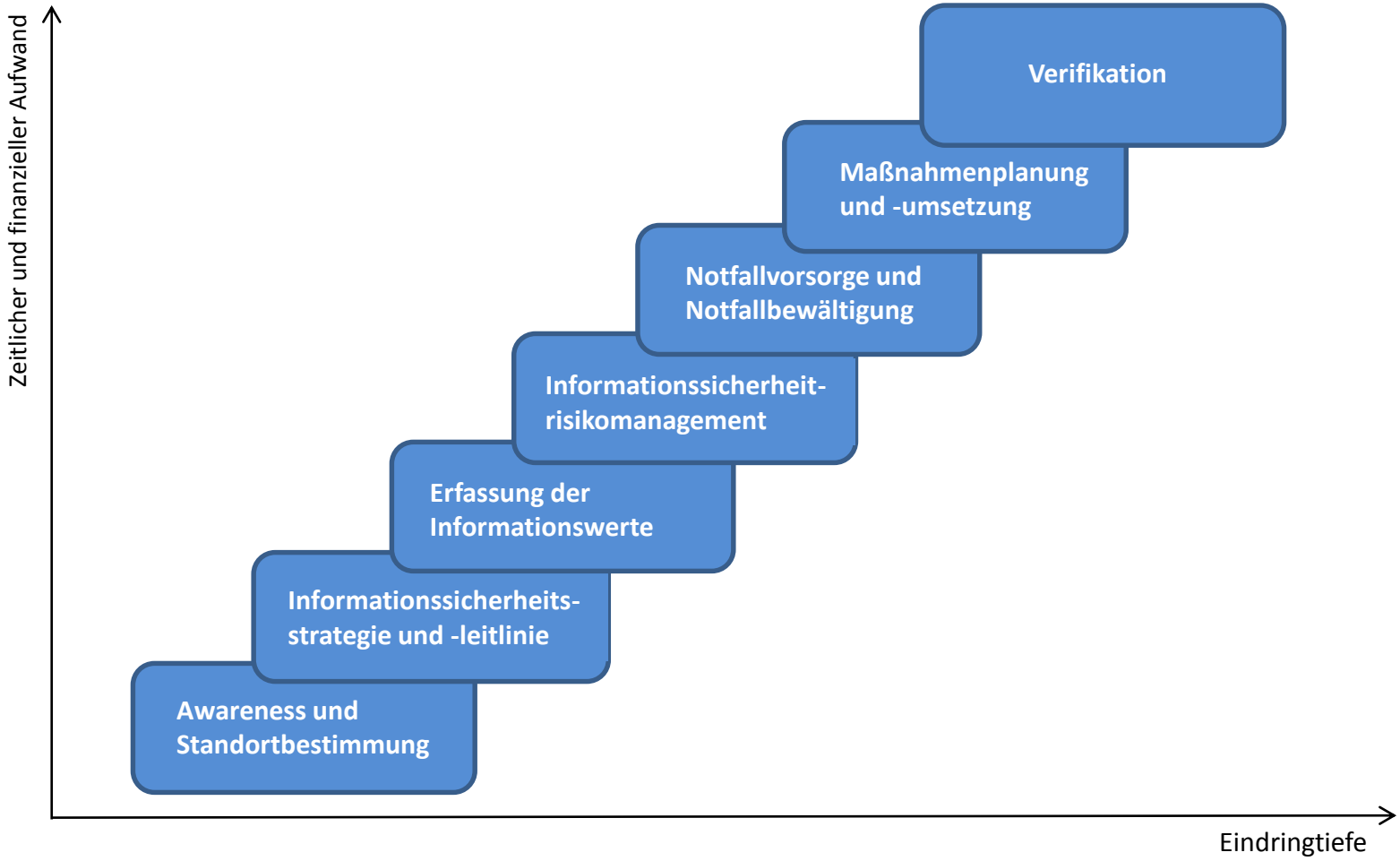
Informationssicherheit im Unternehmen
Vorgehensmodell in 7 Modulen

