Verfügbarkeit, Integrität und Vertraulichkeit - Grundschutz und ISO 27001

EU-DSGVO Konformität durch Data Protection & Network Monitoring

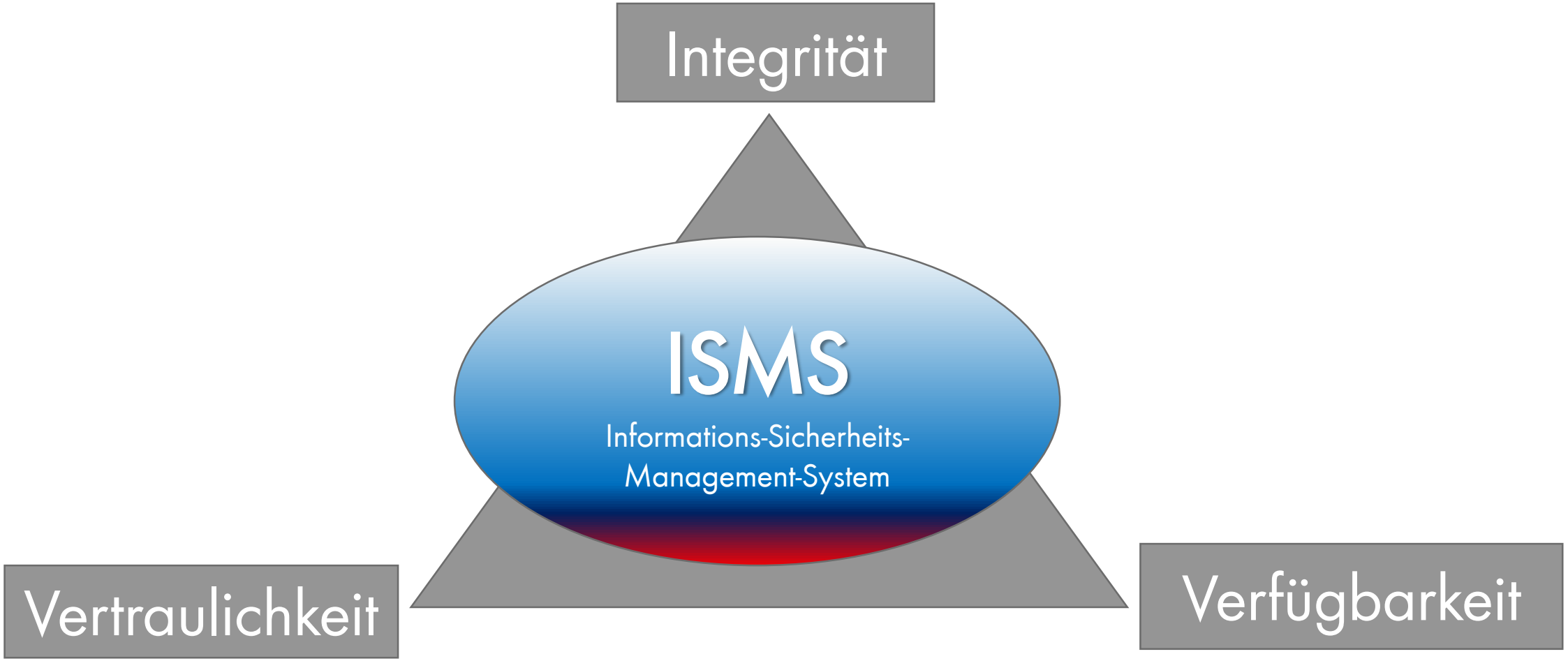
Agenda

- Grundlagen der Informationssicherheit: *Verfügbarkeit*, *Integrität* und *Vertraulichkeit*
- Regelwerke und Zertifizierungen: Grundschutz und ISO 27001
- Die (neuen) Anforderungen durch die EU-DSGVO
- So werden Sie DSGVO Compliant

