- Umfangreiche Berichte, Grafiken und KPIs zu kritischen Systemen und Prozessen (konfigurierbar)
- Arbeiten nach dem Standard ISO/IEC 22301 und dem BSI IT-Grundschutz 200-4

Modul 2: BSI IT-Grundschutz

Mit dem Modul **BSI IT-Grundschutz** bietet QSEC ein Werkzeug, dass die Methodiken der Standards 200-1 und 200-2 unterstützt. In QSEC werden dafür die IT-Grundschutz-Kompendien bereitgestellt und regelmäßig auf die neuste Version aktualisiert. Die in den Kompendien geforderten Anforderungen/Gefährdungen können an den dafür vorgesehenen Assets herangezogen und bewertet werden. QSEC bietet neben der Aktualisierung der Kompendien eine automatisierte Bewertungsübertragung an. Anforderungs- bzw. Gefährdungsbewertungen aus alten Kompendien, die in neuen Kompendien weiterhin enthalten sind, können Asset-bezogen auf die aktuellen Versionen übertragen werden. Folgende Kernfunktionen sind in dem Zusatzmodul enthalten:

- Erweiterung des IT-Risikomoduls um die Methodik des IT-Grundschutzes
- Arbeiten nach BSI 200-1; 200-2; 200-3
- Inhalte des Standards 200-2 können nach Reifegrad bewertet werden
- IT-Grundschutz-Kompendien
  - Toolgestützte Modellierung der Kompendien am Asset
  - Bewertung der Gefährdungen und Anforderungen
  - Ableitung von Risiken und Risikobehandlungsmöglichkeiten
  - Automatische Bewertungsübertragung von alten Kompendien auf den aktuellen Stand
- Die Berichtsanforderungen des BSI (A1. bis A6.) werden abgedeckt

Modul 3: Erweitertes Dienstleistermanagement

QSEC bietet mit dem erweiterten Dienstleistermanagement ein Zusatzmodul zur Implementierung eines durchgängigen Dienstleister-Managementprozesses an. Beginnend bei der Ermittlung von Dienstleistern über die Fortführung der geforderten Prüfungen und Bewertungen, einem komplexen Vertragsmanagement und endend mit der Erfüllung erweiterter Gesetzesanforderungen wie z.B. dem Lieferkettengesetz.

Die Analysen können im Reporting und auf der Oberfläche jederzeit nachvollzogen und ausgeleitet werden. Der Informationsgehalt der Berichte kann frei eingestellt werden und die Berichtsausgabe erfolgt elektronisch. Folgende Kernfunktionen sind in dem Zusatzmodul enthalten:

- Darstellung von Dienstleistern und Sub-Dienstleistern
- Einbindung der Dienstleister in die Schutzbedarfsanalyse
- Bewertung von Dienstleisterrisiken (Datenschutzrisiken, Informationssicherheitsrisiken, Individuelle Risiken)
- Darstellung der Verbindung von Dienstleistern zu IT-Assets, Geschäftsprozessen, Informationswerten, Vorfällen
- Ausgeprägtes Vertragsmanagement
- DEA (Dienstleister-Erfassungs-Applikation: Zusätzliche Web-Anwendung zur Bewertung von Dienstleistern über konfigurierbare Abfrageformulare)

Modul 4: Unternehmensrisiko-Management

Neben der Verwaltung des IT-Risikomanagements kann in QSEC durch Lizenzierung des Zusatzmoduls **Unternehmensrisiko-Management** ein ganzheitlicher Risikoprozess etabliert werden. Mit der Verwaltung von Einzelrisiken an IT-Assets, der Betrachtung von Geschäftsprozess-, Organisations- und Marktrisiken und der Zusammenführung der gesamten Risiken in einer einheitlichen Sicht kann QSEC einen ganzheitlichen Risikoprozess unterstützen. Folgende Kernfunktionen sind in dem Zusatzmodul enthalten:

