36 %

CertMe

Mit uns sicher zertifiziert.

Widerstandsfähigkeit gegen Cybervorfälle durch ISO 27001 und EU NIS2

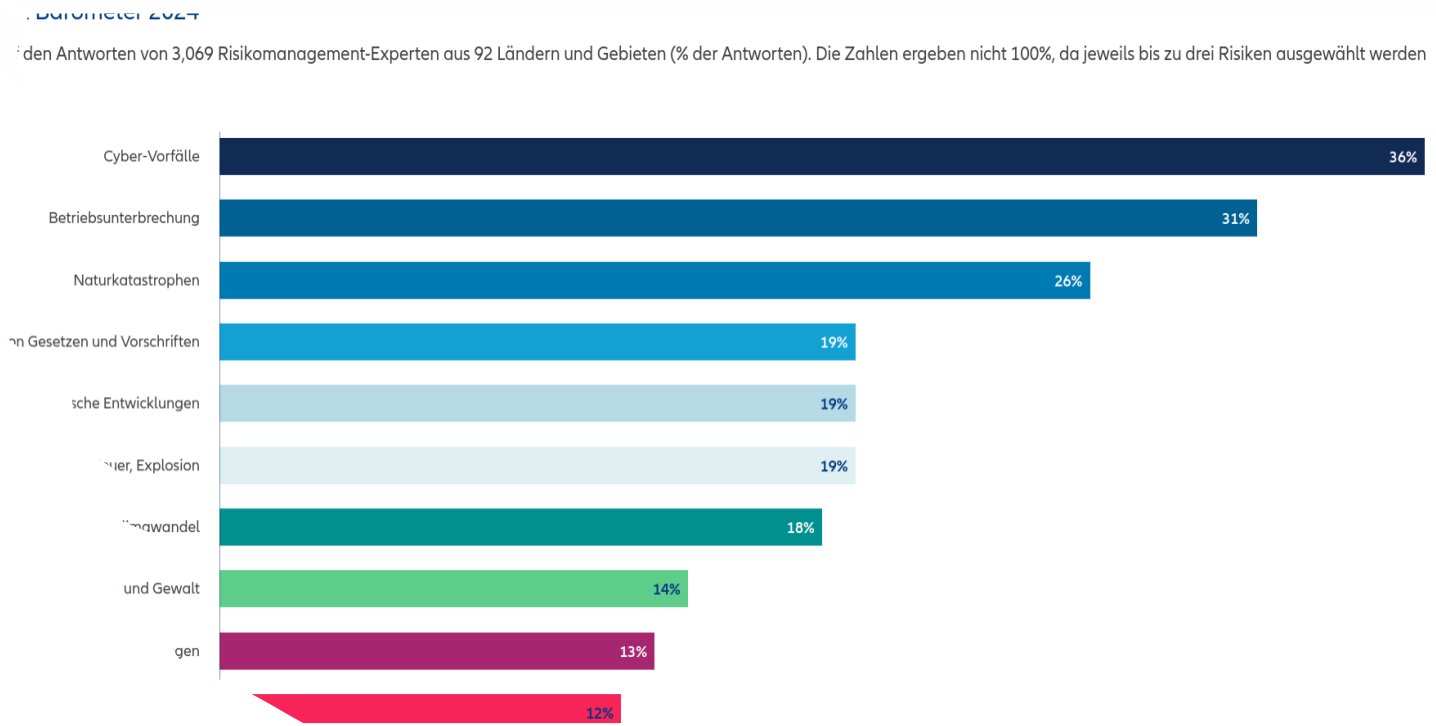
Version: 2 rev 4;
Autor: Eduard Senn am 26.12.2023;
Last Modify: 08.01.2024

Hard Facts 2023

1. Cyber Incidents (36%)
2. Business Interruption (mit Lieferkette) (31%)
3. Naturkatastrophen (26%)

Hard Facts 2024 (Global)

1. Cyber Incidents
2. Business Interruption (mit Lieferkette)
3. Naturkatastrophen
4. Änderungen von Gesetzen
5. Makroökonomische Entwicklungen
6. ...



Hard Facts 2024 (Österreich)

1. Cyber Incidents
2. Makroökonomische Entwicklungen
3. Betriebsunterbrechung
4. Änderungen von Gesetzen
5. Klimawandel
6. Naturkatastrophen
7. ...