ISMS

Grundlagen der Informationssicherheit

Grundlagen der Informationssicherheit

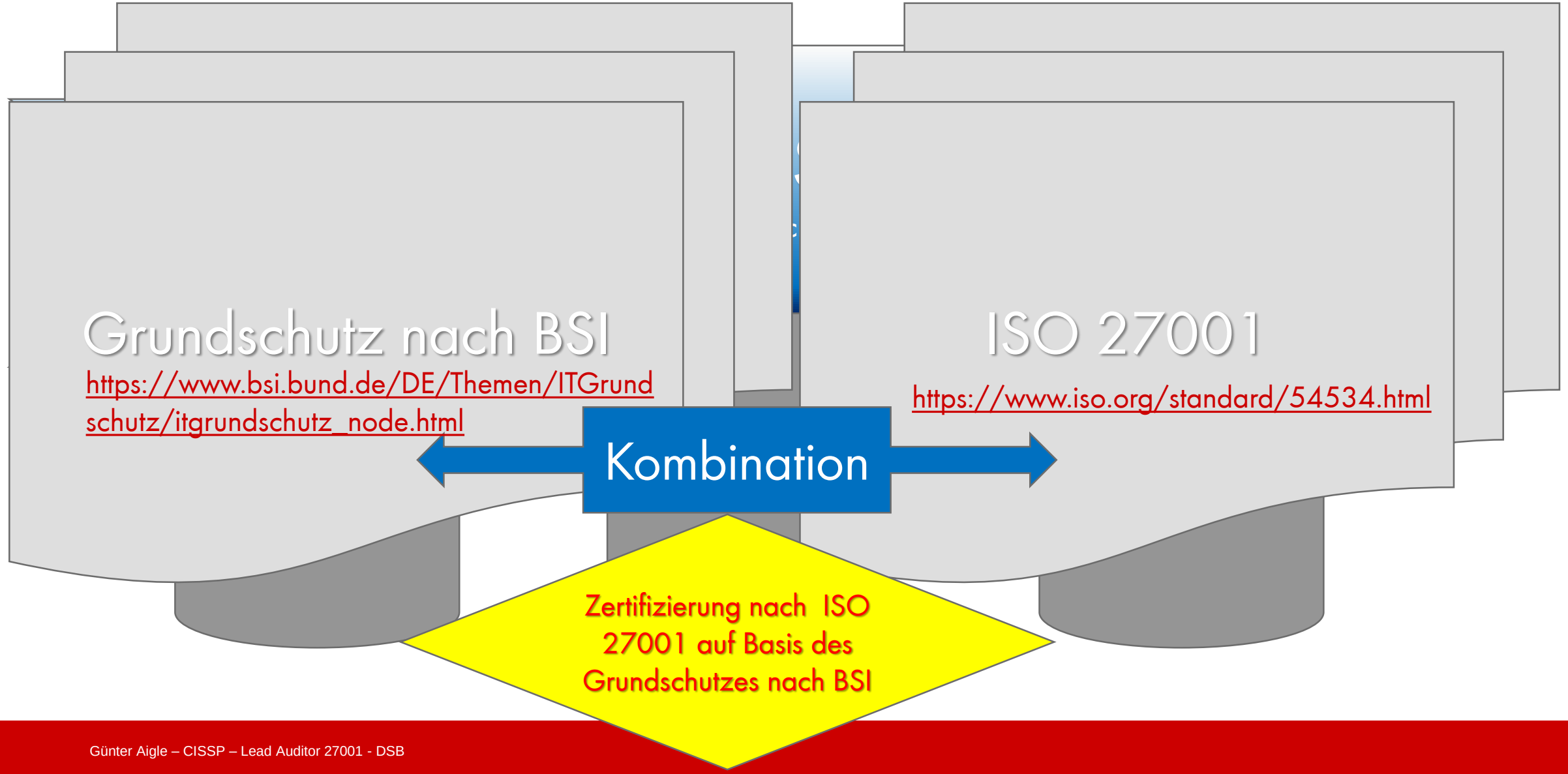


ISMS
Informationssicherheitsmanagementsystem

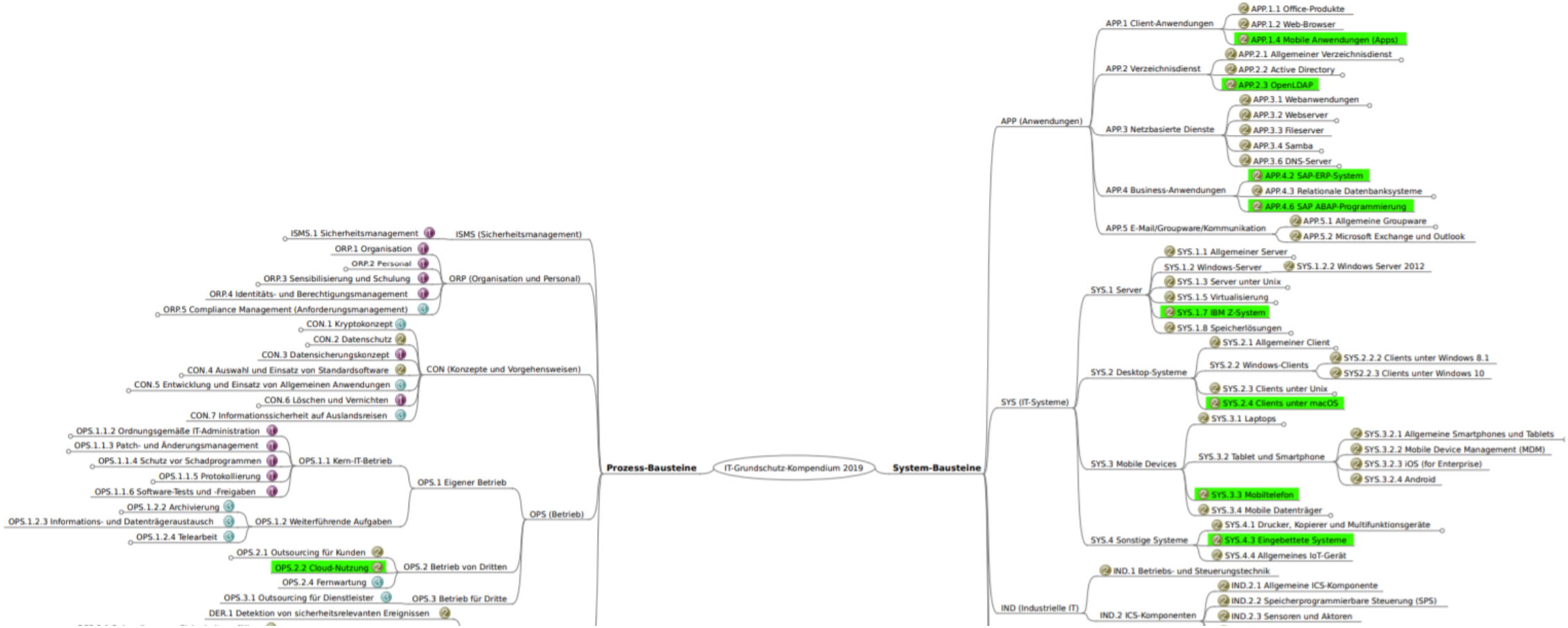
BSI Grundschutz –versus ISO27001

ISMS nach BSI und ISO 27001

Hilfsmittel für die Erstellung eines ISMS



IT-Grundschutz-Kompendium 2019 | 2. Edition



https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Struktur_2019.pdf?__blob=publicationFile&v=11

WÜRTH | IT

Anhang A der ISO 27001

Anhang A
(normativ)

Referenzmaßnahmenziele und -maßnahmen

Die in Tabelle A.1 aufgeführten Maßnahmenziele und Maßnahmen sind aus denjenigen, die in ISO/IEC 27002, Abschnitte 5 bis 18, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit Abschnitt 6.1.3 angewendet werden.

