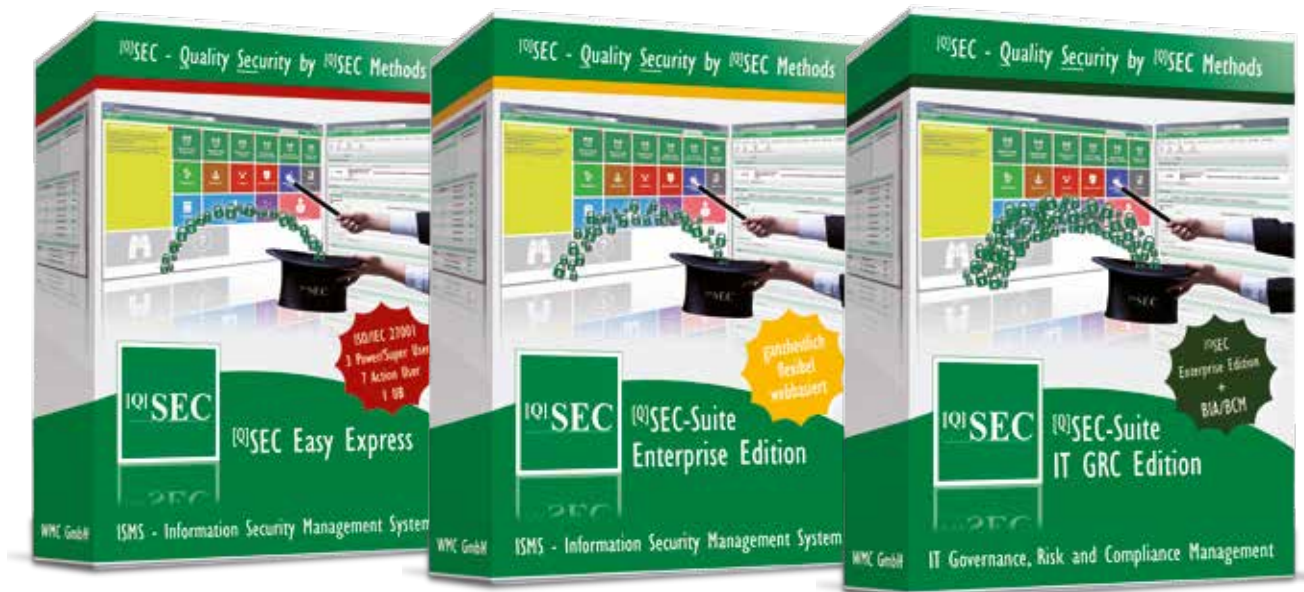


# [Q]SEC Produktvergleich

Version 5.3

WMC bietet Ihnen drei Lösungen für Ihre  
**IT Governance, Risk und Compliance** Themen:



## [Q]SEC Easy Express

für Ihren ISMS-Einstieg

## [Q]SEC-Suite Enterprise Edition

für Ihr ganzheitliches  
und nachhaltiges Information  
Security Management

## [Q]SEC-Suite IT GRC Edition

für Ihr ganzheitliches und  
nachhaltiges IT Governance,  
Risk und Compliance Management

Vergleichen Sie die Leistungsmerkmale der QSEC Produkte in unserem  
Produktüberblick und wählen Sie das Ihren Anforderungen entsprechende Paket aus.

