Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

Information Security Management
05 – Policies, Concepts & Guidelines

HSLU – Informatik

Mathias Bücherl (M.Sc.)

Tel. +41 79 746 10 98

mathias.buecherl@hslu.ch

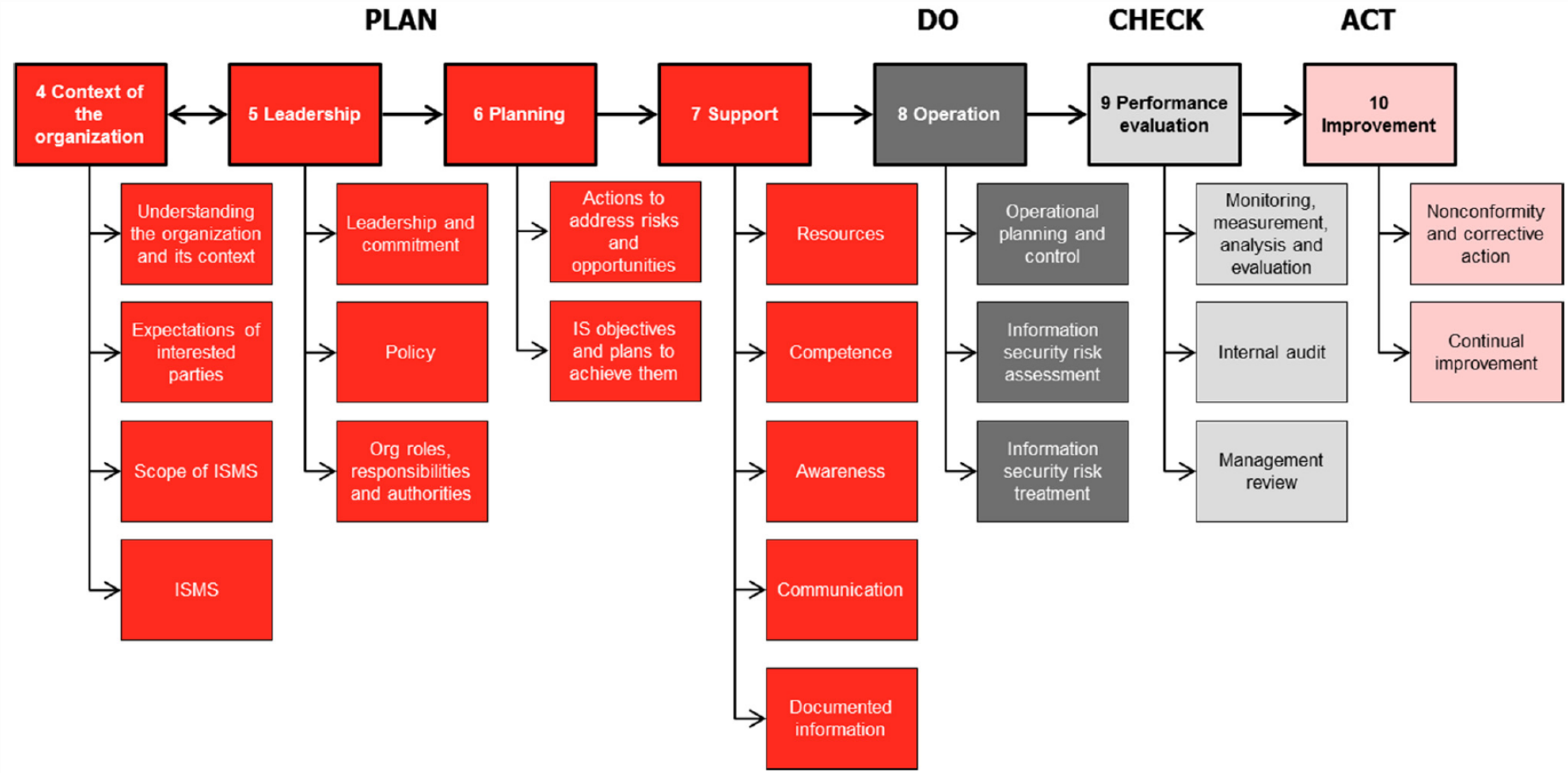
Ziele

- Sie verstehen das Vorgehen für den Aufbau eines ISMS (Vorbereitung, Dokumente, Risikomanagement, KVP etc.)
- Sie unterscheiden den Aufbau nach deutschem und anglo-amerikanischem Einteilung
- Sie kennen die geforderten Inhalte von EISP, ISSP, SSSP und Guidelines
- Sie haben eine Vorstellung, wie diese Dokumente in Ihr Unternehmen eingeführt werden

