Security-Check nach ISO 27001

„Stage-Reviews helfen in der Implementierungsphase von Informationssicherheit – als unabhängige Projekt-fortschrittsüberwachung."

- **CIS-Stage-Review liefert Stärken-/Schwächen-Profil und Optimierungspotential für Informationssicherheit**
- **BRZ, Telekom Austria und Tectraxx profitieren durch Kurz-Audit**

Für Unternehmen, die Informationssicherheit nach einem internationalen Standard implementieren wollen, bietet die Zertifizierungsorganisation CIS sogenannte Stage-Reviews als „Standortbestimmung". Diese Beurteilung durch unabhängige Auditoren gibt Aufschluss über Stärken und Schwächen eines InformationsSicherheitsManagementSystems (ISMS) und zeigt Verbesserungspotenziale auf.

So werden Fragen beantwortet, die im Zuge eines ISMS-Projekts oft zu Unsicherheit führen: Wurden alle Risiken richtig bewertet? Gibt es unentdeckte Gefahrenpotenziale? Wurde der ISO-Standard richtig interpretiert? Sind die Security-Maßnahmen ausreichend?

Inhaltlich richtet sich ein CIS-Stage-Review an der international anerkannten Norm für Informationssicherheit ISO 27001 aus, die neben technischer IT-Sicherheit auch Aspekte wie Organisation, Gebäude- und Umgebungssicherheit oder Mitarbeiter-Awarness einbezieht. „Ein Stage-Review ist **besonders in der Implementierungsphase** von Informationssicherheit empfehlenswert – als unabhängige Projektfortschrittsüberwachung und zur besseren Einschätzung der tatsächlich notwendigen Sicherheitsmaßnahmen“, erklärt CIS-Geschäftsführer Erich Scheiber. Denn ein Zuwenig an Sicherheit könne genauso unwirtschaftlich sein, wie ein Zuviel.

Zur Durchführung einer Ist-Analyse mit Stärken/Schwächen-Profil im Rahmen eines CIS-Stage-Reviews werden die individuellen Risiken in Abhängigkeit von der Firmengröße und Branche erhoben, die bereits vorhandenen Sicherheitseinrichtungen sowie organisatorische Security-Maßnahmen evaluiert und dem Anforderungsprofil nach ISO 27001 gegenübergestellt. Das Ergebnis ist ein mehrseitiger Auditbericht, der eine Stärken-/Schwächen-Beurteilung sowie konkrete Verbesserungsmöglichkeiten liefert.

Standortbestimmung im Bundesrechenzentrum

Das Bundesrechenzentrum setzte im Zuge seiner ISMS-Implementierung zwei Stage-Reviews der Zertifizierungsorganisation CIS als strategische Meilensteine ein: einmal zu Beginn der Implementierungsphase sowie einige Monate später als Zwischen-Check. „Beim Aufbau eines InformationsSicherheitsManagementSystems – ISMS – in einem so komplexen Rechenzentrum bietet ein Stage-Review dem Projektteam geplante Kontrollpunkte, an denen die Angemessenheit der Maßnahmen geprüft wird. Diese Zwischenbeurteilung steigert die Motivation des Teams und liefert zusätzliche Anregungen. Der Auftraggeber erhält damit einen objektiven Fortschrittsbericht“,erklärt Johannes Mariel, IT-Leiter im Bundesrechenzentrum.

„Ein Stage-Review steigert die Motivation des Teams und liefert zusätzliche Anregungen.“

Johannes Mariel,
Bundesrechenzentrum GmbH

Die Durchführung eines CIS-Stage-Reviews brachte eine Projektzeitverkürzung um sechs Monate.

