secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

SBA Research
ISO 27001 Vorbereitung
Theorie und Wirklichkeit

19.09.2013

secure
sba-research.org

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfj
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

Agenda

- Treiber einer ISO27001 Zertifizierung
- Grundlegende Rahmenbedingungen
- Herausforderung an die Organisation

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

ISO27001 Treiber

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfi
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

secure
sba-research.org

ISO27001 Treiber

- Externe Treiber
  - Kunden fordern Zertifizierung
  - Wettbewerbsvorteil
  - Nachweisbarkeit
- Interne Treiber
  - … ? … abgesehen von einem gravierenden Vorfall >> *externe Treiber*

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

ISO 27001

Grundlegende Rahmenbedingungen

ISMS

Ein Informationssicherheitsmanagementsystem (ISMS)…

„… ist der Teil des gesamten Managementsystems, der auf der Basis eines ***Geschäftsrisikoansatzes*** *die* ***Errichtung, die Umsetzung, den Betrieb, die Überwachung, die Überprüfung, die Instandhaltung und die Verbesserung der Informationssicherheit*** *abdeckt.“*

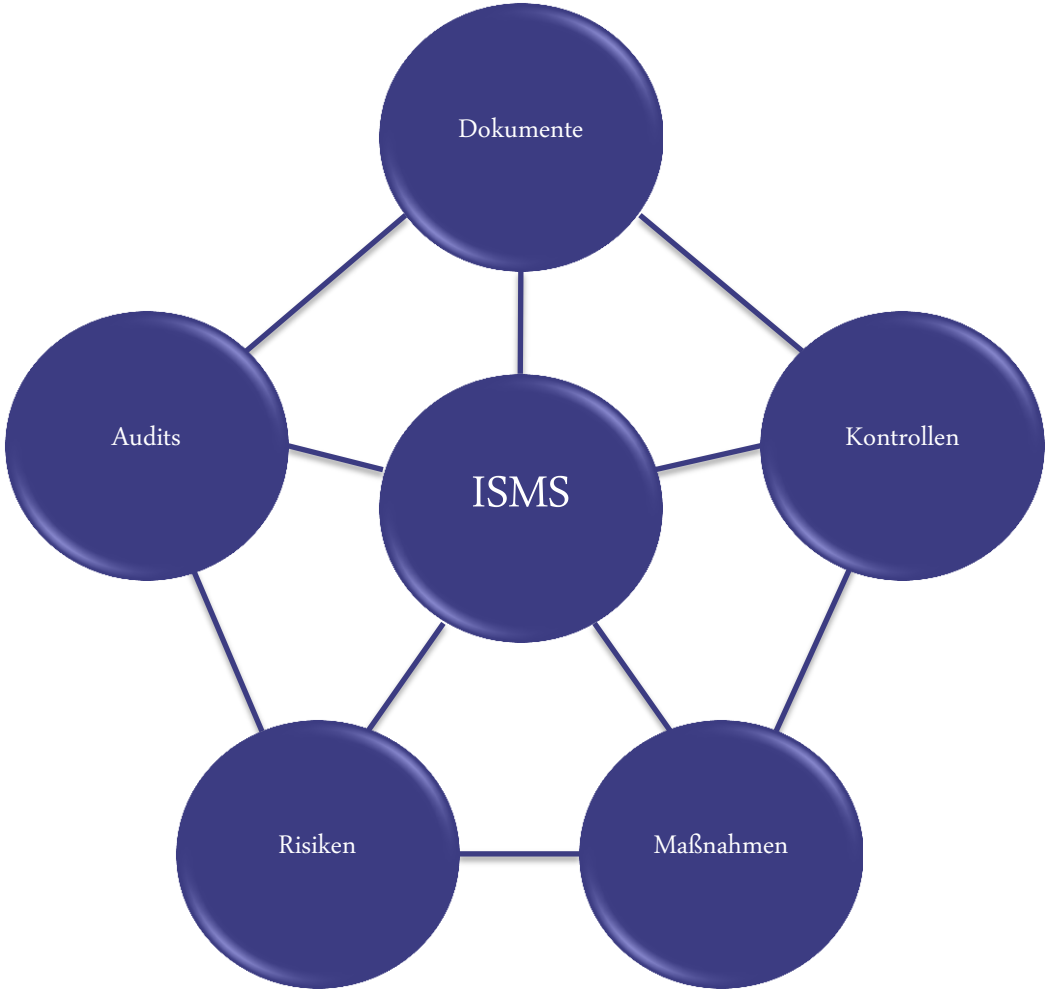
>> ISO27001 zertifiziert dieses ISMS

ISMS

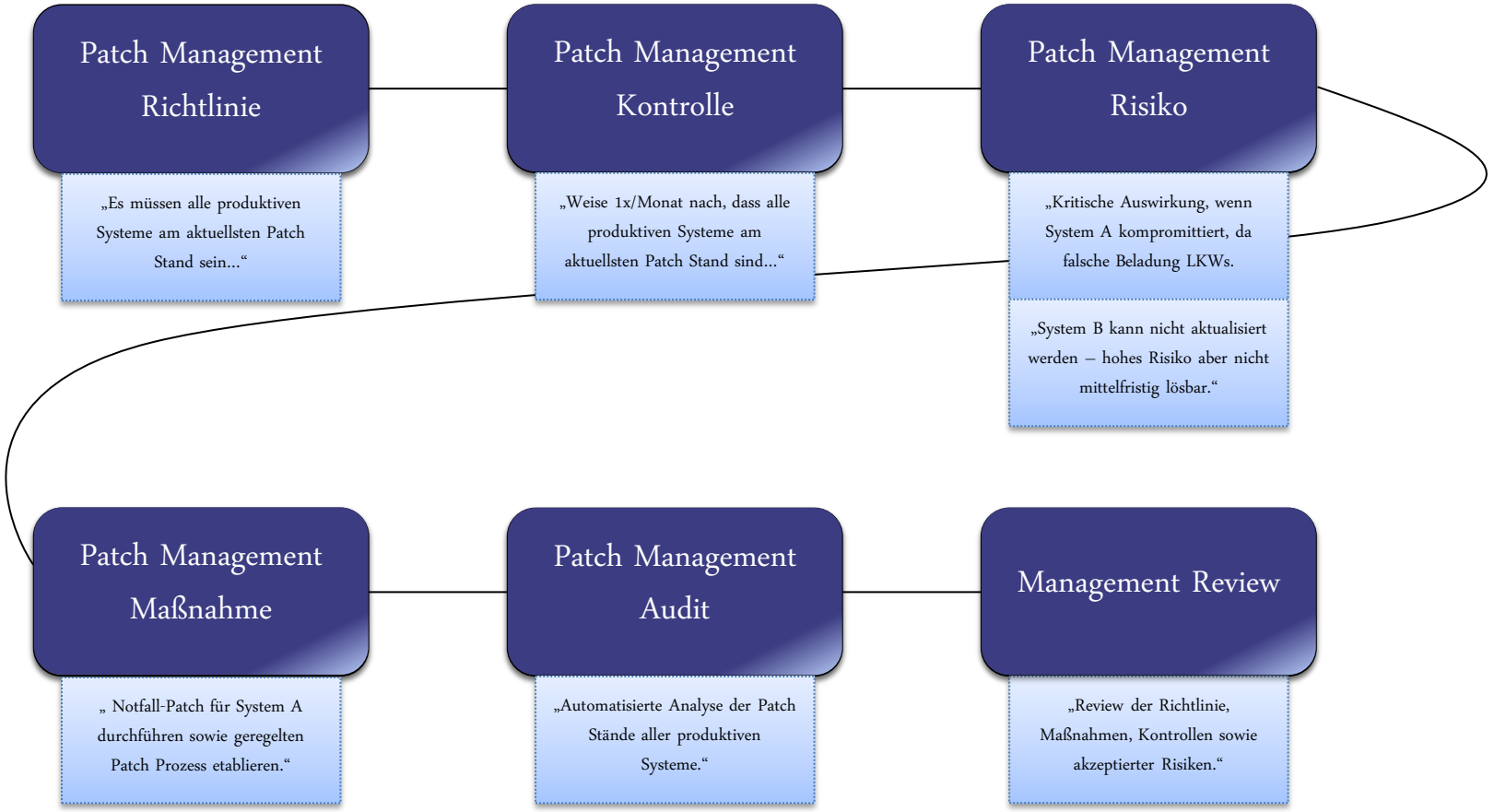
Phase	Beschreibung
Plan *ISMS einrichten*	Einführen einer ISMS Policy, von Zielen, Prozessen und Prozeduren, die für das Management von Risiken und die Verbesserung der Informationssicherheit relevant sind sowie Ergebnisse liefern, die in Einklang mit den Unternehmensvorgaben und –Zielen stehen
Do *ISMS implementieren*	Konkrete **Umsetzung und Betrieb der ISMS Policy, Kontrollen, Prozesse und Prozeduren**.
Check *ISMS überwachen*	Bewertung und (wo möglich) Messung der Prozess-Performance auf Basis der ISMS Policy, Zielen und praktischen Erfahrungen. Die Ergebnisse werden dem Management für ein Review vorgelegt.
Act *ISMS warten und verbessern*	Korrektive und vorbeugende Aktionen auf der Basis der Ergebnisse interner ISMS Audits sowie dem Management Review, um eine kontinuierliche Verbesserung des ISMS zu erreichen.

