TEMET
end-to-end IT security

Daniel Felix Maurer

ISMS im IT-Projektvorgehen -Wunsch und Wirklichkeit

Breakout-Session an der security-zone 2012

Inhalt

- Angaben zum Referenten / zur TEMET AG
- Einleitung (um was es geht…)
- ISMS nach ISO/IEC 27001 – Gliederung, Ziele
- «The Big Picture»
- Sicherheitsprozeduren im IT-Projektablauf
- Werkzeuge/Tools
- Beispiele aus der Praxis
- Zusammenfassung

Angaben zum Referenten:
Daniel Felix Maurer

- lic. phil. UZH, Informationssystem-Architekt
- 29 Jahre Tätigkeit in der IT
  - 14 Jahre Credit Suisse, u.a. Leitung der Fachstelle für technische Informatiksicherheit
  - 14 Jahre IT Security Consulting, u.a. Leitung eines Teams von 15 Beratern
- Mitglied der Geschäftsleitung und Partner TEMET AG (seit November 2011)
- Persönliche Schwerpunkte
  - IT-Sicherheitsarchitektur
  - Information Security Management Systems (ISMS)
  - Governance, Risk & Compliance
  - Kryptologie und Internet Sicherheit

Informationen zur TEMET AG

- Die Temet wurde 2010 von erfahrenen IT Security Experten mit Sitz in Zürich gegründet
- Die Temet bietet ausschliesslich hochwertige IT Security Beratung an, ihre Berater vereinen technische Expertise mit Management- und Projektleiter-Kompetenz
- Die Temet ist als unabhängige und herstellerneutrale Beratungsfirma nur ihren Kunden verpflichtet
- Bereits 20 renommierte Unternehmen vorab aus dem Finanzsektor und der öffentlichen Verwaltung vertrauen auf die Kompetenz der TEMET AG

Einleitung (um was es geht)

TEMET
end-to-end IT security

Systemanforderungen für die Informationssicherheit und Prozesse für die Implementierung von Sicherheit sollten Bestandteil der *frühen* Stadien von Projekten für Informationssysteme sein.

Maßnahmen, die bereits während der Entwurfsphase eingeführt werden, sind signifikant *preiswerter* zu implementieren und zu warten als während oder nach einer Implementierung eingebrachte Maßnahmen.

Auszug aus DIN ISO/IEC 27002:2008-09
Kapitel 12.1.1 «Analyse und Spezifikation von Sicherheitsanforderungen»