Darum, macht’s Sinn

Die ISO/IEC 27001 Norm ebenso wie Network and Information Systems Directive (NIS2) der Europäischen Union sind beides risikobasierende Ansätze, die darauf abzielen die Cyber- und Informationssicherheit in kritischen Sektoren (KRITIS) zu stärken sowie die Zusammenarbeit zwischen den Mitgliedsstaaten, den Behörden und Unternehmen zu fördern.

Im Zuge der Einführung der EU NIS2 Richtlinie wurde der Anwendungsbereich deutlich breiter gefasst, in dem auch Bereiche wie die öffentliche Verwaltung, das Gesundheitswesen sowie das herstellende bzw. verarbeitende Gewerbe uvm. aufgenommen wurden.

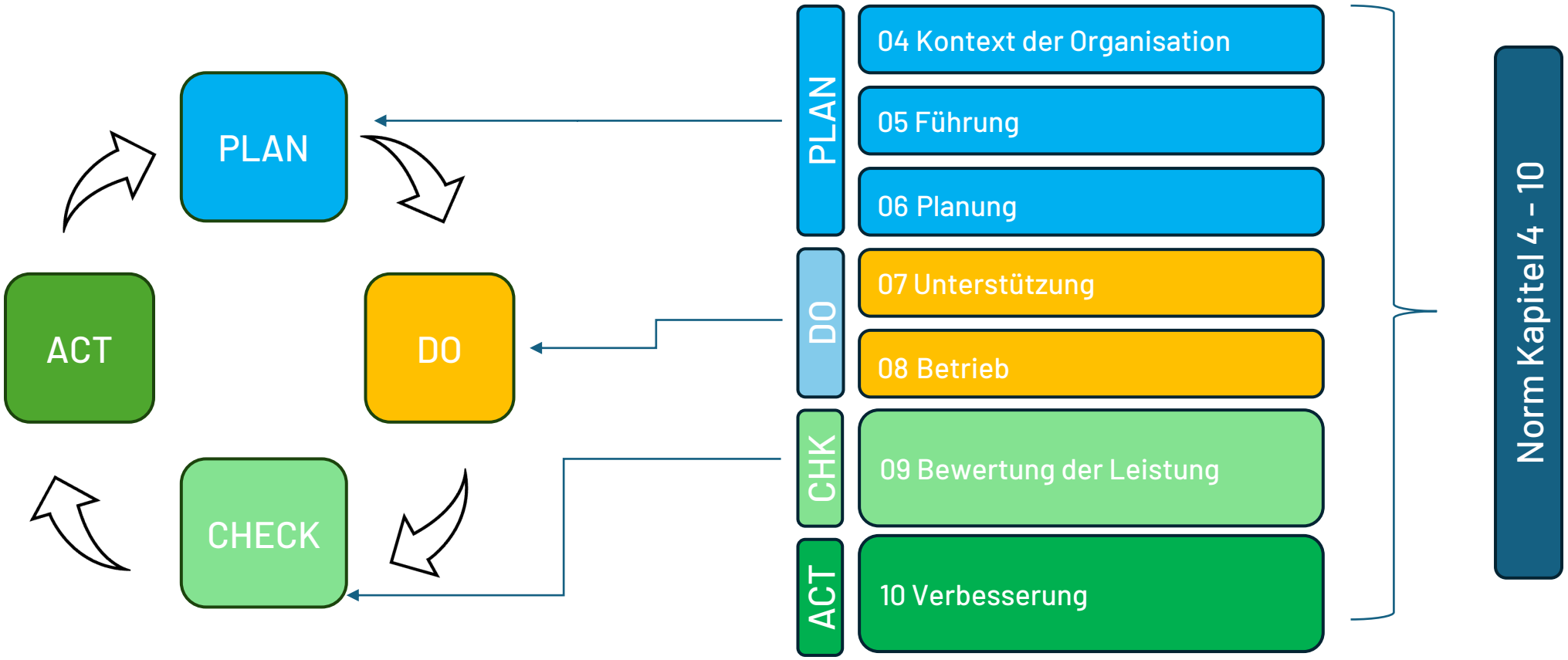
Da die Maßnahmen der NIS2 Richtlinie vom Annex A der ISO/IEC 27001 abgeleitet wurden, macht es Sinn bei der Umsetzung auch die Zertifizierung nach ISO/IEC 27001 anzudenken.