Tabelle A.1 – Maßnahmenziele und Maßnahmen

A.5 Informationssicherheitsrichtlinien		
A.5.1 Vorgaben der Leitung für Informationssicherheit Ziel: Vorgaben und Unterstützung für die Informationssicherheit sind seitens der Leitung in Übereinstimmung mit geschäftlichen Anforderungen und den relevanten Gesetzen und Vorschriften bereitgestellt.		
A.5.1.1	Informationssicherheitsrichtlinien	*Maßnahme* Ein Satz Informationssicherheitsrichtlinien ist festgelegt, von der Leitung genehmigt, herausgegeben und den Beschäftigten sowie relevanten externen Parteien bekanntgemacht.
A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien	*Maßnahme* Die Informationssicherheitsrichtlinien werden in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.
A.6 Organisation der Informationssicherheit		
A.6.1 Interne Organisation Ziel: Ein Rahmenwerk für die Leitung, mit dem die Umsetzung der Informationssicherheit in der Organisation eingeleitet und gesteuert werden kann, ist eingerichtet.		
A.6.1.1	Informationssicherheitsrollen und -verantwortlichkeiten	*Maßnahme* Alle Informationssicherheitsverantwortlichkeiten sind festgelegt und zugeordnet.
A.6.1.2	Aufgabentrennung	*Maßnahme* Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche sind getrennt, um die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der Werte der Organisation zu reduzieren.
A.6.1.3	Kontakt mit Behörden	*Maßnahme* Angemessene Kontakte mit relevanten Behörden werden gepflegt.