Quelle: ISO/IEC 27001:2005

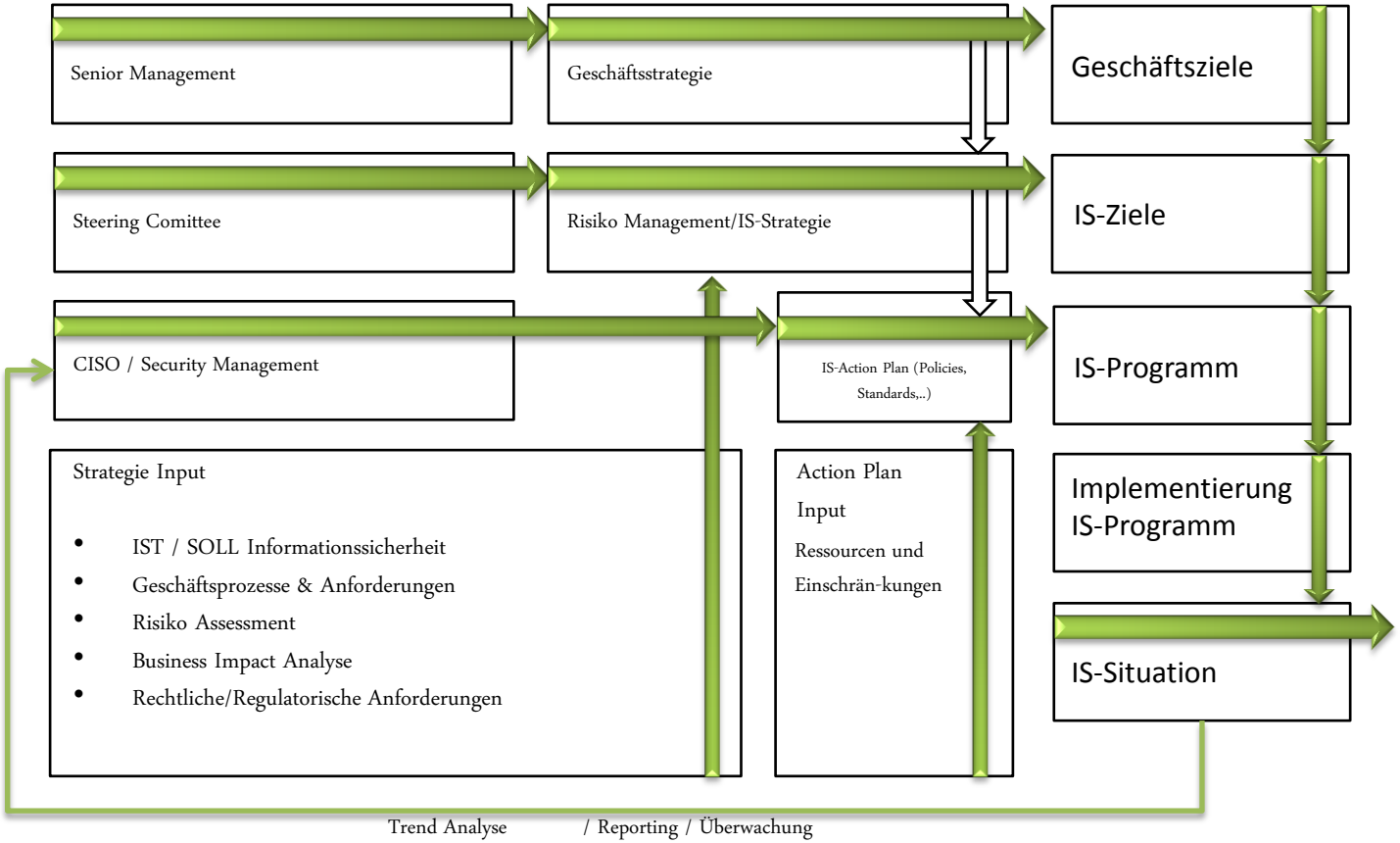
ISMS
Wesentliche Bausteine



ISMS
Wesentliche Bausteine



ISMS
IS Organisation



STOP – ein Schritt zurück!