Zeitersparnis bei Telekom Austria

Für den Bereich Services & Network Operations (SNO) der Telekom Austria brachte die Durchführung eines CIS-Stage-Reviews eine Projektzeitverkürzung um sechs Monate. „Das Management wollte eine rasche Implementierung in zwölf Monaten, während die IS-Beauftragten eher mit 18 Monaten gerechnet hätten. Nach dem Stage-Review hatten wir einen so guten Überblick über die noch zu bewältigenden Aufgaben, dass der Zeitplan revidiert werden konnte. Schließlich wurde die Zertifizierung schon nach elf Monaten realisiert", berichtet Mag. Krzysztof Müller, Informationssicherheitsbeauftragter der Telekom Austria.
Insgesamt ging es dabei um die Präzisierung von Normforderungen, zugeschnitten auf den SNO-Bereich der Telekom Austria. Denn beim Durcharbeiten des Implementierungsleitfadens ISO 27002 hatte sich heraus kristallisiert, dass die Norm viel Interpretationsspielraum zulässt. So wird ein „angemessenes Risikomanagement" gefordert, aber nicht näher ausgeführt, was „angemessen" bedeutet – da dies von den individuellen Sicherheitsanforderungen abhängt. „Daher war uns eine Zustandsbestimmung von Seiten des Zertifizierers wichtig. Wenn die Auditoren, die später das ganze System begutachten, zu Projektbeginn eine Kursbestätigung oder -korrektur anzeigen, kann man nicht so falsch liegen", betont Müller und führt aus: „So eine freiwillige Vorbegutachtung können wir empfehlen – als hilfreiche Wegbegleitung, weil die Umsetzung der Norm alles andere als Routine ist."

Wettbewerbsvorteil für Tectraxx

Auch kleinere Dienstleister im Umfeld von Großunternehmen nutzen die Vorteile der ISO 27001 und einer Standortbestimmung mittels CIS-Stage-Review. Der zuständige Information-Security-Manager bei Tectraxx, einem Anbieter für Logistic- und After-Sales-Services in der Telekommunikation: „Schon die Ankündigung, dass wir ein Sicherheitssystem nach ISO 27001 einführen, hat sich als wesentlicher Unterschied zum Mitbewerb erwiesen. Unsere Kunden wie Nokia oder Siemens sind sehr daran interessiert, dass ihr Dienstleister diesen Sicherheitsstandard erfüllt." Die Geschäftsführung konnte nach dem Stage-Review die Leistungen des IT-Teams objektiver einschätzen, während die IT-Beauftragten Bestätigung und Kurskorrektur erhielten.

Das CIS-Stage-Review

Auditplanung: garantiert die effiziente Abwicklung
Audit: Evaluierung von Risiken, Stärken/Schwächen und Optimierungspotenzial
Auditbericht: Bewertung von Stärken/Schwächen und Verbesserungsmöglichkeiten

Von der Implementierung zum Zertifikat

- **Informationssicherheit nach ISO 27001**
- **IT-Service-Management nach ISO 20000**

Informationsgespräch
CIS-Erstgespräch: Details über Zertifizierungsprozess. Dann Registrierung, Projektplanung.

Analyse
Interne Evaluierung des Verbesserungspotentials, Bewertung vorhandener Maßnahmen.*

Implementierung
Maßnahmenumsetzung nach ISO 27001 und/oder ISO 20000 im Unternehmen.*

*Die CIS als unabhängige Prüfstelle ist nicht involviert

CIS Stage Review (Vorbeurteilung)
Optional: Projektbegleitende Prüfung der implementierten Elemente durch CIS-Auditoren.

CIS System & Risk Review (Vorbegutachtung)
CIS prüft Interpretation der Normforderungen und Dokumentation, „Generalprobe".

CIS Certification Audit
Überprüfung des Systems durch multiple Stichproben. Auditbericht mit zukünftigem Verbesserungspotenzial. Das CIS-Zertifikat nach ISO 27001 / ISO 20000 gilt 3 Jahre.

CIS Surveillance Audit
Das einmal pro Jahr durchgeführte Surveillance Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.

CIS Recertification Audit
Nach 3 Jahren haben Sie die Möglichkeit, das abgelaufene Zertifikat erfolgreich zu erneuern.

CIS - Ihr Standard für Sicherheit

CIS - Certification & Information Security Services GmbH • A - 1010 Wien • Gonzagagasse 1/4/25 A • Tel: +43 (0)1 532 98 90, Fax: +43 (0)1 532 98 90 9 • E-Mail: office@cis-cert.com • Web: www.cis-cert.com