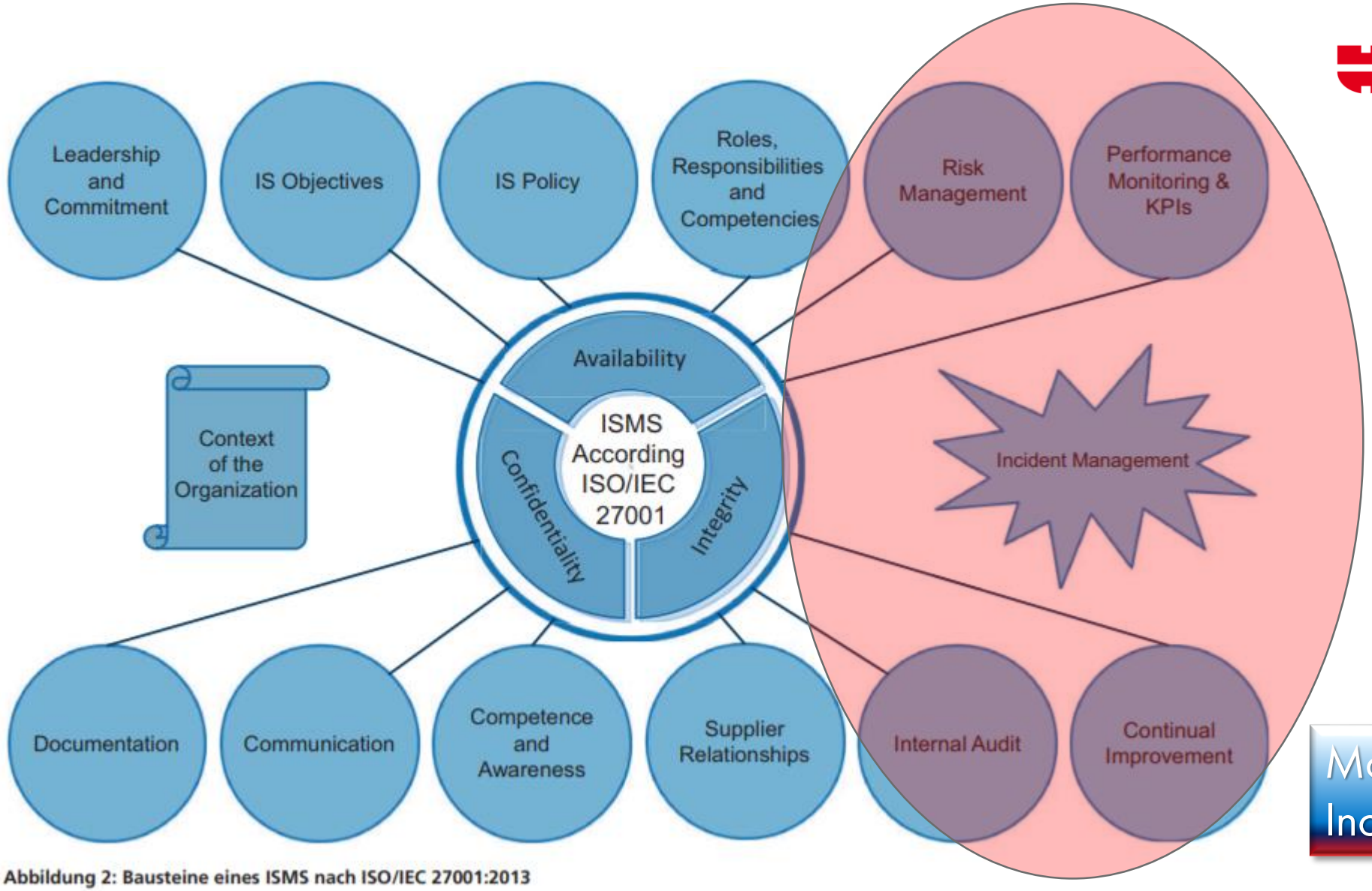


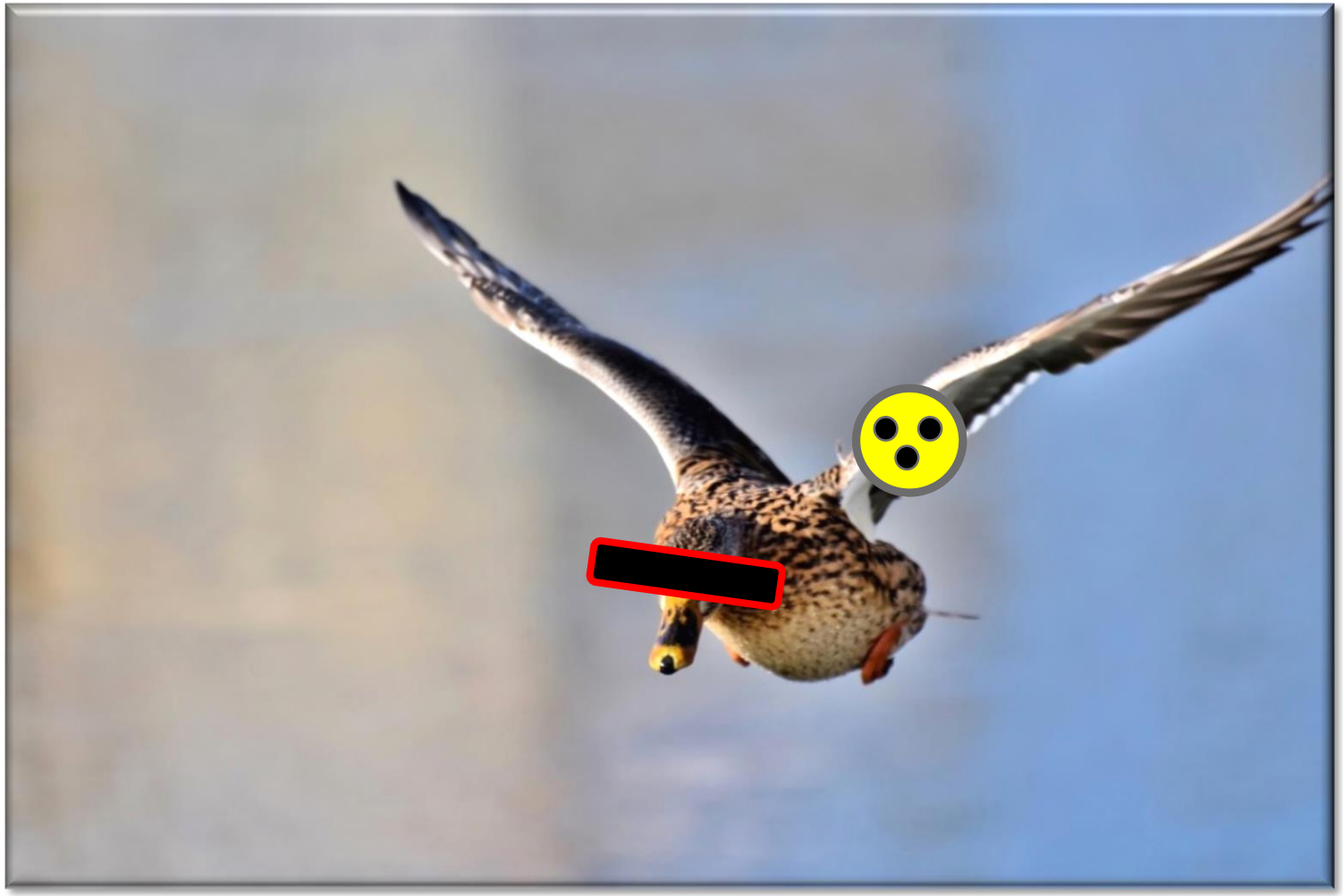
Abbildung 2: Bausteine eines ISMS nach ISO/IEC 27001:2013

Monitoring
Incident Management

https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_i_gesamt_web.pdf

Die zwei größten Herausforderungen

Die beiden größten Herausforderung für Firmen: fehlendes Netzwerk Monitoring und nicht vorhandene Datenklassifizierung und dem daraus resultierenden Unvermögen zu bestimmen, wo welche Daten liegen!