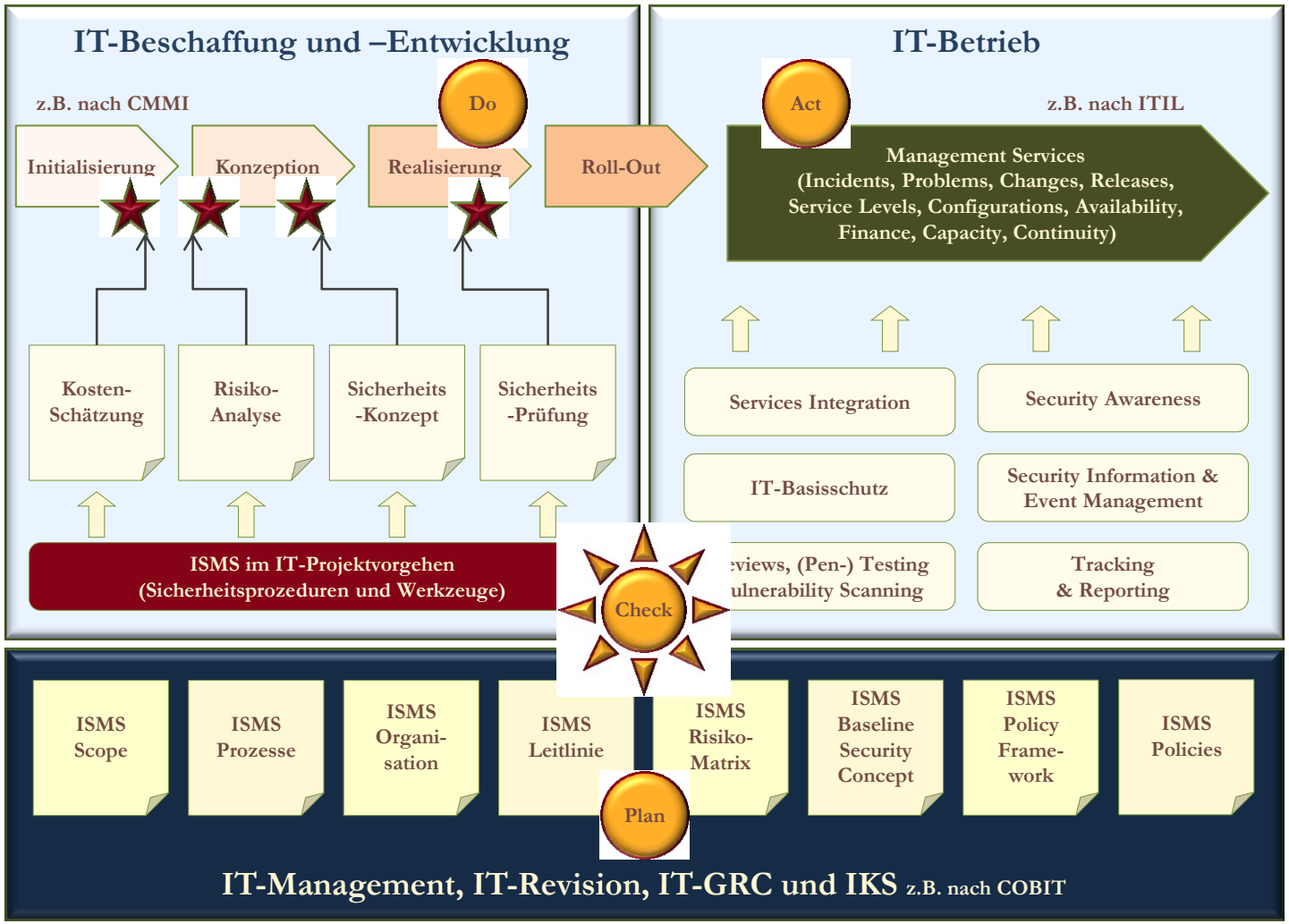
Ein ISMS nach ISO/IEC 27001 gliedert sich in…

- Scope & Geltungsbereich = Statement of Applicability *SoA*
- *Sicherheitsprozeduren* (Risk Treatment Plan, Kontinuierlicher Verbesserungsprozess (i.e. Non-Compliances Management), Internal Audit, Security Incident Handling, Management Review)
- *Sicherheitsorganisation* (inkl. AKV beteiligter Fachstellen z.B. CISO, IT-SiBe, physische Sicherheit, HR, Legal & Compliance, 3rd Party Provider)
- *Sicherheitsregulativ* (Top Policy, firmenweite Regelungen, IT Policies)