AGENDA

1. **Überblick**
2. Enterprise IS Policies
3. Conceptual IS Policies (issue / system specific)
4. Guidelines
5. Übung

Vorgehen ISMS nach ISO27001



Quelle: Präsentation zum bsi ISO/IEC 27001 Launch Event, London, 27 November 2013

Vorgehen ISMS

Vorbereitung	Dokumente	Risikomgmt.	KVP

Gruppenübung:
Füllen Sie die zu erbringenden Teile *chronologisch* in die Kolumnen ein!

Vorgehen ISMS

Vorbereitung	Dokumente	Risikomgmt.	KVP
Auftrag durch GL	InfoSec Policy	Asset Register	Kontrolle
Auslegeordnung	Issue-specific SP	Risk Estimation	Sanktionen
Vorschlag an GL	System-specific SP	Risk Evaluation	KVP
Budget-Gutsprache	Guidelines	Risk Treatment	Audit
	Freigabe / Kommunikation	Umsetzung / Schulung	Bericht an GL

Plan, Do, Check, Act

Wichtige Dokumente 1/3

Externe Dokument

1. Gesetzliche Grundlagen: Gesetze, Verordnungen
2. Regulatorische Vorgaben: branchenabhängig
3. Standards: ISO 2700x, BSI 200-x, Cobit, ITIL etc.
4. Frameworks, z.B. NIST Cybersecurity Framework

Firmenspezifische Dokumente

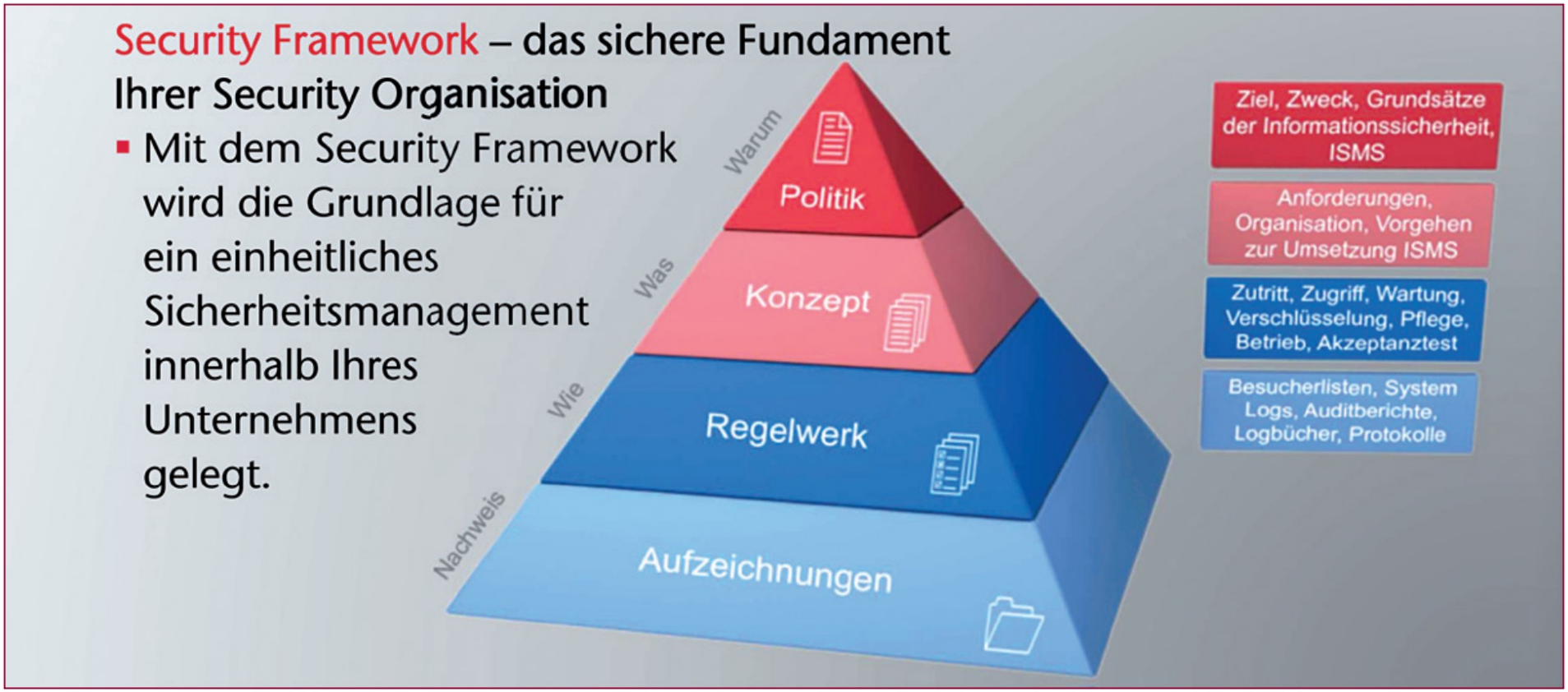
1. Mission Statement der Firma
2. Strategie der Firma
3. Governance der IT