**Wir beraten Sie gerne oder machen Ihnen ein Angebot: +49 40 650336-0**

## Usability

QSEC bietet eine einfache Benutzerführung für Anwender und Experten.	[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
Anwendermodus für „nicht Experten“ mit Kacheldesign	✓	✓	✓
Expertenmodus zur Steuerung der Management (ISMS)-Anforderungen und Verwaltung	✓	✓	✓
Wizards für Anwenderprozessworkflows - Compliance-Wizard - Assessmentplanungs-Wizard - Interview-Wizard (Bestimmung von Geschäftsprozessen, Informations- und Assetbewertungen) - Interview Übernahme-Wizard - Risikobewertungs-Wizard - Maßnahmen Bewertungs-Wizard - Security Incident Wizard	✓	✓	✓
Erfassung von fehlenden Daten bei der Bearbeitung in den Formulare (Fenstertechnik) <b>NEU!</b>	✓	✓	✓
Suchfunktion über alle Module	✓	✓	✓
Fragen & Antworten mit Administratorenbenachrichtigung	✓	✓	✓
Bestätigungs-/ Freigabeworkflow für Security Level Stufen	✗	✓	✓
Wiedervorlagen mit Statusanzeige nach optischer Ampelfarbdarstellung für - Compliance-Bewertungen - Maßnahmenbearbeitungsstatus - Risikobewertungen - Security Incident Bearbeitungen - Security Level Einstufungen - Dokumentenbearbeitungen - BIA/BCM Bearbeitungen	✓	✓	✓
Task-Manager für manuell- und systemerzeugte Aufgaben - Task Übersicht mit Übertragung der Daten in Excel und direkt in Outlook (automatische Aktualisierung) - Integration der Taskerstellungs- und /-bearbeitungsfunktion in jedem Modul - systemerzeugte Task bei Bewertungsveränderungen	✓	✓	✓
Systemerzeugte Benachrichtigungs-Mails für Tasks und Wiedervorlagen	✓	✓	✓
Kundenspezifischer Farbraum einstellbar (RGB) zur Eingliederung in die CI <b>NEU!</b>	✓	✓	✓



## Modul Compliance Management

Ermitteln und verbessern Sie den Compliance Status Ihres Unternehmens.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	- Selfassessment / Ermittlung des Compliance-Status nach PDCA: - Bewerten und kommentieren von PDCA-Status und Reifegraden der Controls - Bewerten und Kommentieren der Fragen	✓	✓	✓
	Planung von Selfassessments für Untersuchungsbereiche und Fragenkataloge, systemgesteuertes Starten von Selfassessments und Aktualisierung der Wiedervorlagen	✓	✓	✓
	Erstellung und Verknüpfung von Maßnahmen zur Verbesserung der Compliance - direkt zu Controls und Fragen mit Verantwortungszuweisung	✓	✓	✓
	Verknüpfung mit Objekten aus anderen Modulen (z. B. Dokumente, weitere Normen) <b>NEU!</b>	✓	✓	✓
<b>Informieren und Sichten</b>	Übersicht über den Compliance Status	✓	✓	✓
	Soll-Ist-Vergleich der Control-Reifegrade	✓	✓	✓
	Erinnerungsfunktion für Fragen-/ Control-Bearbeitung im System und per E-Mail	✓ * nicht per E-Mail	✓	✓
<b>QSEC HIGHLIGHT</b>	Bearbeitung mit dem Compliance-Wizard	✓	✓	✓
	Methode nach ISO/IEC 27001/27002 und PDCA integriert!	✓	✓	✓
	Fragenkatalog nach ISO/IEC 27001/27002 bereits integriert!	✓	✓	✓
	Fragenkatalog nach Bundesdatenschutzgesetz bereits integriert!	✗	✓	✓
	Weitere Normen/ eigene Fragekataloge integrierbar (optional, siehe folgende Seiten)!	✗	✓	✓
	Maßnahmenvorschläge zu Controls 27001 bereits integriert!	✓	✓	✓
	zusätzliche Control- und Fragenerläuterungen, individuell mit dem Administrations-Tool erfassbar	✓	✓	✓
	Abbildung von Key Performance Indikatoren (Reifegrad Scope gesamt und je Control, Verbesserungsmaßnahmen und Kosten)	✓ * eingeschränkt	✓	✓

