>>EGOS! Comprehensive Security & Functionality Check

*Wenn die Fähigkeit einer Organisation **Informations- oder IT-Sicherheit** zu implementieren, Dritten gegenüber bewiesen werden muss (z.B. Kunden, internen oder externen Auditoren) oder intern auf Basis eines pragmatischen Ansatzes getestet werden soll, ist es empfehlenswert einen **Sicherheitstest** anzuwenden, der generisch genug ist, dass er an die Bedürfnisse der Organisation und des Audits angepasst werden kann.*

Die hier im Weiteren dargelegte Vorgangsweise kann auch unter dem Aspekt der **Funktionalitätsüberprüfung** (Validierung oder Audit) einer IT-Landschaft angewendet werden, sodass diese Aspekte vorrangig vor reinen Informations- oder IT-Sicherheitsaspekten behandelt werden. Ein generischer Sicherheitstest behandelt alle wesentlichen Aspekte von Informations- und **IT-Sicherheit in Hinblick auf die Informationswerte** der betrachteten Organisation.

Wir bieten dazu den Comprehensive Security & Functionality Check an, der aus ISO27001, anderen relevanten Standards des Risiko- und Continuity Managements sowie einem Schichtenmodell zusammengesetzt wurde.

Der Comprehensive Security & Functionality Check ist ein Ergebnis kontinuierlicher Forschung nach verbesserten Test- und Auditmethoden und kombiniert technische und organisatorische Zugänge aus internationalen, generischen und branchenspezifischen Standards und Best Practice. Zur Implementierungsreife gelangt im Jahr 2002 wurde der Comprehensive Security & Functionality Check seither in zahlreichen Organisationen und Unternehmen von 100 bis 2000 Mitarbeitern eingesetzt.

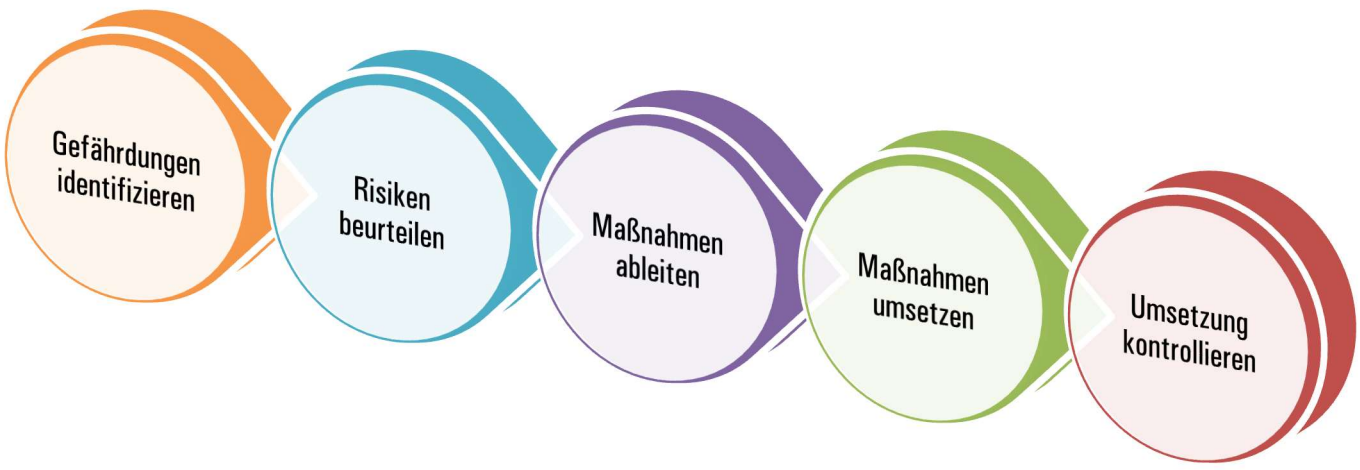
Ein CSFC kann wirkungsvoll eingesetzt werden, wenn

- die **Funktionalität** von IT-Abläufen Bezug nehmend auf IT-Betriebsabläufe oder Geschäftsprozesse geprüft werden sollen.
- die **Informationssicherheit** eines Unternehmens ganzheitlich betrachtet werden soll.
- punktgenau **Verbesserungspotential** auf den funktionellen Ebenen des CFSC festgestellt werden soll.