Wichtige Dokumente 2/3

Dokumente der Informationssicherheit

1. Strategie der Informationssicherheit
2. Enterprise Information Security Policy
   (Ziele, Organisation, Vorgehen)
3. Issue Specific Security Policy (Cyber Crime, Feuer)
4. System Specific Security Policy
   (Rechenzentrum, Netzwerk, Endgeräte)
5. Guidelines, OnePagers etc. (Benutzerrichtlinie, Evakuationsplan, Backup-Richtlinien, Passwort-Richtlinien, Checklisten etc.)
6. Dokumentation (Netzpläne, Protokolle, Log Files etc.)

Wichtige Dokumente 3/3

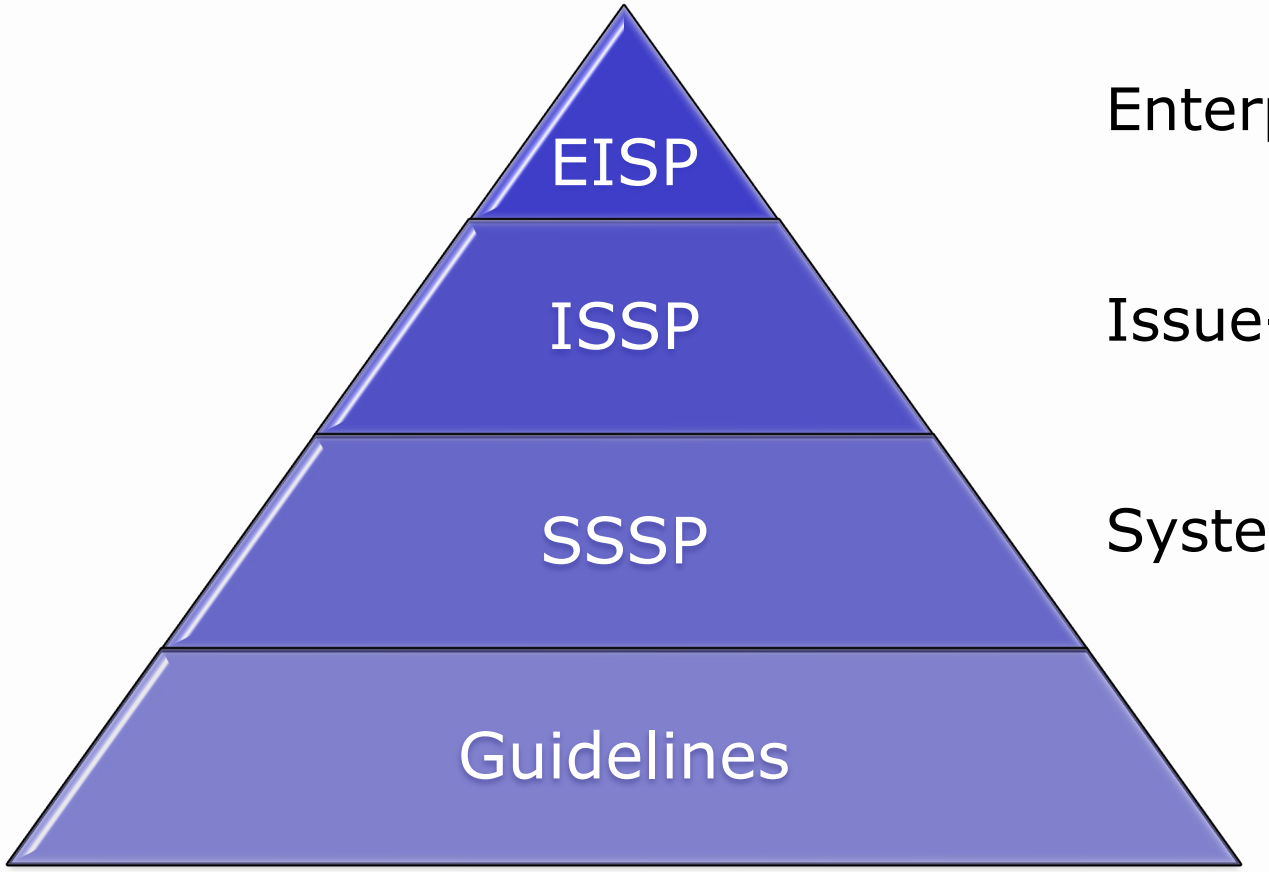


Experten raten wegen der zunehmend professionelleren Cyberattacken zu umfassenden Strategien zum Schutz der IT. Bildquelle: Swiss Infosec

AGENDA

1. Überblick
2. **Enterprise IS Policies**
3. Conceptual IS Policies (issue / system specific)
4. Guidelines
5. Übung

Security Pyramid (english split)



Enterprise IS Policy

Issue-specific IS Pol

System-specific ISP

Erstellung einer Enterprise InfoSec Policy (1/2)

Erstellung einer Enterprise InfoSec Policy (2/2)

Jede Unternehmung sollte eine schriftliche IS Policy haben, um zu demonstrieren, dass

- die Firma InfoSec und Datenschutz ernst nimmt
- sie Systeme vorhält, die diese beschützen
- es eine klare Abstimmung zwischen IS und GL gibt
- eine gezielte Strategie verfolgt wird
- eine wirkungsvolle Organisation aufgebaut wird
- genügend Finanzen und Ressourcen vorhanden sein müssen