CertMe

Mit uns sicher zertifiziert.

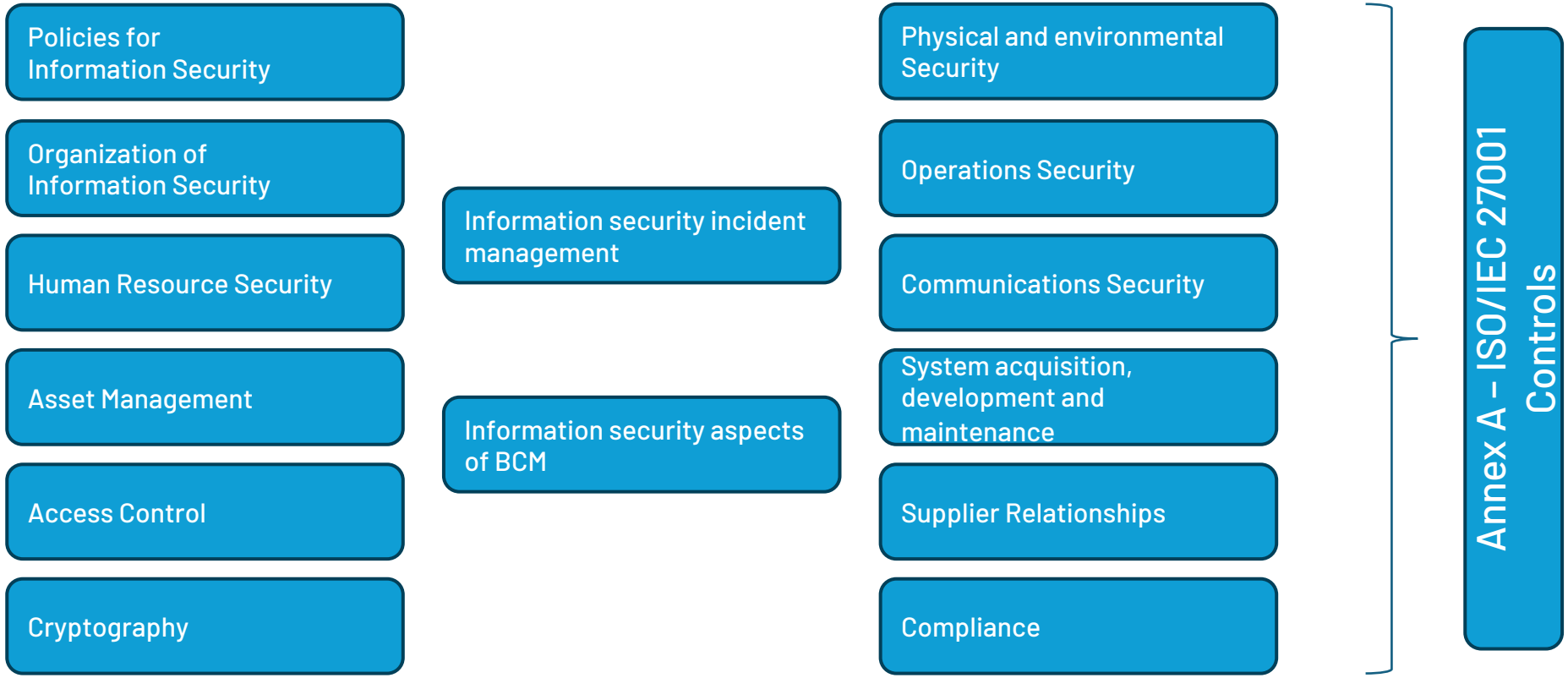
Cert Me
Mit uns sicher zertifiziert.

Bestandteile der ISO/IEC 27001



CertMe
Mit uns sicher zertifiziert.

Bestandteile der ISO/IEC 27001



CertMe
Mit uns sicher zertifiziert.