Fürstenfeldbruck, Januar 2017

Präambel

- Das modulare Vorgehensmodell der ESG Consulting bildet alle spezifischen Erfordernisse der Kunden flexibel ab.
- Die Inhalte der Module orientieren sich an dem international anerkannten Standard der ISO 27001 ff. und sind somit auch bei zukünftigen Anforderungen verwendbar.
- Definierte Übergabepunkte zwischen den Modulen ermöglichen ein flexibles Vorgehen nach den Voraussetzungen, Anforderungen und verfügbaren Ressourcen auf der Kundenseite.
- Die gewünschte bzw. erforderliche Eindringtiefe kann in jedem Modul variiert und auf die jeweiligen Interessen, Gefährdungslage und Risikobereitschaft beim Kunden angepasst werden.
- Nach Bedarf lassen sich die einzelnen Module zu einem kompletten Informationssicherheitsmanagementsystem ausbauen.

Von der Awareness bis zur Verifikation in 7 Modulen



Schaffung von Awareness
Übersicht

- Motivation
  - Informationssicherheit wird meist als kostspielig und lästig empfunden. Meistens ist der Unternehmensleitung die Gefahrenlage und der Höhe eines eventuellen Schadens nicht bewusst. Solange alles funktioniert, besteht aus Sicht der Unternehmensleitung kein Handlungsbedarf. Die Arbeit und Leistung der IT-Abteilung wird dabei oft nicht gebührend gewürdigt.

- Inhalt
  - Allgemeine Trends bzgl. Gefährdungen und Sicherheitsvorfälle
  - Aktuelle Beispiele
  - Anforderungen aus Gesetzen, Wirtschaftsprüfung etc.
  - Beispiele für Anforderungen aus dem geschäftlichen Umfeld des Unternehmens
  - Wirtschaftliche Betrachtung von Schadensfällen
  - Konkrete Tipps für die Erhöhung der Informationssicherheit

- Nutzen
  - Bewusstseinsbildung des Managements über die geschäftliche Bedeutung und Wichtigkeit der Informationssicherheit

Standortbestimmung
Übersicht

- Motivation
  - Oft gibt es kein klares Bild, wie man bzgl. Informationssicherheit aufgestellt ist. Dazu hilft es, eine unabhängige Analyse der Situation durchzuführen und zu dokumentieren.

- Inhalt
  - Auswahl geeigneter Methoden (z.B. Interviews, Workshop, Self-Assessment, Benchmarking)
  - Evaluierung der Anforderungen aus Stand der Technik, geschäftlichem Umfeld, Gesetzen, Branchenstandards etc.
  - Auswahl spezifischer Untersuchungsbereiche
  - Bestandsaufnahme der aktuellen Situation
  - Schwachstellenanalyse bei Organisation, Infrastruktur, Prozessen, Dokumentation, Kommunikation und Nachhaltigkeit der etablierten Maßnahmen
  - Systematische Untersuchung von potentiellen Gefährdungen
  - Beurteilung der Ergebnisse und Zusammenfassung in einem Abschlussbericht

- Nutzen
  - Systematischer, unabhängiger Bericht über den Zustand der Informationssicherheit in Bezug auf Anforderungen und Branchenstandards

Informationssicherheitsstrategie
Übersicht

- Motivation
  - 100% Sicherheit gibt es nicht. Deshalb muss man mit den Schutzmaßnahmen dort ansetzen, wo die wichtigsten Werte und die größten Gefährdungspotentiale liegen. Dazu dient die Entwicklung einer Sicherheitsstrategie.