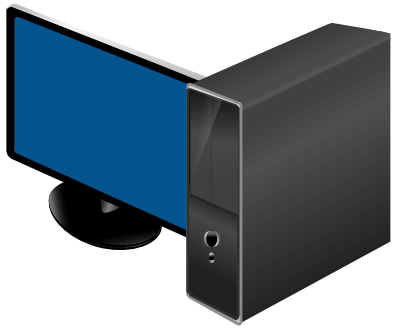


Im Blindflug durch das Netzwerk... „wir haben doch eine Firewall, die schützt uns doch, oder?“

Was geschieht in meinem Netzwerk?

- Was passiert auf meiner Firewall? Werden wir angegriffen? Wer liest die FW-Logs?
- Was geschieht in meinem Netzwerk? Haben wir ungewöhnlichen Datenverkehr, z.B. nach China? Oder in den Nachtstunden?
- Wie viele Geräte sind in meinem Netzwerk? Wem gehören diese und vor allem: was machen die denn so?
- Was geschieht auf meinen Servern? Vorhandene Eventlogs sollten sinnvollerweise auch mal ausgewertet werden!
- Wer sind die „Bandbreiten-Fresser“?

„Wo sind meine Daten?“



Server

„Wo sind meine Daten?“

Ich kann nur Schützen, was ich kenne!

- Richtlinien und Policies: nur wenn ich Regeln habe, kann ich die Einhaltung dieser auch verlangen!
- „Wo sind die Kronjuwelen?“ – Beim Verlust welcher Daten machen wir morgen zu?
- Datenklassifizierung: „Öffentlich“ – „Intern“ – „Geheim / Sensitiv“
- Wer hat Zugang zu den Kronjuwelen? -> wer greift darauf zu? Wie wird darauf zugegriffen?
- Überwachung durch Monitoring

EU-DSGVO

Die besondere Herausforderung durch die DSGVO – Einhaltung der TOM´s

Anforderungen durch die DSGVO

Artikel 5 (1) (f)
„Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“)

Artikel 5 (2)
„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

TOM´s

Aber wie?

TOM´s

Artikel 32 (1) (b)
„(…) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;“

Artikel 25 (2)
„Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“

Die DSGVO ist voller Anforderungen an eine „funktionierende“ IT

Artikel 32 (1) (d)
„(…) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.“

Sanktionen

Art. 83 DSGVO Allgemeine Bedingungen für die Verhängung von Geldbußen

...

d)

Grad der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters unter Berücksichtigung der von ihnen gemäß den Artikeln 25 und 32 getroffenen technischen und organisatorischen Maßnahmen;

...

Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu **10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs** verhängt, je nachdem, welcher der Beträge höher ist:die Pflichten der Verantwortlichen und der Auftragsverarbeiter gemäß den Artikeln 8, 11, 25 bis 39, 42 und 43;

So werden Sie Compliant:

- Etablierung der notwendigen Prozesse -> Aufbau eines ISMS
- „Nehmen Sie die Augenbinde ab!“ -> kein Blindflug im Netzwerk
- Setzen Sie Monitoring ein -> Setzen Sie auf eine „Unified Monitoring“ Lösung
- Sorgen Sie für ein SIEM (security information and event management) -> damit Vorfälle nicht „unbearbeitet“ bleiben

Zukunft(s)Aussichten

Unternehmen, welche sich heute nicht mit den Themen Informationsmanagement , IT Sicherheit und Monitoring beschäftigen, werden morgen nicht mehr existieren...

Günter Aigle
IT-Sicherheitsexperte

THANK YOU FOR YOUR ATTENTION

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT

MUCHAS GRACIAS POR SU ATENCIÓN