Maßnahmenkatalog NIS2

- Risikoanalyse und Sicherheit für IT-Systeme
- Konzept zur Bewältigung von Sicherheitsvorfällen
- Business Continuity und Krisenmanagement
- Sicherheit in der Lieferkette
- Sicherheitsmaßnahmen Erwerb/Wartung von IKT
- Schulungen zur Cybersicherheit
- Kryptografie
- Sicherheit bei Personal, Zutritts-/Zugriffskontrolle
- Multifaktor Authentifizierungen
- Konzept/Verfahren zur Bewertung d. Wirksamkeit des Riskmanagements

} Kernelemente NIS2

Dabei sind folgende Aspekte zu berücksichtigen:

- Der Stand der Technik
- EU und internationale Normen
- Kosten der Umsetzung
- Bestehendes Risiko

Bei der Bewertung der Verhältnis-mäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen.

Nutzen & Beweggründe

NIS2 steht für Netzwerk- und Informationssicherheitsrichtlinie 2 und hat, wie die ISO/IEC 27001 als Ziel jegliche Informationen des Unternehmens gegen interne und externe Bedrohungen und unerlaubte Zugriff zu schützen. Das umfasst ua.

- Prozessmanagement
- klare Rollenverteilung und Verantwortlichkeiten
- Robustes Risikomanagement
- Business Continuity Management (BCM)
- Sicherheit in der Lieferkette

CertMe

Mit uns sicher zertifiziert.

Nutzen & Beweggründe

Der reale Nutzen für das Unternehmen einer Zertifizierung nach ISO/IEC 27001 & NIS2 und ihre Stakeholder bestehen aus:

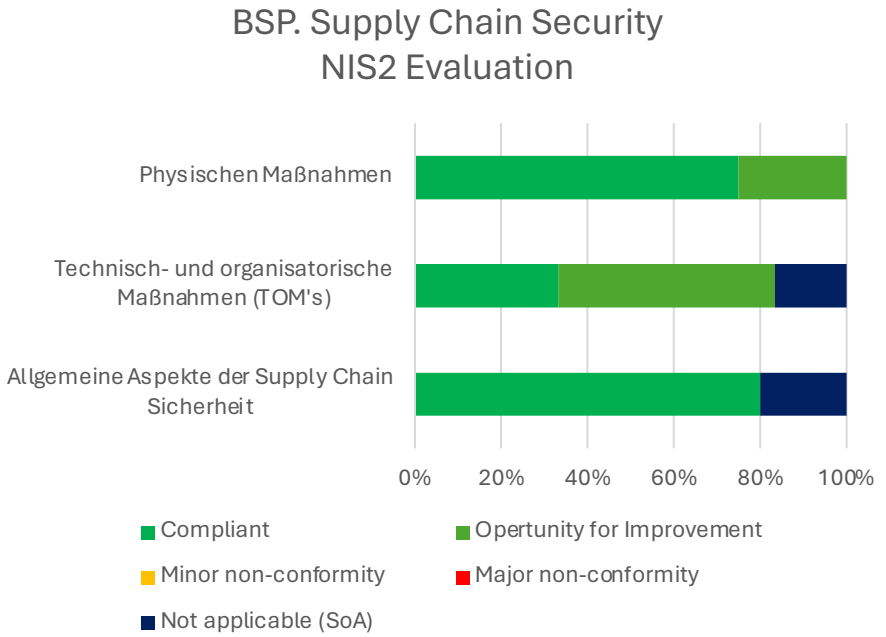
- ✓ Schutz kritischer Infrastrukturen
- ✓ Förderung der Zusammenarbeit
- ✓ Meldepflicht für informationssicherheitsrelevante Vorfälle
- ✓ Mindestsicherheitsanforderungen
- ✓ Robustes Risikomanagement
- ✓ Stärkung der Resilienz
- ✓ Anpassung an den technologischen Fortschritt
- ✓ Versicherbarkeit gegen Cyberrisiken (ISO/IEC 27001)

CertMe

Mit uns sicher zertifiziert.

Lieferkettensicherheit nach NIS2

Die EU NIS2 Richtlinie sieht, ebenso wie die ISO/IEC 27001, explizit vor, das Organisationen die Sicherheit -technisch und organisatorisch- der Lieferkette, regelmäßig überprüfen und die Nachweise darüber wie folgt protokollieren:



- ✓ Von NIS2 betroffene Einrichtungen müssen die Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern beachten.

