# Service Certificate Nexis QSEC

## Service certificate (Leistungsschein) – Version 8.0

**As of:** October 22, 2026 | **Status:** Approved · Convenience translation

# Table of Contents


Definitions and preface 2
1. Editions of the QSEC software 2
1.1. QSEC Core 3
1.2. QSEC Professional 3
1.3. QSEC Enterprise 3
2. Basic functions of all QSEC editions 3
2.1. Measure management 4
2.2. Compliance management 5
2.3. Information asset management 5
2.4. Data protection management 5
2.5. Incident management 6
2.6. IT risk management 6
2.7. Document and contract management 7
3. Optional QSEC add-on modules 7
3.1. Module 1: Business Continuity Management 7
3.2. Module 2: BSI IT-Grundschutz 8
3.3. Module 3: Extended service provider management 8
3.4. Module 4: Enterprise risk management 9
4. Standards that can be worked with in QSEC 9


*Please note: This English version of the service certificate (Leistungsschein) is a convenience translation only. In case of conflicts between the German and the English version, the German version shall prevail.*

This document describes the QSEC software and provides an overview of the available software editions and their limitations. Basic functions are presented and distinguished from the functionalities of the optional add-on modules subject to a charge. In addition, an overview is given of the standards whose implementation is supported by QSEC. Depending on the licensed QSEC edition, customers can select from this list the standards according to which work is to be carried out in their specific implementation.

# Definitions and preface

- The QSEC software is offered in the form of different editions (see Chapter 1) and optional add-on modules (see Chapter 3). The relevant basis of calculation for any licensing of QSEC results from the General Terms and Conditions for QSEC - Software as a Service Solution.
- The individual QSEC editions contain different functionalities and are subject to predefined usage limitations (e.g. the number of permitted users per user type and the number of standards that can be worked with).
- QSEC distinguishes between two user types: Expert users (all functionalities can be used, including administrator rights) and Action users (only assigned interviews, measures and documents can be edited). Each QSEC edition defines a maximum number of both user types.
- QSEC works on the basis of scopes. A scope ("Geltungsbereich") is any defined organisational area of companies and public authorities for which a standard is applied and separately examined or audited. The scope determines the basis on which the processing (assessment, standards, etc.) is to be carried out for the assigned business units. Within one scope, it is in principle also possible to work according to different standards; in this case, however, the individual standards are not separated. If standards are to be considered separately, different scopes must be created. It is generally recommended to create a scope concept before QSEC is put into operation. Depending on the licensed edition, a maximum number of scopes is available.
- The ISO/IEC and DIN/ISO standards according to which methodical work can be carried out in QSEC must be licensed or provided by the customers themselves.

# 1. Editions of the QSEC software

Three different editions are offered for the use of the QSEC software. The following table provides an overview of the license limits of the individual QSEC editions. Each edition contains various basic functions, which are presented in Chapter 2 of this document.

| Software edition | Expert users | Action users | Scopes | Add-on modules | Connectivity |
|---|---|---|---|---|---|
| QSEC Core | 2 | unlimited | 3 | as required | - |
| QSEC Professional | 5 | unlimited | 6 | as required | + |
| QSEC Enterprise | unlimited | unlimited | unlimited | as required | + |

The connectivity packages integrated from QSEC Professional onwards contain functions for integrating QSEC into the corporate landscape. The connectivity package includes functions for Microsoft (Azure) Active Directory / Entra ID import, use of the QSEC API and extended administration in QSEC (customisation of functionalities and user interface). In addition, the recording/management of projects is possible as standard. Furthermore, the connectivity package offers functions for recording events and incidents (EVA: security incidents can be reported without logging in to QSEC and forwarded to the QSEC database).

## 1.1. QSEC Core

QSEC Core is the entry-level edition with the most compact range of functions and includes all basic functionalities of the software. It is used by Expert users (e.g. an administrative user who carries out maintenance work in QSEC without involving specialist departments) and Action users. Working according to the requirements of the GDPR and ISO 27001/27002/27005 as well as further standards is included. In addition, the customer can select further standards from the list at the end of this document. An extension by the connectivity package is not possible.

## 1.2. QSEC Professional

QSEC Professional includes the full scope of the Core edition and extends it by the connectivity package. Optional add-on modules subject to a charge can be licensed in the same way as for the Core edition. In addition, an increased number of Expert users and scopes is available.

## 1.3. QSEC Enterprise

QSEC Enterprise includes the full scope of the QSEC Professional edition and removes the existing limitations on the number of scopes, Expert users and Action users. It is typically used in companies with a high number of different users (Action users and Expert users) and scopes. Additional functions can optionally be booked in the same way as for the QSEC Core and QSEC Professional editions.