- ✓ Vorherige Folien dürften bekannt sein
- ✓ Vorherige Folien klingen schlüssig & sinnvoll

- ➢ Ist das ein Unternehmensziel?
- ➢ Kennt das Unternehmen seine Ziele punkto Informationssicherheit
  - ➢ … präziser als „höchstmögliche Vertraulichkeit, Integrität und Verfügbarkeit“?
- ➢ Bewusstsein über Implikationen?

Was ist überhaupt das Ziel?

Stufe 3: Informationssicherheitsmanagementsystem (ISMS)

- Alle Managementprozesse sind definiert, dokumentiert, gesteuert, nachvollziehbar und kontrolliert (Reifegrad 3+)
- Alle Managementprozesse sind aufeinander abgestimmt
- Nachweisbares internes Kontrollsystem sowie etablierter kontinuierlicher Verbesserungsprozess
- Security Awareness, Education & Training (SEAT) Konzept
- Regelmäßige interne & externe Qualitätssicherung – Audit Konzept

Stufe 2: Sicherheitsmanagement

- Sicherheitspolitik & Strategie
- Etablierte Informationssicherheits-Organisation
- Wesentliche Managementprozesse sind definiert, dokumentiert und umgesetzt (Reifegrad 2+)
- Risikoorientierte Vorgehensweise = Wissen über den Schutzbedarf wertschöpfender Prozesse sowie eine differenzierte Vorgehensweisen je Schutzbedarf
- Punktuelle Security Awareness
- Regelmäßige interne & anlassbezogen externe Qualitätssicherung

Stufe 1: Sicherheitsbasis

- Keine unmittelbare Gefährdung wertschöpfender Unternehmensprozesse
- Beseitigen von Schwachstellen, die leicht von einem Angreifer ausgenutzt werden können
- Operative Tätigkeiten erfüllen ihren Zweck (Reifegrad 1+)

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

ISO27001

Herausforderungen an die Organisation

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfj
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

secure
sba-research.org

ISO27001 Herausforderungen

- Bewusstsein über Implikationen bzw. Umfang
  - Planung und schrittweise Verbesserung
- „Es menschelt“
  - Änderungen sollten nicht einfach verlangt werden sondern müssen begleitet werden
  - Forderungen des Unternehmens bei gleichzeitigem Verständnis (Awareness) der Mitarbeiterinnen und Mitarbeiter des Unternehmens
- Positionierung des Unternehmens
  - Klarstellung der Erwartungshaltung
  - Klare Definition von (nicht nur) Verantwortlichkeiten sondern auch Kompetenzen
  - Verständliche, sinnvolle & messbare Ziele

Verbesserung des Reifegrads

Reifegrad	Beschreibung / Leitfaden
NR	Der Prozess / das Kontrollziel sind nicht anwendbar (Begründung erforderlich).
0 – unvollständig	Der Prozess nicht implementiert oder verfehlt sein Ziel. Auf dieser Stufe gibt es kaum oder gar keine Hinweis auf eine systematische Erfüllung des Prozesszwecks.
1 – durchgeführt	Der Prozess ist ad-hoc, unorganisiert und abhängig vom Einsatz handelnder Personen. Grundlegend erfüllt der Prozess jedoch seinen Zweck.
2 – gemanagt	Der Prozess unterliegt einer strukturierten und wiederholbaren Vorgehensweise (Muster), um wesentlichen Risiken entgegenzusteuern. Der implementierte Prozess sowie dessen Arbeitsprodukte sind geplant, überwacht und abgestimmt, um die identifizierten Ziele zu erreichen.
3 – etabliert	Der Prozess ist definiert, dokumentiert und kommuniziert. Der implementierte Prozess basiert auf einem definierten und wirksamen (effektiven) Standardprozess. Der Standardprozess beinhaltet einen kontinuierlichen Feedbackzyklus für Prozessverbesserungen.
4 – vorhersehbar	Der Prozess ist überwacht, gemessen und voraussagbar. Ein voraussagbarer Prozess operiert innerhalb definierter Grenzen und ist auf Basis quantitativer Informationen gesteuert.
5 – optimierend	Der Prozess wird kontinuierlich verbessert, um relevante aktuelle und künftige Unternehmensziele zu erreichen.

Quelle: COBIT5

Implikationen?