- ✓ Sie müssen die spezifischen Schwachstellen der einzelnen unmittelbaren (Dienste-)Anbieter sowie die Gesamtqualität der Produkte und der Cybersicherheitspraxis ihrer Anbieter und Diensteanbieter, einschließlich der Sicherheit ihrer Entwicklungsprozesse, berücksichtigen

CertMe

Mit uns sicher zertifiziert.

Es beginnt mit dem Commitment ...

... der sogenannten „obersten Leitung“ (Geschäftsführung, Vorstand, Aufsichtsrat ...) welcher hierbei besondere Bedeutung zukommt.

Es liegt in Ihrer, sowie in der Verantwortung jeder operativen Führungskraft, innerhalb des jeweiligen Wirkungsbereiches die Umsetzung der NIS2 Richtlinie zu gewährleisten.

Im Zuge dessen ist es notwendig, dass gewisse Schlüsselpositionen innerhalb der Organisation besetzt werden, um die Wirksamkeit der Umsetzung der Richtlinie sowie der ISO/IEC 27001 zu gewährleisten ...

CertMe

Mit uns sicher zertifiziert.

Es beginnt mit dem Commitment ...

... und somit die Organisation bestmöglich, wirksam und nachhaltig vor bestehenden und zukünftigen Cyber- und Informationssicherheitsrisiken zu schützen.

Zum Wohle der Organisation aber auch um Ihre persönliche und uneingeschränkte Haftung als oberste Leitung und operative Führungskraft -die in der Richtlinie vorgesehen ist- zu vermeiden.

CertMe

Mit uns sicher zertifiziert.

ISO27001 & NIS2 sind KEINE reinen IT-Projekte

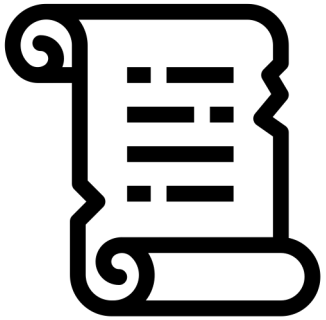
Die EU NIS2 Richtlinie verfolgt einen ganzheitlichen Ansatz beim Schutz kritischer Infrastrukturen ...

Nicht nur die technischen Schnittstellen sind im Scope der EU NIS2 Richtlinie relevant, sondern auch alle organisatorischen Schnittstellen wie zB.

- ✓ die Abholung von Unterlagen zwecks Vernichtung durch die Firma Reisswolf,
- ✓ Sichere Verfahren zur Anlieferung von Produkten, Komponenten oder auch externen Dienstleistungen ...

CertMe

Mit uns sicher zertifiziert.



Grundbegriffe

Informationen müssen nicht zwangsläufig elektronisch sein, sondern können auch (Hier einige Beispiele):

- ✓ Wissen
- ✓ Sprache
- ✓ Daten
- ✓ Unterlagen

sein.

CertMe
Mit uns sicher zertifiziert.

Der Chief Information Security Officer

CertMe

Mit uns sicher zertifiziert.

- ✓ Gesamtverantwortung für die Informationssicherheit in Unternehmen und benötigen daher einen ganzheitlichen Blick,
- ✓ Etablierung eines Managementsystems zur Informationssicherheit (ISMS – Information Security Management System),
- ✓ Erarbeitung von Schutzzielen für die unternehmenskritischen Werte (Assets), deren Bedrohungen und ihren Risiken,
- ✓ Durchführung von Risikoassessments und Business Impact Analysen,
- ✓ Ausarbeitung, Anpassung, Etablierung und Überprüfung von Sicherheitsrichtlinien und Sicherheitsvorgaben (Reifegradprüfung),
- ✓ Bewusstsein der Mitarbeiter für Informationssicherheit durch Trainings, Kampagnen (Awareness) und Schulungen schaffen,
- ✓ Kontinuierliche Analyse und Optimierung der Informationssicherheit im Unternehmen.