# 2. Basic functions of all QSEC editions

QSEC offers the following basic functionalities, grouped by content, in all editions. Functionalities that are only available in certain editions are marked accordingly.

| Name | Description |
|---|---|
| Search function and data filtering | Centralised search for managed elements (e.g. measures, responsibilities, ...) and configurable data filtering. |
| Follow-ups and mailing | Automatic reminders for upcoming tasks, assessments, approvals etc.; sending of emails via QSEC (adapted to the desired CI) via an SMTP server provided by the customer |
| Workflow functions | Wizard-based technologies; individual workflows from QSEC Core onwards. |
| Substitutions | During the absence of the responsible persons, responsibilities can be passed on to colleagues via a substitution function. |
| Copy, lock, freeze | Duplication of elements, locking against simultaneous editing and freezing of elements (freeze, prevents subsequent manipulation). |
| History | QSEC keeps a history of the data so that changes and updates can be traced subsequently. |

| Name | Description |
|---|---|
| Import | Excel lists with information on the master data (business processes, employees, assets, etc.) can be imported into QSEC. |
| Business and organisational units | Mapping of company structures and assignment of employees to restrict the views of the data (e.g. own department). |
| KPI mapping | Mapping of key performance indicators (ISO FTE per business/organisational unit, number of employees per ISO). |
| User administration | Creation and management of user accounts. Definition and assignment (optionally automated via an AD connection) of role permissions. |
| Permission control | Role permissions can be defined and assigned. The assignment of employees can be automated, e.g. via an AD connection. |
| General administration | Resetting of persisted data, cache deletion, overview of logs. Configurable corporate identity and language (German, English). |
| Report generation | Creation of reports and report templates. Export in different formats, e.g. .docx, .xlsx, .pdf. |
| Standard reports | Working and management reports with administrable access control, e.g. status of compliance management, risk matrix report, ... |

## 2.1. Measure management

QSEC measure management enables central maintenance, evaluation and export of measures.

| Name | Description |
|---|---|
| Improvement of maturity levels/risks | Specification of maturity level improvements for linked controls. |
| Measure catalogue/individual views | Summarised overview of all maintained measures including insight into relevant attributes (e.g. status, responsibilities, type, ...). |
| Measure assessment | Measures can be checked for their cost-effectiveness and legal relevance and, if necessary, related risks can be accepted. |
| Measure proposals | Best practice approaches for the treatment of risks/implementation of controls in the form of measure proposals. |
| Measure dashboard | Mapping of performance indicators (number of measures per employee, by status, by cost, by follow-up) in the form of a dashboard. |

## 2.2. Compliance management

In QSEC compliance management, a large number of different compliance requirements such as laws, guidelines, standards etc. can be stored and assessed according to various maturity models.

| Name | Description |
|---|---|
| Compliance assessment | Assessment of compliance requirements according to the PDCA cycle and an individually selected maturity methodology. |
| Self-assessment | Planning of self-assessments for scopes, areas of application, areas of investigation and compliance requirements. |
| Additional questions | Catalogues of additional questions that break down the contents of selected standards into individual questions and thus support the maturity assessment. |
| Compliance wizard | Separate user area in which standards and norms can be assessed in a simplified manner. |
| Extended standards, guidelines, laws | Contents to be assessed can be freely extended and edited from QSEC Professional onwards. |

## 2.3. Information asset management

Information asset management enables business processes, IT assets and information assets to be stored. It lays the foundation for the relevant assessments for the ISMS (protection requirements, IT risk, BIA/BCM etc.) and for data protection (identification of data types, recipients etc.).

| Name | Description |
|---|---|
| Structure analysis | Clear management of business processes, information and asset groups (= IT assets) |
| Criticality assessment and determination of protection requirements | Criticality assessment of business processes on the basis of the linked information and its classification according to confidentiality, availability, integrity, data protection relevance etc. |
| Setting up an asset register | Individual assets can be assigned to the respective asset groups and customised with individual fields (serial number, license etc.). |

## 2.4. Data protection management

The QSEC data protection functionalities provide a view of processing activities and the data processed in them. In addition, further topics such as service providers and contracts can be handled. QSEC includes electronic report generation for evaluation, e.g. for creating the "record of processing activities".