## Modul IT Risk Management

Ermitteln Sie den Risikostatus Ihrer Assetgruppen. Bewerten Sie die Effektivität Ihrer Maßnahmen.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	Risikobewertung der Assetgruppen nach ISO/IEC 27005:			
	- über Bewertung der Kriterien Vertraulichkeit, Verfügbarkeit, Integrität, Authentizität, Wiederbeschaffungskosten (anpassbar)	✓	✓	✓
	- über Bedrohungs- und Schwachstellenlisten inkl. der möglichen Kombinationen; Basis- der Detailbewertung der Assetgruppen aufgrund der aus den Geschäftsprozessen und Informationen geerbten Kritikalität	✓	✓	✓
	- Angabe des Risikowertes in €	✓	✓	✓
	- Angabe der Risikostufe (A-D) aufgrund der individuell einstellbaren Werte - Angabe der Netto-Risikostufe nach Umsetzung der Maßnahmen	✓	✓	✓
	weitere Attribute individuell erfassbar (Checkboxes, Textfelder, Drop-Down-Felder, Auswahlfelder)	✓	✓	✓
	Anlegen von Bewertungsvorlagen für Assetgruppen	✓	✓	✓
	Planung von Riskassessments für Untersuchungsbereiche und Assetgruppen, systemgesteuertes Starten von Riskassessments und Aktualisierung der Wiedervorlagen	✓	✓	✓
	Generierung von Maßnahmen mit Angabe der Schwachstellenreduzierung direkt aus den Assetgruppen heraus	✓	✓	✓
	Risikobewertung von Maßnahmen: - Kosteneffektivität - gesetzlich vorgeschrieben - Risikoakzeptanzpapier mit Exportfunktion in den Formaten DOC, PDF	✓	✓	✓
<b>Informieren und Sichten</b>	Übersicht über vorbereitende Aktivitäten und Riskassessment-Aktivitäten	✓	✓	✓
	Detaillierte Statusübersicht über die Assetgruppen-Bewertung	✓	✓	✓
	Detaillierte Statusübersicht über die Maßnahmen-Bewertung	✓	✓	✓
	Übersicht über die Spitzenrisiken (Filterfunktion)	✓	✓	✓
<b>QSEC HIGHLIGHT</b>	Risikobewertung über Risikobewertungs-Wizard	✓	✓	✓
	Risiko-Assesment Planung über Wizard	✓	✓	✓
	Methode nach ISO/IEC 27005 integriert!	✓	✓	✓
	Best Practice Schwachstellen- und Bedrohungskataloge bereits hinterlegt!	✓	✓	✓

**NEU!**  
**NEU!**

Individuelle Schwachstellen- und Bedrohungskataloge hinterlegbar (optional)!	✓	✓	✓
Maßnahmenvorschläge zu erkannten Risiken bereits hinterlegt!	✓	✓	✓
Musterdokument zur Methode des IT-Risikomanagements auf Basis ISO/IEC 27005	✓	✓	✓
Risiko-Assessmentverwaltung	✓	✓	✓
Schwachstellen- und Bedrohungserläuterungen über Information-Icons einblendbar, individuell mit dem Administrations-Tool erfassbar	✓	✓	✓
Abbildung von Key Performance Indikatoren (Anzahl Risiken gesamt und je Assetgruppe, Anzahl Risikoakzeptanzen, Risikobearbeitungskosten)	✓* eingeschränkt	✓	✓

## Modul Security Incident Management

Erfassen Sie Incidents, definieren Sie Sicherheitsziele und ergreifen Sie gezielte Maßnahmen bei Security Incidents.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	Erfassung von Incidents: - Kategorien, Schadensarten - Bewertung von Schweregrad, Schadensklasse - Erfassung des Sicherheitsziels - Bemerkungsfelder - Zuweisung zu Verantwortlichen und betroffenen Mitarbeitern/Assetgruppen - mit Erfassung der geplanten / Berechnung tatsächliche Dauer - Verbindung der Incidents mit den Bedrohungen und Schwachstellen	✗	✓	✓
	- weitere Attribute individuell erfassbar (Checkboxes, Textfelder, Drop-Down-Felder, Auswahlfelder)	✗	✓	✓
	Verknüpfung mit Objekten aus anderen Modulen (z. B. Maßnahmen)	✗	✓	✓
<b>Informieren und Sichten</b>	Statusüberblick über laufende und abgeschlossene Incidents mit Kategorisierung, Schweregradbewertung, Schadensklassenbewertung, Verantwortlichen und Wiedervorlagdatum	✗	✓	✓
	Überblick über Spitzen-Incidents, ihre Häufigkeit und betroffene Assetgruppen	✗	✓	✓
<b>QSEC HIGHLIGHT</b>	Best Practice Incident-Kategorien bereits hinterlegt!	✗	✓	✓
	Bearbeitungslaufzeiterfassung Plan/Ist			
	Abbildung von Key Performance Indikatoren (Anzahl Security Incidents in einem Zeitraum, betroffene Assetgruppen, betroffene Geschäftsprozesse)	✗	✓	✓