Tipp

Der CSFC ist als Baustein auf dem Weg zu einer ISO27001 Zertifizierung verwendbar. Der Ergebnisreport kann als Nachweis der Basis-Sicherheitschecks verwendet werden.

Version 14-02.05.16



>>EGOS! Comprehensive Security & Functionality Check

EGOS! the education company

Der EGOS! Comprehensive Security & Functionality Check (CSFC)

Im Rahmen eines CSFC wird das Unternehmen in funktionelle Schichten „geteilt“, auf denen sich jeweils sehr spezifische Funktionalitäts- und Sicherheitsfragen stellen, die im Rahmen einer **ganzheitlichen Betrachtung** berücksichtigt werden müssen, um sicherzustellen, dass **Betriebsabläufe oder Geschäftsprozesse** effektiv, effizient und ihrer definierten Funktionalität entsprechend ablaufen können.

Funktionelle Schichten des CSFC

Im Zuge des Testes werden diese fünf Schichten nunmehr ausgehend von einer Definition des Betriebsablaufs oder Geschäftsprozesses vertikal durchlaufen, sodass in jeder Schicht die Tragfähigkeit der bereits existierenden Maßnahmen gegenüber definierten Anforderungen überprüft werden kann.

Layer	Schicht	Teilbereiche (Auszug)	Testing
 **5**	Prozesse	Geschäfts- und IT-Prozesse	internal
		Security Management	internal
		Backup- und Notfall-Strategien	internal
		ITIL-Konformität	internal
 **4**	Applikationen	Web-Seiten und Web-Applikationen	internal/external
		E-Commerce Lösungen	internal/external
		Communication & Collaboration	Internal/external
		ERP/CRM	internal
 **3**	Hardware Betriebssysteme	Servers (Betriebssysteme, Applikationsserver,..)	internal/external
		Clients (PC’s, Mobile Devices, Antivirus,…)	internal/external
		Large Scale Systems	internal/external
		Cloud Security	internal/external
 **2**	Networking	Network Devices (Routers, Switches, Firewalls, Access Points,…)	internal/external
		Network Infrastructure (DMZ, WAN, Internet,…)	internal/external
 **1**	Physical Security	Zutritt zu Räumen & Zutritts-Kontrollen	external
		Überwachung und Monitoring (Loging, Brand, Wasser, Notfallpläne,..)	internal
		Benutzerverhalten, Benutzerrichtlinien	internal/external

>>EGOS! Comprehensive Security & Functionality Check

Worin liegt der Nutzen eines CFSC?

Nutzen auf organisatorischer Ebene

- Eine klare strategische Übersicht über Möglichkeiten, Geschäftsprozesse in Hinblick auf Informationssicherheit oder Funktionalität zu verbessern.
- Identifizierung organisatorischer Risiko und Bedrohungsfaktoren bzw. Rückkopplungsaussage über den Einfluss von technischen oder sicherheitstechnischen Störungen auf die untersuchten Geschäftsprozesse oder Betriebsabläufe.

Nutzen auf technischer Ebene

- Bestimmung des Grades physikalischer Sicherheit für Informationswerte.
- Detaillierte Sicherheitsstudie über Sicherheitsrisiken, Bedrohungen und technische Schwachstellen (Vulnerabilities) sowie organisatorische Sicherheitsprobleme.
- Genaue Dokumentation der IT Umgebung auf OSI-Schichten 2, 3 und 7 (falls notwendig)
- Dokumentierte Bestimmung von Abhängigkeiten in der IT Landschaft, die in kritischen Situationen reduzierter Verfügbarkeit, Vertraulichkeit oder Integrität unterstützend zur Problemlösung verwendet werden kann.
- Bei Rückkopplungstests: Bestimmung der Funktionsfähigkeit von technischen Betriebsabläufen und deren genaues Auswirkungspotential im Störungsfall in Hinblick auf die vorgelagerten Geschäftsprozesse.