| Name | Description |
| --- | --- |
| Record of processing activities | QSEC offers the option of exporting the record of processing activities I and II (VVT I and VVT II) electronically. |
| Assessment form page | Form in which the data protection requirements can be reviewed, processed and verified. |
| Data protection impact assessment | Performance of data protection impact assessments directly on the processes. |
| Service providers & data processing agreements | Service providers that process personal data can be referenced in the processing activities, and linked contracts can be checked. |

## 2.5. Incident management

Incident management enables the documentation and handling of security incidents. Security incidents can be linked to other functions (IT risk, data protection, IT assets, processes etc.).

| Name | Description |
| --- | --- |
| Incident recording | Recording of security incidents, definition of security objectives, implementation of targeted measures and determination of affected systems. |
| Documentation of reportable incidents | Form for recording and forwarding reportable data protection and information security incidents to the competent authorities in the case of KRITIS organisations. |
| Incident evaluation | Overview of top incidents, their frequency and the affected systems. |
| Incident period | Recording and tracking of incident handling periods. |

## 2.6. IT risk management

QSEC IT risk management covers the risk management process for IT assets according to the methodologies of ISO 27005. As a rule, the methodology can also be adapted to existing company guidelines.

| Name | Description |
| --- | --- |
| Determination of protection requirements | Definition of the protection requirement criteria (stored by default with confidentiality, availability, integrity and data protection relevance). |
| Individual risk catalogues | QSEC has a range of risk catalogues that can be applied individually and depending on the risk methodology. |
| Risk assessment | Individual or bulk risk assessment (bulk editing). |
| Risk treatment plan | Listing of risks by level. Configuration of the information content of the risk treatment plan. |

| Name | Description |
|---|---|
| Iterative assessment cycles | After assessment and treatment, the recertification processes can be automated in QSEC. |

## 2.7. Document and contract management

Document management can be used to manage the documents for IT and information security and to support document maintenance through workflows (e.g. document approvals & recertifications, ...).

| Name | Description |
|---|---|
| Document recording | Storage of metadata for each document (e.g. setting a follow-up date, document owner, versioning etc.) |
| Contract attributes | Contract criteria/assessments (data protection requirement) available for the document type "contract" and individually customisable. |
| Contract overview | Overview of all contracts, their responsible persons and other important information (e.g. contract term etc.). |
| Access rights | Assignment of access rights per document, multiple assignment of access rights for several documents. |

# 3. Optional QSEC add-on modules

In addition to the basic functionalities (Chapter 2), customers can license the following further add-on modules for QSEC, which are subject to a charge.

## 3.1. Module 1: Business Continuity Management

The add-on module BCM (Business Continuity Management) implements the requirements of ISO 22301 and BSI IT-Grundschutz 200-4. This includes the options for analysing business processes by means of a BIA (business impact analysis), the continuation of the GAP analysis of the linked resources and their risk analysis, and the management of documents for emergency planning. The analyses in QSEC can be evaluated in the reporting area and communicated (e.g. to the management). The add-on module contains the following core functions:

- Display of the BIA-relevant processes
- Performance of the business impact analysis
- Assessment of potential damage by time horizon (reputational damage, financial damage, legal damage, further configurable types of damage)
- Determination of the target RTO (specification of the recovery time)
- Determination of the target RPO (specification of the recovery point)

- Planning & assessment of resources (employees, service providers, systems, information, ...)
- Gap analysis
- Identification and treatment of availability risks
- Definition of emergency planning and emergency tests for critical business processes
- Review and assessment of the documentation for critical asset groups (IT emergency plan, operating manual, restart plan) with any test results (individually configurable)
- Comprehensive reports, charts and KPIs on critical systems and processes (configurable)
- Working according to the ISO/IEC 22301 standard and BSI IT-Grundschutz 200-4

## 3.2. Module 2: BSI IT-Grundschutz

With the BSI IT-Grundschutz module, QSEC offers a tool that supports the methodologies of standards 200-1 and 200-2. For this purpose, the IT-Grundschutz Compendia are provided in QSEC and regularly updated to the latest version. The requirements/threats demanded in the compendia can be applied to and assessed on the assets intended for this purpose. In addition to updating the compendia, QSEC offers an automated transfer of assessments. Requirement and threat assessments from old compendia that are still contained in new compendia can be transferred to the current versions on an asset-specific basis. The add-on module contains the following core functions:

- Extension of the IT risk module by the IT-Grundschutz methodology
- Working according to BSI 200-1; 200-2; 200-3
- Contents of standard 200-2 can be assessed according to maturity level
- IT-Grundschutz Compendia
  - Tool-supported modelling of the compendia on the asset
  - Assessment of threats and requirements
  - Derivation of risks and risk treatment options
  - Automatic transfer of assessments from old compendia to the current version
- The reporting requirements of the BSI (A1. to A6.) are covered

## 3.3. Module 3: Extended service provider management

With extended service provider management, QSEC offers an add-on module for implementing an end-to-end service provider management process. It starts with the identification of service providers, continues with the required audits and assessments and complex contract management, and ends with the fulfilment of extended legal requirements such as the German Supply Chain Act (Lieferkettengesetz).