Inhalte einer Enterprise Information Security Policy

- **Grundsätzliches:**
- Geschäfte des Unternehmens und Rolle der Informationen und der IT
- Umwelt u.a. für Unternehmen wichtige Märkte und Technologien
- Wichtige Unternehmens-Assets, Geographische und örtliche Charakteristiken, Hauptsächliche Bedrohungen, Anspruchsgruppen und deren Sicherheitsbedürfnisse, Anforderungen gesetzlicher, regulatorischer und vertraglicher Art
- Für Informations-Sicherheit relevante Ziele und Grundsätze aus Unternehmens-Risiko-Politik und Kommittment des Managements bezüglich Einhaltung der Anforderungen , Ziele und Grundsätze
- Hinweis auf Risiko- und Sicherheitskultur, -bewusstsein, -kommunikation und Schulung
- Hinweis auf Mass der angestrebten „Unternehmens-Sicherheitsreife" (entspr. Maturity Modell)
- Begriffsdefinition Informationen, IT-Systeme und deren Komponenten
- Einsatzbereich und Abgrenzung (Assets, Umfang) der Informationssicherheit und des ISMS
  - Informationen, IT-Systeme, IT-Prozesse über den gesamten Lebenszyklus, IT-Benutzer
  - Nicht zur Informations-Sicherheit gehörende Funktionen (z.B. physische Objekt-Sicherheit)
- Sicherheits- und Risikoziele und generelle Aussagen über deren Einhaltung
  - Vertraulichkeit (Datenschutz, Bankkundengeheimnis, Geschäfts-Geheimnis)
  - Integrität (allenfalls auch Authentizität, Non-Repudiation und Zuverlässigkeit), Verfügbarkeit
- Risiko-Management
  - Unternehmens-Risikomanagementprozess
  - Kriterien zur Risikoeinschätzung und Risikoakzeptanz
  - Methode und Hinweise auf Prozess-Beschreibungen
- Referenzierung der Prozesse für Geschäftskontinuität und IT-Notfall-Planung hinsichtlich Informationssicherheit
- Referenzierung der Informationssicherheits-Vorschriften
  - für Outsourcing
  - für Externe und Vertragspartner
- Bereitstellung der erforderlichen Mittel und Ressourcen
- Bezugnahme auf weitere Weisungen über einzelne Risiko-Bereiche
- **Festlegung der Verantwortlichkeiten und Kompetenzen:** Leiter von Geschäftseinheiten,
- CISO, CIO, IT-Prozess- und IT-System-Owner, Internes Audit, MitarbeiterInnen…
- **Policy-Geltungsbereich:** Z.B. MitarbeiterInnen ganzes Unternehmen
- **Inkraftsetzung:** Datum Unterschrift CEO

Struktur einer InfoSec Policy (1/3)

Inhalt

Struktur einer InfoSec Policy (2/3)

Struktur einer InfoSec Policy (3/3) - Templates

http://templatelab.com/security-policy-templates
s. Ilias

PB&J Restaurants PHI and other sensitive data Security Policy.

I. POLICY

A. It is the policy of PB&J RESTAURANTS that information, as defined hereinafter, in all its forms--written, spoken, recorded electronically or printed--will be protected from accidental or intentional unauthorized modification, destruction or disclosure throughout its life cycle. This protection includes an appropriate level of security over the equipment and software used to process, store, and transmit that information.

B. All policies and procedures must be documented and made available to individuals responsible for their implementation and compliance. All activities identified by the policies and procedures must also be documented. All the documentation, which may be in electronic form, must be retained for at least 6 (six) years after initial creation, or, pertaining to policies and procedures, after changes are made. All documentation must be periodically reviewed for appropriateness and currency, a period of time to be determined by each entity within PB&J RESTAURANTS.

C. At each entity and/or department level, additional policies, standards and procedures will be developed detailing the implementation of this policy and set of standards, and addressing any additional information systems functionality in such entity and/or department. All departmental policies must be consistent with this policy. All systems implemented after the effective date of these policies are expected to comply with the provisions of this policy where possible. Existing systems are expected to be brought into compliance where possible and as soon as practical.

II. SCOPE

A. The scope of information security includes the protection of the confidentiality, integrity and availability of information.

B. The framework for managing information security in this policy applies to all PB&J RESTAURANTS entities and workers, and other Involved Persons and all Involved Systems throughout PB&J RESTAURANTS as defined below in **INFORMATION SECURITY DEFINITIONS.**

C. This policy and all standards apply to all protected health information and other classes of protected information in any form as defined below in **INFORMATION CLASSIFICATION.**

III. RISK MANAGEMENT

EXAMPLE OF INFORMATION SECURITY POLICY

It is the established policy of (Company Name) to operate within the requirements of a documented Information Security Policy statement as a means to comply with all statutory, regulatory and contractual requirements, and, to protect the interests, property and information of the company, and of its clients and employees, against threats or loss.

In pursuance of this policy its stated requirements have been implemented together with the specified requirements of the company's associated information security and computer system access management work instructions.

The purpose of this Information Security Policy statement is to describe how security is implemented, to give guidance to our employees whose actions can affect the confidentiality and integrity of the business, its product and services, and, to illustrate the overall commitment to security issues within our company.