## Modul Business Continuity Management

**Analysieren Sie Ihre Geschäftsprozesse und die Auswirkungen von Ausfällen. Erfassen Sie Gegenmaßnahmen. Hinterlegen Sie die zugehörige Notfallmanagement-Dokumentation.**

		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	Business Impact Analyse von Prozessen: - Erfassen der regulatorischen, vertraglichen oder technischen Prozessvorgaben (MTPD, RPO, RTO*) mit Wiedervorlagdatum und Kommentarmöglichkeiten - Bewerten von Impacts/ Auswirkungen auf die Prozesse (finanziell, Reputation, Steuerung, rechtlich), Kategorien anpassbar - Ermitteln der Prozesskritikalität und Vorgaben für die sie unterstützenden Assetgruppen	✗	✗	✓
	Erfassen von Maßnahmen für Assetgruppen zur Gap-Reduzierung direkt aus der BIA Gap-Analyse heraus	✗	✗	✓
	BCM: Zuweisen von Notfallplänen zu Geschäftsprozessen und Erfassen von zugehörigen Tests	✗	✗	✓
<b>Informieren und Sichten</b>	BCM: Zuweisen von IT-Notfallplänen, Betriebshandbüchern, Wiederanlaufplänen zu Assetgruppen und Erfassen von zugehörigen Tests	✗	✗	✓
	Übersicht über Impact bewertete Prozesse mit Status, Prozessklassen, Kritikalität, Verantwortlichen und Wiedervorlagdatum	✗	✗	✓
	Überblick auf resultierende Impacts/ Auswirkungen pro Prozess	✗	✗	✓
<b>QSEC HIGHLIGHT</b>	Impact Gap-Analyse der Assetgruppen: - Übersicht über RTO-Soll / RTO-Ist der Assetgruppen und des ermittelten Gaps sowie der zugehörigen Prozessbewertungen - Übersicht über Maßnahmen für Gaps	✗	✗	✓
	Business Impact Zeit- und Werteskalen anpassbar - unternehmensindividuelle Konfiguration der BIA möglich!	✗	✗	✓
	Musterdokument zur Methode des BCM/BIA-Managements inklusive!	✗	✗	✓
	Abbildung von Key Performance Indikatoren (Anzahl kritische Geschäftsprozesse, Anzahl Assetgruppen mit Soll/Ist SLA's, kritische Geschäftsprozesse ohne/mit Notfallplänen, kritische Assetgruppen ohne/mit IT-Notfallplänen, Betriebshandbüchern, Wiederanlaufplänen)	✗	✗	✓

<sup>1)</sup> RTO: Recovery Time Objective  
RPO: Recovery Point Objective  
MTPD: Maximum Tolerable Period of Disruption

## Modul Reporting / Dashboard

Generieren Sie alle benötigten Arbeits- und Managementberichte.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Informieren und Sichten</b>	Standard Reports: Arbeits- und Managementberichte mit administrierbarer Zugriffskontrolle, z. B. Status Compliance Management, Reifegrade im Vergleich von Stichtagen, SoA Bericht	✓	✓	✓
	Export von Reports (z. B. in MS Word, MS Excel, PDF)	✓	✓	✓
<b>QSEC HIGHLIGHT</b>	Individuelle Reports möglich (optional)!	✓	✓	✓
	Verfahrensbericht nach dem BDSG je Geschäftsprozess	✗	✓	✓
	Dashboardgrafiken individuell den Anwendern zuordbar	✗	✓	✓