- Identifizierung verschiedener Risikoarten
  - Betrachtung von typischen Risiken in Katalogen
  - Aufnahme von neuen Risiken (ad hoc-Risiken)
  - Unterscheidung zwischen internen und externen Risiken
  - Unterscheidung zwischen verschiedenen Risikoarten
  - Bewertung von Eintrittswahrscheinlichkeit und Schadenshöhe

  - Festlegung von Risikoeigentümern (Risk-Owner)
  - Definierung von betroffenen Bereichen
  - Benachrichtigung an relevante Personen bei neuen Risikoidentifikationen
- Risikobehandlung (Risikovermeidung, Risikoreduzierung, Risikoverlagerung, Risikoakzeptanz)
- Kontrolle und Tracking (Maßnahmentracking, Automatische Erinnerungen, Rezertifizierung von Risiken)
- Dokumentation
  - Erstellen von notwendigen Managementreports
  - Zusammenführung von verschiedenen Risikotypen in eine Gesamtübersicht
  - Betrachtung der Veränderungen durch Berichte auf Basis der Historie

4. Standards, nach denen in QSEC gearbeitet werden kann

Die Standards **ISO 27001, 27002, 27005** und **DSGVO** werden von Nexis für das Arbeiten in QSEC bereitgestellt (sofern die notwendigen ISO-Werke durch den Kunden lizenziert wurden, siehe Kapitel 1). Wird eine neue Version eines der Standards veröffentlicht, wird Nexis innerhalb von 12 Monaten nach Veröffentlichung den Fragenkatalog des betroffenen Standards aktualisieren.

Nach den folgenden weiteren Standards kann mit QSEC gearbeitet werden, jedoch erfolgt eine kostenpflichtige Aktualisierung nur auf Anfrage.

Erweiterter Standard	Thema
B3S- Gesundheit	Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus
BAIT	IT-Anforderungen an Banken
BDSG	Bundesdatenschutzgesetz
BNetzA IT-Sicherheitskatalog 1a	IT-Sicherheit für Energiewirtschaft (gem. §11 Abs 1a EnWG)
BNetzA IT-Sicherheitskatalog 1b	IT-Sicherheit für Energiewirtschaft (gem. §11 Abs 1b EnWG)
BSI C5	Kriterienkatalog Cloud Computing
BSI TR-03109-6	TR Smart Meter Gateway - SMGW
DORA	Digital Operational Resilience Act
IATF 16949	Qualitätsmanagement in der Automobilindustrie
ISO/IEC 13485	Qualitätsmanagement für Medizinprodukte
ISO/IEC 14001	Umweltmanagement
ISO/IEC 19600	Compliance
ISO/IEC 20000-1	IT-Servicemanagement
ISO/IEC 27001 (i.v.m. 27019)	ISMS nach 27001, erweitert um Anforderungen an Steuerungssysteme
ISO/IEC 27018	Personenbezogene Daten in der Public Cloud
ISO/IEC 27019	Informationssicherheit für Steuerungssysteme
ISO/IEC 27701	Datenschutzerweiterung der ISO 27001

ISO/IEC 28000	Schutz der Sicherheit in den Lieferketten
ISO/IEC 37001	Anti-Korruptions-Managementsysteme
ISO/IEC 45001	Sicherheit und Gesundheit bei der Arbeit
ISO/IEC 50001	Energiemanagement
ISO/IEC 55001	Assetmanagement
ISO/IEC 9001	Qualitätsmanagement
IT-Grundschutz für Kommunalverwaltungen	Basisabsicherung für Kommunalverwaltungen
KAIT	IT-Anforderungen an Kapitalgesellschaften
MaRisk	Mindestanforderungen das Risikomanagement
OH SzA	Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung
PCI DSS	Payment Card Industry Data Security Standard
TISAX	Informationssicherheit Automotive
TKG	Telekommunikationsgesetz mit Anlage 1 & 2
VAIT	IT-Anforderungen an Versicherungen
VDV 4400	IT-Sicherheit für Verkehrsunternehmen
ZAIT	IT-Anforderungen an Zahlungs- und E-Geld-Institute