- Inhalt
  - Ermittlung der Einflussfaktoren wie Geschäftsstrategie, Anforderungen aus Gesetzen, Wirtschaftsprüfung, Kunden- oder Lieferantenverträgen
  - Identifikation der wertvollsten Informationsgüter
  - Beurteilung der Gefährdungslage
  - Festlegung der Risikostrategie
  - Formulierung der Informationssicherheitsstrategie
  - Festlegung konkreter Ziele und des Anwendungsbereichs
  - Dokumentation in der Informationssicherheitsleitlinie
  - Abstimmung mit der Unternehmensleitung

- Nutzen
  - Transparenz über die wertvollsten Informationsgüter und eine von der Unternehmensleitung verantwortete und unterstützte Informationssicherheitsstrategie

Erfassung der Informationswerte (Assets) Übersicht

- Motivation
  - Für die Entwicklung gezielter und wirksamer Schutzmaßahmen ist es notwendig die Informationswerte des Unternehmens zu identifizieren, zu dokumentieren und. bzgl. ihrer Bedeutung für das Unternehmen einzustufen.

- Inhalt
  - Systematische Erfassung und Dokumentation der Informationswerte nach Informationskategorien, z.B. Kundendaten, Vertragsdaten, Forschungs- und Entwicklungsdaten, Personaldaten
  - Unterstützende Werte und Systeme wie Organisation, Gebäude, Hardware, Software oder Personal
  - Bewertung der Assets bzgl. Vertraulichkeit, Integrität und Verfügbarkeit

- Nutzen
  - Transparenz über die zu schützenden Werte und ihrer Bedeutung für das Unternehmen

Informationssicherheitsrisikomanagement Übersicht

- Motivation
  - Fast alle Geschäftsprozesse sind von Informations- und Kommunikationstechnik abhängig. Angriffe auf die Informationssysteme können zu gravierenden finanziellen Schäden führen. Deshalb muss man sich der potentiellen Risiken bewusst werden und eine der Risikostrategie entsprechende Risikobehandlung durchführen.

- Inhalt
  - Einführung eines Informationssicherheitsrisikomanagements gemäß ISO/IEC Standard
    - Festlegung der Rahmenbedingungen (z.B. Risikoakzeptanzkriterien)
    - Identifikation der Risiken (Gefährdungskatalog)
    - Analyse der Risiken (Schadenshöhe, Eintrittswahrscheinlichkeit)
    - Bewertung der Risiken (Vergleich, Priorisierung)
    - Behandlung der Risiken
    - Kontinuierliche Überprüfung und Verbesserung
    - optional: Beratung bei der Auswahl eines Tools zur Unterstützung der Durchführung und Dokumentation
- Nutzen
  - Standardkonformes Informationssicherheitsrisikomanagement kombinierbar mit bestehenden oder einzuführenden Governance, Risk und Compliance Systemen

Informationssicherheitsnotfallmanagement Übersicht

- Motivation
  - Auch mit umfassenden Vorsorgemaßnahmen lässt es sich nicht ausschließen, dass doch einmal etwas passiert. Notfallmanagement ist eine wesentliche Komponente in einem ganzheitlichen Informationssicherheitskonzept für die Vorbereitung auf den Notfall und die Handlungsfähigkeit im Fall der Fälle.
- Inhalt
  - Notfallvorsorge: Maßnahmen wie Datensicherungen, Einführung von redundanten Systemen etc.
  - Notfallbewältigung nach einem festgelegten Notfallplan (niedergelegt im Notfallhandbuch):
    - Definition von Notfällen, Einleitung von Sofortmaßnahmen zur Beschränkung/Unterbindung von Folgeschäden, Festlegung eines Notfallstabs bestehend aus definierten Verantwortlichen für die Maßnahmenumsetzung, z.B. bzgl. Meldewesen und Kommunikation, Pläne für die Fortsetzung der wichtigsten Geschäftsprozess im Notfall, Wiederherstellung von Infrastrukturen, Netzen und Systemen und Wiederanlauf der Anwendungen und Prozesse
  - Etablierung und Pflege einer Notfallmanagement-Kultur
  - Planung und Durchführung von Notfallübungen und Tests
  - Permanente Aufrechterhaltung und Verbesserung des Notfallmanagements
- Nutzen
  - Schaffung der Grundlagen für die Folgeschadensbegrenzung und Ermöglichung eines geregelten und schnellen Wiederanlaufen von Netzen, Systemen und Diensten

Maßnahmenplanung und -umsetzung Übersicht

- Motivation
  - Nach vorangegangenen Analysen und Aufdeckung von Schwachstellen und Risiken müssen Maßnahmen getroffen werden, um die Risiken zu vermeiden oder zumindest signifikant zu reduzieren. Diese müssen geplant und entsprechend umgesetzt werden.