- Die Erhöhung der Stufe bedeutet die **Steigerung des Reifegrades**
  - Schrittweise **Erhöhung des Sicherheits-Niveaus**
  - Schrittweiser Übergang **von rein reaktiv zu voraussehbar gesteuert**
  - Schrittweise **Steigerung der Nachvollziehbarkeit und Messbarkeit**
  - Schrittweise **Vereinfachung durch technologische Unterstützung**
  - Falls gewünscht, schrittweise **Annäherung an die ISO27001 Reife**

- Illusorische Vorstellung
  - Erhöhung der Stufe bzw. Steigerung des Reifegrads ohne zusätzliche Ressourcen
  - „…das geht schon noch nebenbei…“

Stufe 1
Sicherheitsbasis

- Beschränkter Zutritt zu bzw. Zugriff auf (kritischen) IT Systemen
- Kontrollierte Berechtigungsvergabe & starke Passwort Policy
- Netzwerkschutz (Firewall, VPN)
- Netzwerksegmentierung (zumindest DMZ, WLAN)
- Durchgängiges Anti-Virenkonzept
- Kontrolliertes Patch Management (Betriebssysteme, Applikationen)
- Backup Konzept
- Verschlüsselung Festplatten (Laptops)
- Service Level Agreements & Wartungsverträge für kritische Infrastruktur
- Dezidierte Zuweisung von Verantwortlichkeiten
- IT Personal mit aktuellem Security Know-How
- Verbindliche Endbenutzerrichtlinie

Stufe 2
Sicherheitsmanagement

- Etablierte Informationssicherheits-Organisation
  - Dezidierte Strategie, Informationssicherheitsverantwortlichkeit, regelmäßige Abstimmungen mit operativer IT, Fachbereichen und Geschäftsführung
- Risikoorientierte Vorgehensweise
  - Business Impact Analyse, Risiko Analyse, Maßnahmensteuerung, regelmäßige interne & anlassbezogene externe Qualitätssicherung
- Wesentliche Managementprozesse erfüllen Reifegrad 2+
  - Patch Management, Change Management, Vulnerability Management, Asset Management, Backup & Wiederherstellung, Incident Management, Notfallmanagement, Konfigurationen (Performance & Sicherheit/Hardening), Logging & Monitoring (Performance & Sicherheit), Dokumentation, Externe
- Review, Freigabe & Kontrolle
- Security Awareness Trainings
  - Umgang mit sensiblen Informationen, Anti-Viren Maßnahmen, Netzwerkzugriff
  - Dezidierter Schulungs- & Fortbildungsplan

Stufe 2
Sicherheitsmanagement

- Kein „Wildwuchs“ in der Infrastruktur
- Fortgeschrittener Netzwerkschutz
  - IDS/IPS
  - Vulnerability Scanner
  - Dedizierte Segmente für Clients, Server, Management
  - Kontrollierter Netzwerkzugriff (z.B.: 802.1x, NAC/NAP)
  - Remote Access Konzept (inkl. 2-Faktor Authentifizierung)
- Fortgeschrittenes Anti-Malwarekonzept
  - Mehrstufiges Konzept (Proxy, Mail, Clients/Server)
  - Kontrollierter Internetzugriff (URL Filter, SSL Inspection)
  - Application Management
- Fortgeschrittenes Datensicherheitskonzept
  - Verschlüsselung (Laptops, Workstations, Server, SmartX, mobile Datenträger)
  - Verschlüsselung Backup-Medien in Einklang mit Notfallkonzept
  - Berechtigungsvergabe (je nach Schutzklasse und Ablageort)
- Fortgeschrittene Management Tools
  - Vulnerability Management
  - Secure Configuration Management
- Sicherer Softwareentwicklungslebenszyklus (SDLC)

Stufe 3
ISMS

- Alle Managementprozesse erfüllen Reifegrad 3+
- Nachvollziehbares Management System
- Kontinuierlicher Verbesserungsprozess
  - Regelmäßige Überprüfung der Wirksamkeit des ISMS
  - Messung der Wirksamkeit der Maßnahmen
  - Regelmäßige Überprüfung/Anpassung der Risikobewertung und Berücksichtigung von eventuell geänderten Rahmenbedingungen
  - Durchführung interner ISMS Audits
  - Durchführen von Überprüfung des ISMS durch das Management
  - Aktualisierung von Sicherheitsplänen
  - Aufzeichnen von Ereignissen, die die Wirksamkeit des ISMS beeinflussen können
  - Umsetzung von identifizierten Verbesserungen
  - Anwendung von Korrektur- und Vorbeugemaßnahmen
- Business Continuity Management (System)