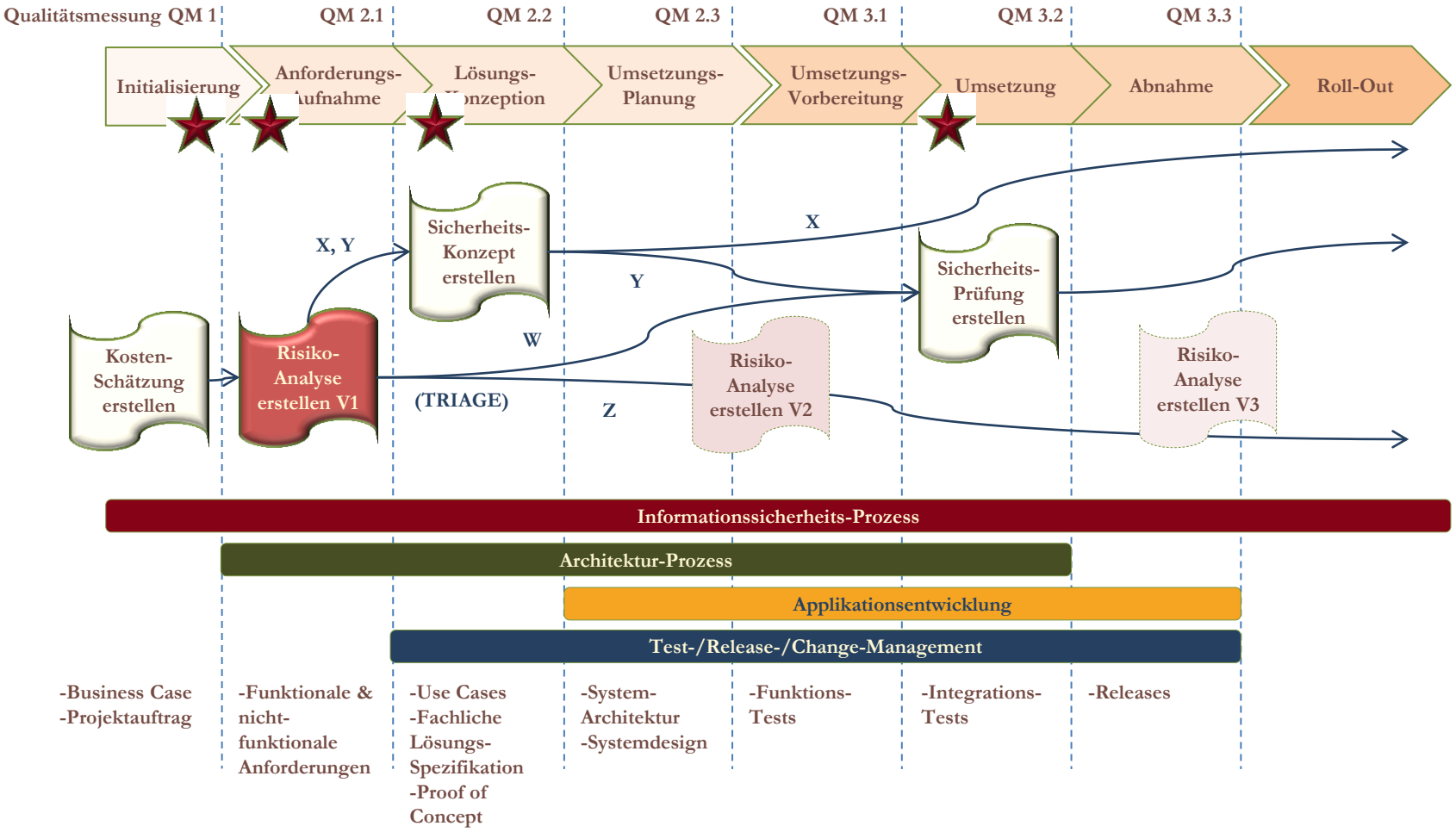
Ein ISMS (nach ISO/IEC 27001) bewirkt für die IT…

- Verbesserung des IT-Risikomanagements
  - macht die *Risiken* des Einsatzes von Informationstechnologie *bewusst* und *messbar* (und damit erst begrenzbar)
- Verringerung der Eintretenswahrscheinlichkeit von IT-Sicherheitsvorfällen
  - hilft Kosten *sparen*
- Planung und Überschaubarkeit für die Optimierung und Erweiterung der IT-Infrastruktur
  - bringt *Investitionssicherheit*
- Sensibilisierung bezüglich IT-Sicherheit (Awareness)
  - klare Anweisungen und Zuständigkeiten für die Mitarbeitenden
  - führt zu mehr und bewusster *Mitverantwortung*

«The Big Picture»