## Modul Maßnahmen Management

Verwalten Sie die Compliance-, IT Risk-, Security Incident- und Business Continuity- Maßnahmen in Ihrem Unternehmen.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	Erstellen, Bearbeiten, Verknüpfen, Klonen, Zusammenführen von Maßnahmen unter Angabe von: - Ziel- und Wiedervorlage-Daten (mit Erinnerungsfunktion) - Umsetzungsstatus - Kosten - Anforderungsarten - Verantwortlichkeiten - Verknüpfungen mit Objekten in den übrigen Modulen (z. B. Dokumente)	✓ * nicht per E-Mail	✓	✓
	Manuell auslösbare E-Mail-Aufforderung zur Maßnahmen-Aktualisierung an den Verantwortlichen (Status anfordern)	✓	✓	✓
	weitere individuelle Attribute erfassbar (Checkboxen, Textfelder, Drop-Down-Felder, Auswahlfelder)	✗	✓	✓
	Angabe von Reifegradverbesserungen von verbundenen Controls	✓	✓	✓
	Angabe von Schwachstellenverbesserungen (Risikoreduzierung) von verbundenen Schwachstellen	✓	✓	✓
	Maßnahmenschnellerfassung auf der Übersichtsseite	✓	✓	✓
<b>Informieren und Sichten</b>	Benutzerindividuelle Maßnahmen-Übersicht (Filterfunktion): - über laufende, fällige, abgeschlossene, abgebrochene oder durch Risikoakzeptanz nicht durchzuführende Maßnahmen - über Zieldatum, Status, Priorität, Wiedervorlage und Verantwortlichkeiten zu den Maßnahmen	✓	✓	✓
	Maßnahmenbewertung mit den Maßnahmenbewertungs-Wizard <b>NEU!</b>	✓	✓	✓
<b>QSEC HIGHLIGHT</b>	Maßnahmen bei Abwesenheit übertragbar an Stellvertreter, Nachfolgeregelung	✗	✓	✓
	- Abbildung von Key Performance Indikatoren (Anzahl Maßnahmen je Mitarbeiter, nach Status, nach Kosten, nach Wiedervorlage)	✓ * eingeschränkt	✓	✓

# [Q]SEC - integrierte Software, Methodik und Best Practice nach internationalen Standards!

## Modul Dokument Management

Verwalten Sie Ihre IT- und Informationssicherheitsdokumente innerhalb und außerhalb von QSEC.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Bedienen und Steuern</b>	individuell anlegbare Ordnerstruktur	✓	✓	✓
	alle gängigen Dateitypen und Links auf externe Systeme hinterlegbar	✓	✓	✓
	ausführliche Metadaten zu jedem Dokument hinterlegbar	✓	✓	✓
	Zuweisen von Zugriffsrechten pro Dokument	✓	✓	✓
	Verknüpfen mit Objekten aus den übrigen Modulen (z. B. Maßnahmen)	✓	✓	✓
	Versionierung je Dokument einstellbar	✓	✓	✓
	Erinnerungsfunktion im System und per E-Mail	✓* nicht per E-Mail	✓	✓
Intelligente Suchfunktion in Dateinamen und Beschreibung	✓	✓	✓	
<b>Informieren und Sichten</b>	Übersicht über Version, Uploader, Upload-Datum, Größe, Verantwortlichen, Wiedervorlage, Bearbeitungsstatus, Klassifizierung und Inhaltstyp	✓	✓	✓
<b>QSEC HIGHLIGHT</b>	ISM-Platzhalterdokumente (nach der ISO 27001) sind hinterlegt!	✓	✓	✓
	Bereitstellung aller/ausgewählter Dokumente zum Download möglich (.zip)	✓	✓	✓
	Abbildung von Key Performance Indikatoren (Anzahl Dokumente mit Bearbeitungsstatus, Dokumentenart, je Verantwortlicher)	✓* eingeschränkt	✓	✓



## Information Assets

Legen Sie den Grundstein für die Nutzung des IS-Risikomanagements: erfassen Sie die Information Assets (Geschäftsprozesse, Informationen, Assets) Ihres Unternehmens(bereiches).