- Inhalt
  - Beurteilung der notwendigen Maßnahmen
  - Kostenabschätzung (Anschaffungs- und laufende Kosten inklusive Personalaufwand)
  - Auswahl von angemessenen (Preis-/Leistungsverhältnis) Lösungen
  - Priorisierung der Maßnahmen
  - Erstellung eines Umsetzungsplans mit Zeitrahmen und Verantwortlichkeiten
  - Steuerung und Kontrolle der Umsetzung im Rahmen des Umsetzungsplans

- Nutzen
  - Zeitgerechte und kosteneffiziente Umsetzung der notwendigen und wirkungsvollsten Maßnahmen

Verifikation – Penetrationstest Übersicht

- Motivation
  - Die Verifikation aller Maßnahmen zur Informationssicherheit wird sich – wie schon im Falle der Umsetzung - stark an der Gefährdungseinschätzung bzw. dem Schutzbedürfnis des einzelnen Unternehmens ausrichten. Ob Testat oder formale Zertifizierung, ob Self Assessment oder Penetrationstest, alle diesbezüglichen Maßnahmen orientiert sich an den jeweiligen Erfordernissen.
- Inhalt
  - Perimeter**analyse** (Auflistung der von außen erreichbaren Systeme bzw. IP-Adressen)
  - System- und Dienste-**Inventarisierung** (Erfassung der Dienste- bzw. Systemversionen, soweit von außen erreichbar)
  - Schwachstellen**scans** (Versuch über bekannte Schwachstellen Zugriff auf Systeme und Dienste zu erhalten) und Detailanalyse der so gefundenen Schwachstellen
  - Nicht autorisierte **Rechteübernahme** bei ausgewählten Systemen und Diensten innerhalb nachgestellter typischer Angriffsszenarien
  - **Dokumentation** festgestellter Schwachstellen und Bewertung von **Handlungsoptionen** zur Schließung der Schwachstellen
- Nutzen
  - Neutrales Bild auf die Wirksamkeit bislang getroffener Maßnahmen
  - Hinweise für weitere Verbesserungsoptionen innerhalb des gesamten Informationssicher-heitssystems (Roadmap)

Verifikation – Zertifizierung
Übersicht

- Motivation
  - Vor einer geplanten Zertifizierung empfiehlt es sich, noch einmal eine möglichst unabhängige Überprüfung auf Erfüllung aller wesentlichen Zertifizierungsanforderungen durchzuführen.

- Inhalt
  - Überprüfung des Erreichungsgrads der Zertifizierungsanforderungen in Dokumentation und praktischer Umsetzung
  - Dokumentation festgestellter Mängel oder Schwachpunkte
  - Vorschläge für Behebung festgestellter Mängel und Schwachpunkte
  - Training der betroffenen Mitarbeiter
  - Empfehlungen für weitere Verbesserungsoptionen innerhalb des gesamten Informationssicherheitssystems
  - Optional: Begleitung der Zertifizierung

- Nutzen
  - Optimale Vorbereitung auf die Zertifizierung durch geschulte, überzeugend auftretende Mitarbeiter

Ihre Ansprechpartner

ESG CONSULTING GMBH
Livry-Gargan-Straße 6
D-82256 Fürstenfeldbruck

Ulrich Bethäuser, Vertrieb Industry
Telefon +49 (0) 89 92161 2517
ulrich.bethaeuser@esg-consulting.com

Johannes Seeberger, Vertrieb Public Sector
Telefon +49 (0) 89 92161 2802
j.seeberger@esg-consulting.com

www.esg-consulting.com