Stufe 3
ISMS

- Fortgeschrittener Netzwerkschutz
  - Web Application Firewall (WAF)
- Fortgeschrittenes Anti-Malwarekonzept
  - Advanced Persistant Threats (APT)
- Fortgeschrittenes Datensicherheitskonzept
  - Data Loss Prevention (DLP)
  - Information Rights Management (IRM)
  - Mobile Device Management (MDM)
- Fortgeschrittene Management Tools
  - Security Incident and Event Management (SIEM)
  - Identity & Access Management

Der/Die Informationssicherheitsverantwortliche

- Aufgedeckte Schwachstellen, Bedrohungen bzw. Risiken
- Maßnahmenstatus zur Risikobehandlung
- Laufende Kontrollen (Sicherstellung der Einhaltung der Security Mindeststandards)
- Qualitätssichernde Kontrollen
- Assets, die vom Standardkatalog abweichen
- Nicht-Umsetzung von State-of-the-Art Schutzmaßnahmen
- Geheimhaltungsvereinbarungen
- Verlust / Diebstahl von Assets
- Qualitätssicherung der Dokumentation (Fokus: Umsetzung der Mindeststandards und Einhaltung der IS Ziele) und Freigabe aus IS Sicht
- Freigabe von Projektanforderungen (vor Umsetzung) aus IS Sicht

Der/Die Informationssicherheitsverantwortliche

- Systeme ohne Testumgebung
- Systeme, die aus Geschäftsgründen, durchgängig verfügbar sein müssen
- Freigabe von Systemen, die vom Internet erreichbar sind
- Freigabe von Systemen, die keinem regelmäßigen (zumindest jährlichen) Sicherheitstest unterliegen
- Changes mit hoher Risikoeinschätzung (durch den System Owner)
- Notfall Changes
- Freigabe der Definition von pre-authorized Changes
- Vorfälle im Rahmen der Change Durchführung
- Audits

Der/Die Informationssicherheitsverantwortliche

- Freigabe von Accounts, die vom Standard abweichen
- Freigabe administrativer Accounts
- Freigabe permanenter Zutritt zu Rechenzentren
- Anomalien bei der Verwendung von Accounts
- Kündigung von Personal mit administrativen Accounts
- Security Incidents
- Freigabe der Risikobewertung aus IS Sicht von Projekten
- BCM Szenarien aus IS Sicht, die nicht getestet werden
- Freigabe von Assets, die nicht (laufend) aus IS Sicht gepatcht werden

Der/Die Informationssicherheitsverantwortliche

- Freigabe von Systemen, für die kein Backup durchgeführt wird
- Freigabe von Systemen, für die kein Wiederherstellungstest durchgeführt wird
- Nicht erfolgreiche Backups
- Nicht erfolgreiche Wiederherstellungstests
- Freigabe von Systemen, die keinem IS Monitoring unterliegen
- Freigabe von Systemen ohne Schutzmaßnahmen gegen schadhafte Software (z.B. Viren, Spam, etc.)
- Freigabe des Standardkatalogs mobiler Geräte
- Freigabe von mobilen Geräten, die vom Standardkatalog abweichen
- Anomalien im Netzwerkmanagement (vor allem Firewall, WAF, etc.)

secure
sba-research.org

COMET
Competence Centers for
Excellent Technologies

Zusammenfassung

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfi
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

Zusammenfassung

- ISO27001 Zertifizierung ist (sofern benötigt) absolut machbar
  - … wenn nicht als „nebenbei zum Tagesgeschäft“ angesehen
- ISO27001 Zertifizierung ist absolut sinnvoll
  - Verbesserung der Strukturiertheit, Nachvollziehbarkeit & Planbarkeit
  - „Von reaktiv zu proaktiv“
  - „Vom Bauchgefühl zu dokumentiertem Wissen“
- Informationssicherheitsverantwortliche ist „kein armes Schwein allein auf weiter Flur“
  - … so lange richtig vom Unternehmen eingesetzt

secure
sba-research.org

COMET

Competence Centers for
Excellent Technologies

Vielen Dank!

mklemen@sba-research.org

bmvit
Bundesministerium
für Verkehr,
Innovation und Technologie

bmwfi
Bundesministerium für
Wirtschaft, Familie und Jugend

Christian Doppler
Forschungsgesellschaft

FFG

wirtschafts
agentur
wien

zit
Die Technologieagentur
der Stadt Wien

secure
sba-research.org