[Q]SEC  
Easy Express

[Q]SEC-Suite  
Enterprise Edition

[Q]SEC-Suite  
IT GRC Edition

- Geschäftsprozesse mit Prozessownern
- Informationen mit Verantwortlichen
- Assetgruppen mit Verantwortlichen



- Erfassung von weiteren individuelle Attributen bei
- Geschäftsprozessen
- Informationen
- Assetgruppen
- Einzelassets

**NEU!**



Kritikalitätsbewertung der Geschäftsprozesse auf der Basis der verknüpften Informationen und der Einstufung der Attribute Vertraulichkeit, Verfügbarkeit, Integrität etc.)



Kritikalitätsbewertung der mit den Geschäftsprozessen und Informationen verknüpften Assetgruppen / Schutzbedarfsbestimmung aufgrund aller verbundenen Geschäftsprozesse / Informationen nach den eingestufteten Attributen Vertraulichkeit, Verfügbarkeit, Integrität etc.)



Angabe der übergeordneten Assetgruppe(n) für die Assetgruppen (Strukturanalyse)



- Einstufung der Assetgruppen nach Security Level
- Bewertung der Vertraulichkeit und Integrität von Informationen
- Motivationsbewertung
- Empfehlungsprozess durch ISO
- Bestätigungsprozess(Mail/Online) durch Geschäftsführer

**NEU!**



ggf. Geschäftsprozessmusterliste (wenn für die Branche vorhanden)



Informationsmusterliste mit 1.500 Informationsobjekten



Erfassung und Verwaltung von Einzelassets je Assetgruppe inkl. individuellen Attributen

**NEU!**



**Informieren  
und Sichten**

Überblick über die erfassten Information Assets nach Hierarchie oder Tabelle



**QSEC  
HIGHLIGHT**

- Anzeige und Bearbeitung der gesamten Strukturanalyse:
- Organisationseinheit
- Untersuchungsbereich
- zugeordnete Normen
- Geschäftsprozesse
- Informationen
- Assetgruppen

**NEU!**



Abbildung von Key Performance Indikatoren (Anzahl Geschäftsprozesse nach Kritikalität, Anzahl kritische Informationen, Anzahl kritische Assetgruppen, Anzahl Maßnahmen nach Status)



# [Q]SEC - flexibel anpass- und erweiterbar an Ihre individuellen Bedürfnisse!

## Stammdaten

Legen Sie den Grundstein für die Nutzung des ISMS: erfassen Sie die Stammdaten Ihres Unternehmens(bereiches).		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Informieren und Sichten</b>  <b>QSEC HIGHLIGHT</b>	- Geschäfts-/Organisationseinheiten - Untersuchungsbereiche - Standorte - Mitarbeiter, Teams - Mitarbeiter-Rollen	✓* eingeschränkt	✓	✓
	Filterfunktionen für Bearbeitungsansichten	✓	✓	✓
	Nachfolgeregelung für Mitarbeiter mit Übertragung aller Zuständigkeiten und Aktivitäten	✓	✓	✓
	Überblick über die erfassten Stammdaten	✓	✓	✓
	Abbildung von Key Performance Indikatoren (ISO je Geschäfts-/Organisationseinheit, Anzahl Mitarbeiter je ISO)	✓* eingeschränkt	✓	✓

## Basisfunktionen

QSEC bietet Ihnen nachfolgende Basisfunktionen.		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
Ausgeprägtes Berechtigungssystem (Benutzertyp-, Benutzerrollen- und Organisationsberechtigungen)		✓	✓	✓
Benutzerverwaltung		✓	✓	✓
Historisierung		✓	✓	✓
Online-Hilfefunktion		✓	✓	✓