This Information Security Policy statement, which is not intended as a stand-alone document, is supported by detailed process operating procedures and where appropriate by quality management system Work Instructions (WI), to form a set of working documents, which define our company's security activities.

The Information Security Policy is maintained by audit and review, and by the methods described in the quality manual, in order to provide effective assurance that all aspects of company, employee and customer specified security requirements are being implemented.

It is company policy to ensure that the use of documents, computers, mobile computing, mobile communications, mail, voice mail, voice communications in general, multimedia, postal services and fax machines must be controlled to prevent unauthorized use and to reduce security risks.

All employees have a responsibility not to compromise the company, e.g. by sending defamatory or harassing electronic mail, or by making unauthorized purchases, and, must also be aware that the confidentiality and integrity of information transmitted by E-mail or facsimile may not be guaranteed.

Access by employees to the Internet is restricted to business use only and any breach of this policy will result in disciplinary action being taken.

The Manager is responsible for managing information security, and he will also ensure that all employees are trained to understand, implement and maintain the security objectives set out in this Security Policy and as detailed in the company's security related Work Instructions.

We publish this policy statement in the knowledge that the security of our company and its employees, products and client services, and our on-going good security reputation, depend upon the every day security awareness and actions of all our employees, both on-site and off-site.

I am wholly committed to this Information Security Policy, and hereby state that it is the responsibility of every individual employee of the company to ensure that all security plans, standards, procedures, work instructions and actions fully meet with agreed company and customer requirements.

TAHO
Tasmanian Archive & Heritage Office

Template Information Security Policy

This template details the mandatory clauses which must be included in an agency's Information Security Policy as per the requirements of the WoG Information Security Policy Manual. In addition, this document also provides context to the mandatory clauses by structuring them within an example Information Security policy, with additional guidance provided on other issues which agencies may wish to consider when developing their policies.

An agency's Information Security policy provides governance for information security management, and direction & support within the agency. The development and approval of an agency's information security policy not only establishes management commitment and governance arrangements, but defines the agency's policy in all aspects of information security, including asset management, human resource management and compliance.

Template Structure

The Whole of Government Information Security Policy Manual will be referred to in this template as 'the manual'.

The manual and supporting Procedures contain mandatory and recommended statements. Terminology is used as follows to indicate whether a Policy or Procedure statement is mandatory, conditional or recommended.

Keyword	Interpretation
MUST	The item is mandatory.
MUST NOT	Non-use of the item is mandatory.
SHOULD	Valid reasons to deviate from the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
SHOULD NOT	Valid reasons to implement the item may exist in particular circumstances, but the full implications need to be considered before choosing this course.
RECOMMENDS RECOMMENDED	The item is encouraged or suggested.

'MUST' and 'MUST NOT' statements are highlighted in red throughout this template. Agencies deviating from these MUST advise the Agency ICT Reference Group of the decision to waive particular requirements. Agencies deviating from a 'SHOULD' or 'SHOULD NOT' statement MUST record:

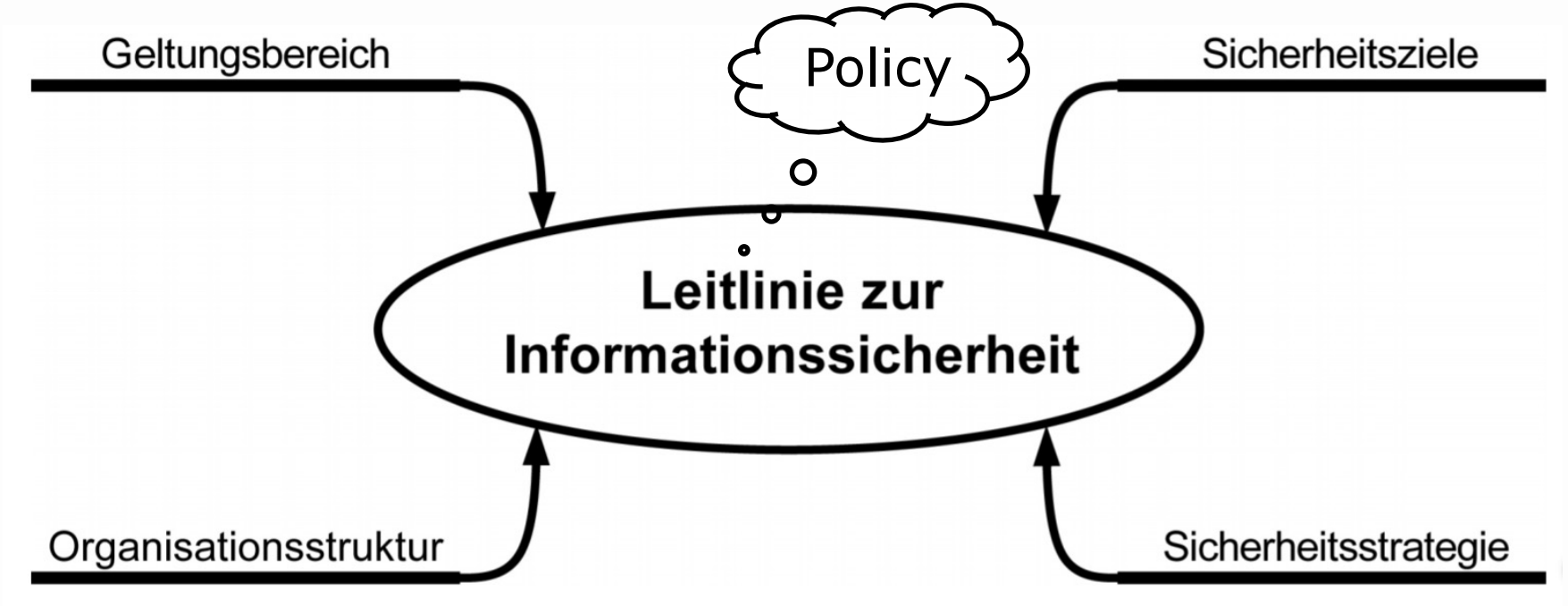
- the reasons for the deviation,
- an assessment of the residual risk resulting from the deviation,
- the date at which the decision will be reviewed, and
- whether the deviation has management approval.

Agencies deviating from a RECOMMENDS or RECOMMENDED requirement are encouraged to document the reasons for doing so.

Department of Education
LINC Tasmania

Tasmania

Das absolute Minimum einer Enterprise IS Policy



AGENDA

1. Überblick
2. Enterprise IS Policies
3. **Conceptual IS Policies (issue / system specific)**
4. Guidelines
5. Übung

Definitionen und Unterscheidung EISP, ISSP, SysSSP:

- **Enterprise Information Security Policy, EISP**, directly supports the mission, vision, and directions of an organization. Also known as the general security policy, EISP sets the direction, scope, and tone for all security efforts. The EISP is the guideline for development, implementation, and management of a security program. The EISP is drafted by the chief executive officer of the organization. This policy is usually modified only if there is a change in strategic direction of the organization.
- **Issue-Specific Security Policy, ISSP**, addresses specific issue, requires updates frequently, and contains a statement on the organization's position on specific issues. This policy addresses topics such as; who has access to the internet, use of personal equipment on company networks, use of photocopy equipment, and prohibitions against hacking.
- **System-Specific Security Policy, SysSSP**, is a policy that functions as instructions or procedures that are to be used when configuring systems. An example of a SysSSP is a document provided by management to guide the configuration of technology intended to support information security.

https://eastonandersonwordpress.wordpress.com/2017/03/15/information-security-policy-types-eisp-issp-syssp/

Aufbau eines Issue Specific Concepts

IssueSSP zum Beispiel für:

- Use of company-owned networks and the Internet
- Use of telecommunications technologies (fax and phone)
- Use of electronic mail
- Specific minimum configurations of computers to defend against worms and viruses
- Prohibitions against hacking or testing organization security controls
- Home use of company-owned computer equipment
- Use of personal equipment on company networks
- Use of photocopy equipment

Aufbau eines System Specific Concepts (1/2)

… wie man individuelle Systeme aufsetzt und betreibt. Bsp. Firewall-Konfiguration

The SysSSP Explained

Unlike an Enterprise Information Security Policy or even an Issue-Specific Security Policy, a **System-Specific Security Policy**, frequently abbreviated SysSSP, has a look of its own. The SysSSP is more like a manual of procedures for how systems should be configured or maintained.