Der Chief Information Security Officer (CISO)

- ✓ Strategisch ist der CISO entweder Mitglied der obersten Leitung (zB. Vorstand, Geschäftsführung ...) oder aber organisatorisch unmittelbar darunter angesiedelt.
- ✓ Er berichtet ausschließlich der obersten Leitung ist auch nur dieser gegenüber weisungpflichtig.
- ✓ Er besitzt aber ein Weisungsrecht in Belangen der Informationssicherheit gegenüber allen Organisationseinheiten innerhalb des Unternehmens.

CertMe

Mit uns sicher zertifiziert.

CertMe
Mit uns sicher zertifiziert.

Berichtspflichten gemäß EU NIS2

Bei erheblichen Cybersicherheitsvorfällen gibt es ein vierstufiges Meldeverfahren an das zuständige CSIRT

(Cybersecurity Incident Response Team).

FRISTEN

Unverzüglich, innerhalb von 24 Stunden: Frühwarnung (ggf. Verdacht auf rechtswidrige und schuldhafte Handlung oder grenzüberschreitende Auswirkungen)	Unverzüglich, jedenfalls innerhalb von 72 Stunden: Meldung (Schweregrad, Auswirkungen, ggf. Komprimittierungsindikatoren)	Unverzüglich, jedenfalls innerhalb von 72 Stunden: Meldung (Schweregrad, Auswirkungen, ggf. Komprimittierungsindikatoren)	Spätestens einen Monat nach Frühwarnung: Abschlussbericht (Beschreibung Vorfall, einschließlich Schweregrad und Auswirkungen, Art der Bedrohung, Ursachen, Abhilfemaßnahmen)

Auf Ersuchen des CSIRT oder der Behörde sind Zwischenberichte über Statusaktualisierungen zu übermitteln.

Cert Me

Mit uns sicher zertifiziert.

Was passiert, Wenn‘s passiert ist ?

Was passiert, Wenn‘s passiert und Unternehmen die Regelungen und gesetzlichen Vorgaben nicht einhalten?

- Bei Nichterfüllung –wesentliche Einrichtungen im Sinne der Richtlinie- drohen Sanktionen bis zu 10 Mio. Euro oder 2 % des Gesamtjahresumsatzes des Konzerns

- bei wichtigen Einrichtungen bzw. 7 Mio. Euro oder 1,4 % des Gesamtjahresumsatzes des Konzerns bei wichtigen Einrichtungen.

Leitungsorgane wie zB. Geschäftsführer, Vorstände, operativ tätige Führungskräfte haften –uneingeschränkt mit dem Privatvermögen- für Verstöße, wenn essenzielle Risikoabwägungen vernachlässigt oder ignoriert wurden

CertMe

Mit uns sicher zertifiziert.

Das Management Review als strategisches Instrument

Das Management Review ist mehr als eine Normvorgabe der ISO 27001.

Es bildet eine fundierte Entscheidungsgrundlage für die Geschäftsleitung, um zielgerichtete Investitionen in die Widerstandsfähigkeit des Unternehmens gegen Cybervorfälle zu tätigen, und somit in die unternehmerische Zukunft zu investieren.

Nur der gezielte, gemeinsame Einsatz von finanziellen, personellen und technischen Ressourcen steigert die Effizienz und bringt echte Mehrwerte mit sich.

Der Klimawandel macht auch vor Normen nicht halt

CertMe

Mit uns sicher zertifiziert.

Dem globalen Wandel geschuldet, rücken auch nicht technische oder organisatorische Maßnahmen in den Fokus der Norm ISO 27001.

Durch die am 22. Februar 2024 verabschiedete Änderung, wurde der Organisationskontext um den Klimawandel erweitert.

Ab sofort müssen sich Unternehmen hierzu Gedanken machen, ob sie oder für die Organisation relevante, interessierte Parteien, die Stakeholder von den Auswirkungen des Klimawandels betroffen sind.

Schlusswort

Der Weg hin zur Compliance & Zertifizierung als Seilschaft auf dem Weg zur Informations- und Cybersicherheit.

Dipl.-Ing. Mag. Eduard Senn, MBA
zertifizierter Lead Auditor nach ISO/IEC 27001 u. NISG

CertMe GmbH
Heiligenstädter Lände 29/OG.2, 1190 Wien
Tel. +43 664 149 01 99
@. hello@certme.at

CertMe

Mit uns sicher zertifiziert.