ISMS als Fundament für den Cybersecurity Schutz

(Information Security Management System)

CAIRO

secure • digital • IT-infrastructures

ISMS (Information Security Management System)

Ein ISMS ein unabdingbar System, um die IT-Sicherheit in ihrem Unternehmen zu garantieren. Es handelt sich dabei nicht um ein IT-System sondern um eine Kollektion von Dokumenten wie z.B. Leitlinien oder Richtlinien, teilweise mit starken Bezügen zu der Organisation, zu den Stellenbeschreibungen inkl. vertraglicher Dokumente zwischen Arbeitgeber und Arbeitnehmer.
Reine technische Lösungen wie Antivirus/Anti-Spam, Firewall oder Schwachstellenmonitoring sind ebenso nötig- sind aber nicht ausreichend. Vielmehr müssen die Organisation, Prozesse und Verfahren bis zu den Notfallplänen richtig aufgesetzt werden, um Attacken zu vermeiden oder bei einer erfolgreichen Attacke richtig zu reagieren. Auch Cyber-Versicherungen fordern zumindest Teile eines ISMS ab, um den eventuellen Schaden überhaupt zu übernehmen.

Der schnelle Weg zu einem ISMS

Die Compliance Normen selbst zeigen den Weg und Struktur für ein ISMS auf. Allerdings sind diese Standards entweder „zu konkret“ bzw. zu „kleinteilig“ formuliert mit Umfängen bis 5.000 Seiten (BSI IT-Grundschutz, ISO 27000) oder sind mittelstandsgerecht klein gehalten mit circa 50 Seiten & flexiblen Kategorien (VdS 10000) ohne konkrete IT-Inhalte.
Völlig unabhängig davon welcher Norm Sie folgen wollen; eine ISMS-Dokumentenstruktur oder Umfang selbst ist nicht vorgegeben – diese muss nur alle Anforderungen abdecken und gleichzeitig praktikabel zu nutzen sein. Der praktische Nutzen ist dann erfüllt, wenn das ISMS leicht und schnell lesbar & verständlich für alle Mitarbeiter, konkret in der Anwendung und auch leicht zu pflegen ist.
Der schnelle Weg zu einem ISMS ist ein Satz von konkreten Dokumenten-Templates, die jeweils leicht zu korrelieren sind, mit Kategorien und geforderten Maßnahmen aller Normen und genau dies ist der **CAIRO ISMS Baukasten.**

CAIRO ISMS Baukasten

Der CAIRO ISMS Baukasten erlaubt die schnelle Realisierung eines normgerechten und praxisnahen ISMS, dass auch von der Organisation akzeptiert und „gelebt“ wird.
Im Zentrum der Richtlinien stehen immer konkrete Dinge wie zum Beispiel ein kritisches System (Applikationen wie ERP, HR, IoT) oder die Aufgaben/Rollen eines Sicherheitsbeauftragten (ISB) der Datenschutzmanager (DSM). Der Baukasten enthält die überschaubare Menge von nur 16 Dokumenten bzw. Templates zur Abdeckung aller Normen.

Leitlinien

- ISMS
- Kritische Systeme
- DSGVO

Verträge

- Vertraulichkeit
- Erklärung und Akzeptanz

Richtlinien

- Informationssicherheit und Organisation
- Nutzung der Kommunikationsinfrastruktur
- Kritisches System im Detail
- Nutzung von Software und Hardware
- Betrieb von Software und Hardware
- Nutzung und Betrieb Rechenzentrum
- Sicherheitsprozesse
- Risikioanalyse und Maßnahmen
- Notfallplan für IT
- Notfallplan für Anwender
- DSGVO

Strukturierung und Dokumenten-Workflow für Compliance

Am Anfang empfiehlt es sich nach Festlegung der Rollen kooperativ die Muster-Dokumente z.B. in Microsoft Teams die firmenspezifischen Dinge zu ergänzen und zu finalisieren.
Danach kann man optional ein Compliance Workflow- & Dokumentationssystem wie Intervalid einführen, um zukünftig schneller und zielgerichtet Anpassungen vorzunehmen.
Gerade wenn die Firma regelmäßig auditiert wird oder einen besonderen Fokus auf Sicherheit hat, hilft Intervalid mit seinen Funktionen wie Normen-Kataloge, Verzeichnis inkl. Bewertung der Lieferanten, Asset Register, Darstellung der Security Organisation, Schulungskontrolle oder Tracking der Vorfälle und Maßnahmen ein ISMS kostengünstig zu erstellen und zu pflegen.
Im Zusammenspiel mit dem CAIRO ISMS Baukasten ist das die aktuell beste Lösung für den Betrieb & die Pflege eines ISMS. CAIRO ist Intervalid Partner für den Verkauf und die Implementierung.

CAIRO und Ihr professionelles ISMS: „Kill three flies with one stone“

CAIRO - mit seinen neuen CAIRO ISMS Baukasten und optional mit Intervalid - bringt Sie schnell und kostengünstig zu Ihrem professionellen ISMS, erhöht damit signifikant Ihre Cyber Sicherheit, schafft die Voraussetzungen für einen erfolgreichen Audit und deckt ebenso die Anforderungen Ihre Cyber-Versicherung ab.
Der Baukasten ist kostenlos – eine Voll-Implementierung startet ab 5.000€ - eine Teilimplementierung bereits ab 2.000€ je nach Umfang und Firmengröße.

Sicherheitsstandards und Normen

Standard	ISO/IEC 27001 TISAX®	BSI IT-Grundschutz Standardabsicherung	VdS 10000
Herausgeber	International Standards Organisation	Bundesamt für Sicherheit in der Informationstechnik	VdS Schadenverhütung GmbH
Zielgruppe	Organisationen jeder Größenordnung	Organisationen jeder Größenordnung, öffentliche Verwaltung	kleine und mittlere Unternehmen
Norm-Umfang	groß (ca. 400 Seiten)	sehr groß (ca. 5.000 Seiten)	klein (ca. 40 Seiten)
Norm-Art	generisch formulierte Anforderungen	konkret formulierte Anforderungen	generisch und praktisch formulierte Anforderungen, mit Kann/ Muss-Kriterien
Aufwand der ISMS Implementierung (extern)	**30 - 300 PT** Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	**30 - 300 PT** Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit	**10 - 100 PT** Beratungsleistung zur Herstellung der Zertifizierungsfähigkeit
Aufwand der ISMS Implementierung (intern)	**60 - 600 PT**	**100 - 1200 PT**	**20 - 120 PT**
interne und externe Aufwand mit dem CAIRO ISMS Baukasten	**50%**	**50%**	**50%**

CAIRO ISMS Baukasten ist ein Teil unseres Security & Compliance Portfolios von normgerechten Security-Prüfungen, über die Behebung aller Schwachstellen bis zum sicheren IT-Betrieb mit modernen Lösungen, CAIRO Security Managed Services oder Security Awareness Trainings.

CAIRO ist VdS 10000 zertifiziert für ein Informationssicherheits-Management System (ISMS).

Tel.: +49 (0)621 86 75 10
Mail: info@cairo.ag
Web: www.cairo.ag

CAIRO
secure • digital • IT-infrastructures

Kontakt