# Profitieren Sie von unserem IT- und Informationssicherheits-Know-how!

## Technik

Für den QSEC-Betrieb gelten nachfolgende technische Voraussetzungen. QSEC ist eine Websolution – keine Softwareinstallation auf dem Client!	[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
- Web-Front-End für mehrsprachigen, unternehmensweiten Zugang zur Software, Internet Explorer ab Version 8, Firefox, Safari usw. - aktuelle .NET-Technologie	✓	✓	✓
- Microsoft SQL Server® 2008 R2, Microsoft SQL Server® 2012 R2 - Windows Server 2008 R2, Windows Server 2012 R2	✗	✓	✓
- Microsoft SQL Server® 2008 R2 Express mit Advanced Services - Windows Server 2008 R2, Windows Server 2012 R2	✓	✗	✗

## Lizenzierung

Lizenzieren Sie QSEC durch Kauf, Miete oder Software as a Service (SaaS).	[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
QSEC Einzellizenz nach Unternehmensgröße	einjährige Nutzungsgebühr	unternehmensgrößenabhängig	
QSEC Komplettlizenz nach Unternehmensgröße	✗	unternehmensgrößenabhängig	
Power/ Super User	max. 3	nach Lizenzierung	
Action User	max. 7	unbegrenzt	
Untersuchungsbereiche	max. 1	nach Lizenzierung	
Erweiterungsmöglichkeiten	✗	✓	

## Update und Support

Für den QSEC-Betrieb gibt es die optimale Unterstützung.	[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
Update	einjährige Nutzungsgebühr	Softwarepflegevertrag	
Support	Support-Service-Karten	Softwarepflegevertrag und nach Vereinbarung	

## QSEC Standard

QSEC - mehr Leistung für Sie!		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Sprachen</b>	Sprache für Benutzeroberfläche und Normencontent: Deutsch (weitere Sprachen siehe Kapitel „QSEC Erweiterungen“)	✓	✓	✓
<b>QSEC-Methode</b>	Norm ISO/IEC 27001/27002 inhaltlich und methodisch bereits integriert	✓	✓	✓
	Methode nach ISO/IEC 27005 integriert	✓	✓	✓
<b>Fragenkataloge</b>	Fragenkatalog nach ISO/IEC 27001/27002 bereits integriert	✓	✓	✓
	Fragenkatalog nach Bundesdatenschutzgesetz bereits integriert	✗	✓	✓
<b>Maßnahmen- vorschläge</b>	Maßnahmenvorschläge zu Controls 27001 bereits integriert	✗	✓	✓
	Maßnahmenvorschläge zu erkannten Risiken bereits integriert	✗	✓	✓
<b>Schwachstellen- und Bedro- hungskataloge</b>	Best Practice Schwachstellen- und Bedrohungskataloge bereits hinterlegt	✓	✓	✓
<b>Incident- Kategorien</b>	Best Practice Incident-Kategorien bereits hinterlegt	✗	✓	✓
<b>Flexibilität</b>	Web-Anwendung mit zentraler Datenbank	✓	✓	✓
	Customizing: Untersuchungsbereiche, Organisation, Prozesse, Skalenwerte, Kriterien, Logo, Farbgebung uvm.	✓	✓	✓
<b>Dokumentation</b>	Online-Hilfefunktion (Online-Benutzerhandbuch)	✓	✓	✓
	Bedienungsleitfaden (in QSEC integrierte Prozesse)	✓	✓	✓
	Musterdokument zur Methode des IT-Risikomanagements auf Basis ISO/IEC 27005	✓	✓	✓
	Musterdokument zur Methode des BCM/BIA-Managements	✗	✗	✓