Ablauf eines Comprehensive Security & Functionality Checks

Ein CSFC wird in den folgenden Schritten ausgeführt

Aufwände für einen CSFC

Basierend auf unserer Implementierungserfahrung können die folgenden Werte angenommen werden:

Service Modul	Dauer (Personentage)		
	Minimum	Maximum	Multiplikator
Bestimmung Organisatorischer Umfang	0,5 Tage	2 Tage	Anzahl Standorte & Prozesse
Bestimmung Technischer Umfang	0,5 Tage	2 Tage	Anzahl Systeme
Risikoanalyse – und bewertung (optional)	0,5 Tage	2 Tage	Branche, Risiken
Durchführen der organisatorischen Tests	1 Tag	3 Tage	Anzahl Systeme
Durchführen der technischen Tests	1 Tag	5 Tage	Anzahl Systeme
IT System Abhängigkeitstest (optional)	1 Tag	5 Tage	Anzahl Systeme
Berichterstellung und Präsentation	1 Tag	2 Tage	Anzahl Findings
Erneute Tests nach Umsetzung der Maßnahmen (optional)	1 Tag	3 Tage	Anzahl Findings
Gesamtdauer	**5 Tage**	**24 Tage**	

Alle Service Module können unabhängig voneinander bestellt und ausgeführt werden mit Ausnahme des Moduls zur Umfangsbestimmung, das vor allen anderen ausgeführt werden muss.

Die maximale Dauer zur Ausführung eines einzelnen Moduls hängt von den genauen inneren, zuvor erfassten, Gegebenheiten ab und muss, abhängig vom Umfang, mit den jeweiligen Multiplikatoren multipliziert werden, um die Gesamtdauer zu erhalten. Die im Rahmen von Angebotsgesprächen oder bei besonders komplexen Projekten im Rahmen des allerersten Projektschritts durchgeführte genaue Umfangsuntersuchung liefert typischerweise die genauen anzuwendenden Maximalwerte.

Anwendungsbeispiel

Eine Organisation mit einem Standort, 3 kritischen Geschäftsprozessen und 5 Systemen benötigt Dienstleistungen zwischen 7,5 und 10 Personentagen; inklusive Dokumentation und Abhängigkeitsanalyse werden zwischen 10 und 20 Personentage benötigt. Der tatsächliche Wert wird durch den Projektteil Umfangsbestimmung festgelegt.

Auf Grund seiner modularen Struktur und seines ganzheitlichen Ansatzes liefert der Comprehensive Security & Functionality Check zügige Ergebnisse in unübertroffener Genauigkeit, die den Kunden in die Lage versetzen, einen klaren Einblick in die Situation der eigenen Sicherheitsmanagement-Organisation und IT-Infrastruktur zu gewinnen. Daraus können gezielte Maßnahmen abgeleitet werden, die zu einer nachhaltigen, langfristigen Verbesserung der unternehmensweiten Informations- oder IT Sicherheit beitragen oder die Gestaltung und Abstimmung von Geschäftsprozessen und technischen Betriebsabläufen wesentlich erleichtern und optimieren.

Sicherheitshinweis

Ein Comprehensive Security & Functionality Check kann innerhalb des EGOS! Sicherheitsmodells in 3 verschiedenen Geheimhaltungsstufen ausgeführt werden, die an die Sicherheitsbedürfnisse der Organisation angepasst werden:

- Grundstufe (Industriestandard)
- Aufbaustufe (Erhöhter Industriestandard)
- Regierungsstandard

In besonders sensiblen Situationen ist die Ausführung aller Arbeiten vor Ort auf Geräten des Kunden empfehlenswert.