Sicherheitsprozeduren im IT-Projektablauf



Werkzeuge/Tools

Werkzeuge	Hilfsmittel	Projekte	Ersteller	Phase
GKS (Sicherheitsgrob-kostenschätzung)	Kritikalitätsbestimmung (z.B. einfache Excel-Tabelle mit Fragen nach System- und Netzwerk-Auslegung, Anwendungstypen, Datenklassifizierung und vordefinierten Kostenrahmen)	alle	PL	Initialisierung
BIA (Business Impact Analysis)	Meeting, Risikotaxonomie (z.B. Matrix zur Einschätzung von Schadenpotential und Eintrittswahrscheinlichkeit)	alle	B-PL, PL	Anford.-aufnahme
SHOCURA (Short-Cut Risk Analysis)	Risikobestimmung mittels generischer Risikoszenarien (z.B. nach CRAMM, ISF IRAM, EBIOS)	alle (evtl. mehrfach)	B-PL, PL, IT-SiBe	Anford.-aufnahme
ISSAC (Information Security Self Assessment Checklist)	Fragebogen (zur Kritikalitätsbestimmung und Fortschrittskontrolle, ausgerichtet am firmeneigenen «Baseline Security Management» z.B. nach BSI, ISO/IEC 27002 (Code of Practice) oder geschäftsspezifischen IT-Basisschutzkatalogen und IS-Policies)	alle (repetitiv, iterativ)	PL, IT-SiBe, Fach-architekt, Engineer	Jederzeit möglich
Sicherheits-konzept	Risikotaxonomie, Word-Template, Homologisierung (z.B. ISDS nach Hermes)	qualitativ riskante P.	(externe) Fachkraft	Lösungs-konzept
Sicherheits-prüfung	Risikotaxonomie, Word-Template, Homologisierung (z.B. nach ISAE 3402)	quantitativ riskante P.	externe Fachkraft	Um-setzung

Beispiel 1 aus der Praxis

Ausgangslage → punktuelle Sicherheitsmassnahmen (z.B. 2-FA für Fernwartungszugriffe), Audits von Fall zu Fall (meist erst nach Einführung eines Projekts), verschärfte Risikosituation durch Einführung von geldwerten Online-Services

Massnahmen → Einführung einer initialen Short-Cut Risk Analysis nach CRAMM, Sicherheitskonzept zwingend für alle Projekte mit vertraulichen Daten und Internetanbindung (Template)

Stärken → alle Projekte eingebunden, proaktive Sicherheitskultur

Schwächen → keine formale Einbindung ins Projektmanagement, Business wird nicht abgeholt, zu viele Sicherheitskonzepte von teilweise fragwürdiger Qualität, fehlendes Massnahmen-Tracking

Weiterentwicklung → nach ca. zehnjähriger Praxis Wechsel zu IRAM, starke Konzentration auf Business Impact Assessments, hohe Formalisierung, Sicherheitskonzepte werden anfangs noch gemacht, später nicht mehr, Verlust der gewachsenen Sicherheitskultur

Beispiel 2 aus der Praxis

Ausgangslage → reaktive statt proaktive Sicherheit (ad-hoc Massnahmen, wenig Standardisierung, viele offene Revisionspendenzen), verschärfte Risikosituation durch Webauftritt und Mehrkanalstrategie

Massnahmen → Grobkostenschätzung und Risiko-Grobanalyse zur Bestimmung von Risiko-Klassen (Excel-Tool, 30 Fragen zu Systemschutz, Datenklassierung und Netzwerksicherheit, 8 Risiko-Szenarien, Eigenentwicklung im Rahmen ISMS-Aufbau), Sicherheitsanalyse und/oder Sicherheitsprüfung auf Basis der Risiko-Klassen (Templates), formal strikte Einbindung ins Projektmanagement

Stärken → alle Projekte eingebunden, Risiko-Klassen bringen Planungs-sicherheit, gute Balance zwischen Analytik und Kontrolle

Schwächen → hoher Betreuungsaufwand seitens Fachstellen, fehlende Baseline Security («jedes Projekt beginnt wieder bei Null»)

Weiterentwicklung →Ergänzung durch iteratives Self Assessment (Checkliste) zur Kritikalitätsbestimmung und Fortschrittskontrolle

Zusammenfassung

- *Formalisierung* durch Integration ins IT-Projekt- und Qualitäts-Management (ab 20 Projekten/Jahr, Qualitätsmesspunkte, Befundungsrunden)
- *Parallelisierung* zu anderen Prozessen (z.B. Architekturprozess, Applikationsentwicklung)
- *Triagierung* zwischen Sicherheitskonzept (proaktiv) und Sicherheitsprüfung (Audit, reaktiv)
- Tool-Unterstützung
- Entlastung durch «Baseline Security Management»
- «Awareness through Self Assessment»

Daniel Felix Maurer
Mobile +41 79 438 65 42
daniel.maurer@temet.ch

Besten Dank für Ihre Aufmerksamkeit!

TEMET AG | Basteiplatz 5 | CH-8001 Zürich
044 302 24 42 | info@temet.ch | www.temet.ch