## QSEC Erweiterungen

Sie haben die Wahl - profitieren Sie optional von den QSEC-Erweiterungsmöglichkeiten!		[Q]SEC Easy Express	[Q]SEC-Suite Enterprise Edition	[Q]SEC-Suite IT GRC Edition
<b>Sprachen</b>	Sprache für Benutzeroberfläche und Normencontent: Englisch	✗	✓	✓
	Weitere Sprachen für Benutzeroberfläche und Normencontent auf Anfrage	✗	✓	✓

<b>Fragenkataloge</b>	Integrierbare Normen/ Fragekataloge:			
	Sicherheitsmanagement (27001 / 27002)	✓	✓	✓
	Bundesdatenschutzgesetz (BDSG)	✓	✓	✓
	Qualitätsmanagement (ISO 9001)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Umweltmanagement (ISO 14001)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Payment Card Industry Data Security Standard (PCI DSS)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Service Management (ISO 20000)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Sarbanes Oxley Act (ohne Fragenkatalog)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Medizinprodukte-Qualitätsmanagement (13485)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Risikomanagement (27005)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Notfallmanagement (22301)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	VDA ISMS (Version 2.0)	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	Österreichisches Datenschutzgesetz	gegen Aufpreis	gegen Aufpreis	gegen Aufpreis
	weitere Normen/ eigene Fragekataloge eigenständig bzw. gegen Aufpreis durch WMC integrierbar	✗	✓	✓
<b>Schwachstellen- und Bedrohungskataloge</b>	Individuelle Schwachstellen- und Bedrohungskataloge hinterlegbar	✓	✓	✓
<b>Reports</b>	Individuelle Reports möglich (optional)	✓	✓	✓
<b>QSEC Administrations-Tool</b>	Katalog-Erfassungs- und Pflgetool KEP-Tool	✗	✓	✓
	Konfigurationsadministrations-Tool	✗	✓	✓
<b>Schnittstellen</b>	Mailsystem	✓	✓	✓
	MS Active Directory (mit SSO Funktion)	✗	✓	✓
	Asset System Spider (Customizing erforderlich)	✗	✓	✓
	Incident Import aus Ticketsystem (Customizing erforderlich)	✗	✓	✓
	individuelle Schnittstellen integrierbar	✗	✓	✓

## Beratung und Schulung (optional)

**Wir liefern mehr als Software. Profitieren Sie von unserem Know-how.**

### **Beratungsfelder** IT-Strategie und -Organisation

Prozess- und Qualitätsoptimierung

ISMS-Einführung

Risikomanagement

Erstellen von Security Policies

Penetrationstests

Vulnerability Assessment

Datenschutz

Assetmanagement

Lizenzmanagement

Vertragsmanagement

Business Impact Analyse

Notfallplanung und Disaster Recovery

Business Process Management

### **Schulungen** Individualschulungen QSEC

Gruppenschulungen QSEC

# Über WMC

**SecurITy** made in Germany Mit den QSEC-Suiten ist WMC ein führender Anbieter integrierter Information Security Management Systeme und ausgezeichnet mit dem Prädikat „IT-Security made in Germany“.

Als Spezialist für Compliance und ganzheitliche Information Security und IT LifeCycle Management verfügt WMC über langjährige Umsetzungserfahrung von weltweiten Projekten.

QSEC unterstützt unsere Kunden im Compliance Management und Information Security Management nach internationalen Standards (ISO 27001, ISO 27005, ISO 20000, PCI DSS u.v.m.) bedienerfreundlich, methodisch und mit allen erforderlichen Leistungsmerkmalen.

Mit zertifizierten Mitarbeitern und tiefen Branchen- und Prozesskenntnissen (und dem WMC-Expertennetzwerk) erzielen wir für unsere Kunden klare Wettbewerbs- und Imagevorteile im Informations- und Prozessmanagement.

WMC ist zertifizierter Microsoft Partner ISV und Mitglied bei TeleTrust – Bundesverband IT-Sicherheit e.V.



TeleTrust – Bundesverband IT-Sicherheit e.V.  
Regionalstelle Hamburg  
vertreten durch die WMC GmbH  
[www.teletrust.de](http://www.teletrust.de)