The analyses can be traced and exported at any time in reporting and on the user interface. The information content of the reports can be freely configured, and reports are output electronically. The add-on module contains the following core functions:

- Representation of service providers and sub-service providers
- Integration of service providers into the protection requirements analysis

- Assessment of service provider risks (data protection risks, information security risks, individual risks)
- Representation of the links between service providers and IT assets, business processes, information assets, incidents
- Comprehensive contract management
- DEA (service provider recording application: additional web application for assessing service providers via configurable questionnaires)

## 3.4. Module 4: Enterprise risk management

In addition to managing IT risk management, a holistic risk process can be established in QSEC by licensing the add-on module enterprise risk management. By managing individual risks on IT assets, considering business process, organisational and market risks and consolidating all risks in a uniform view, QSEC can support a holistic risk process. The add-on module contains the following core functions:

- Identification of different types of risk
  - Consideration of typical risks in catalogues
  - Recording of new risks (ad hoc risks)
  - Distinction between internal and external risks
  - Distinction between different types of risk
  - Assessment of probability of occurrence and extent of damage
  - Definition of risk owners
  - Definition of affected areas
  - Notification of relevant persons when new risks are identified
- Risk treatment (risk avoidance, risk reduction, risk transfer, risk acceptance)
- Control and tracking (measure tracking, automatic reminders, recertification of risks)
- Documentation
  - Creation of the necessary management reports
  - Consolidation of different risk types into an overall overview
  - Consideration of changes through reports based on the history

# 4. Standards that can be worked with in QSEC

The standards ISO 27001, 27002, 27005 and GDPR are provided by Nexis for working in QSEC (provided that the necessary ISO publications have been licensed by the customer, see Chapter 1). If a new version of one of the standards is published, Nexis will update the question catalogue of the standard concerned within 12 months of publication.

QSEC can be used to work according to the following further standards; however, updates are only carried out on request and subject to a charge.

| Extended standard | Topic |
|---|---|
| B3S- Gesundheit | Security standard for healthcare in hospitals |
| BAIT | IT requirements for banks |
| BDSG | German Federal Data Protection Act |
| BNetzA IT-Sicherheitskatalog 1a | IT security for the energy sector (pursuant to Section 11 (1a) EnWG) |
| BNetzA IT-Sicherheitskatalog 1b | IT security for the energy sector (pursuant to Section 11 (1b) EnWG) |
| BSI C5 | Cloud computing criteria catalogue |
| BSI TR-03109-6 | TR Smart Meter Gateway - SMGW |
| DORA | Digital Operational Resilience Act |
| IATF 16949 | Quality management in the automotive industry |
| ISO/IEC 13485 | Quality management for medical devices |
| ISO/IEC 14001 | Environmental management |
| ISO/IEC 19600 | Compliance |
| ISO/IEC 20000-1 | IT service management |
| ISO/IEC 27001 (i.v.m. 27019) | ISMS according to 27001, extended by requirements for control systems |
| ISO/IEC 27018 | Personal data in the public cloud |
| ISO/IEC 27019 | Information security for control systems |
| ISO/IEC 27701 | Data protection extension of ISO 27001 |
| ISO/IEC 28000 | Security in supply chains |
| ISO/IEC 37001 | Anti-bribery management systems |
| ISO/IEC 45001 | Occupational health and safety |
| ISO/IEC 50001 | Energy management |
| ISO/IEC 55001 | Asset management |
| ISO/IEC 9001 | Quality management |
| IT-Grundschutz für Kommunalverwaltungen | Basic protection for municipal administrations |
| KAIT | IT requirements for corporations |
| MaRisk | Minimum requirements for risk management |
| OH SzA | Guidance on the use of attack detection systems |
| PCI DSS | Payment Card Industry Data Security Standard |
| TISAX | Information security in the automotive industry |
| TKG | German Telecommunications Act with Annexes 1 & 2 |
| VAIT | IT requirements for insurance companies |

| Extended standard | Topic |
| --- | --- |
| VDV 4400 | IT security for transport companies |
| ZAIT | IT requirements for payment and e-money institutions |