For example, using a SysSSP to determine how to select and set up the company's firewall. Another example of how this type of policy might work could lie in explaining access levels for different types of computer users in the workplace since not every user will need access to the same levels of controls.

SysSSPs are very targeted documents, relating only to the specific system (get it?) they are designed to address. Therefore, each system in a workplace will likely need its own systems-specific policy to outline how it functions and how it's managed.

Aufbau eines System Specific Concepts (2/2)

… wie man individuelle Systeme aufsetzt und betreibt. Bsp. Firewall-Konfiguration

SysSSP Components

There are two general components affiliated with this type of policy. They are known as **managerial guidance** and **technical specifications**. And, even though there are two groups to be considered, the SysSSP is often written as a single, comprehensive document that includes both. Managerial guidance details a company's security objectives. Security objectives explain how a particular resource or system is used functionally or to support business objectives. It also details how a company's leadership wants systems to be set up or maintained. For example, without a SysSSP that details managerial guidelines for setting up a firewall, an IT administrator may choose certain settings based on his knowledge or personal preferences. This part of the document provides guidance for configuring the firewall system.

AGENDA

1. Überblick
2. Enterprise IS Policies
3. Conceptual IS Policies (issue / system specific)
4. **Guidelines**
5. Übung

Erstellung von Guidelines

„Beispiele“ aus der Google-Suche – Achtung!

- IT-Sicherheitsleitlinie
- Richtlinie zur IT-Nutzung
- Richtlinie zur Internet- und E-Mail-Nutzung
- Richtlinie zum Outsourcing
- Sicherheitshinweise für IT-Benutzer
- Sicherheitshinweise für Administratoren

- Viren-Schutz*konzept*
- Datensicherungs*konzept*
- Notfallvorsorge*konzept*
- Archivierungs*konzept*

AGENDA

1. Überblick
2. Enterprise IS Policies
3. Conceptual IS Policies (issue / system specific)
4. Guidelines
5. **Übung**

Übung

- Gruppe 1 „Security Policy“
- Gruppe 2 „Standards“
- Gruppe 3 „Baseline“
- Gruppe 4 „Guideline“
- Gruppe 5 „Procedure“

- Gruppengröße: Kurs /5
- Vorbereitungszeit: 60 Minuten

- Erstellung einer Definition der oben genannten Begriffe
- Erstellung einer Präsentation mit einem Zeitrahmen von max. 10 Minuten
- Erstellung eines One-Pagers für die Prüfung

Übung: Analyse / Bewertung von InfoSec-Dokumenten

Suchen Sie die Dokumentenarten “Policy”, “Konzepte” (SysSSP und IssueSSP), sowie “Guidelines”

1. Suchen Sie *passende* Beispiel-Dokumente im Internet, keine Muster, sondern *reelle* Dokument.
2. Analysieren Sie deren Ziel, Struktur, Zielgruppen etc.
3. Vergleichen Sie diese mit den oben erklärten Dokumenten
4. Stellen Sie Ihre Findings in einer PPT zusammen und stellen Sie diese in die Übungsablage auf Ilias.
5. Bringen Sie Ihre Findings in die anschliessende Diskussion ein.

Übung: Analyse und Bewertung von InfoSec-Dokumenten

Gruppe 1: EISP
Gruppe 2: IssueSSP
Gruppe 3: SysSSP
Gruppe 4: Guideline
Gruppe 5: EISP
Gruppe 6: IssueSSP
Gruppe 7: SysSSP
Gruppe 8: Guideline
Gruppe 9: EISP
Gruppe 10: IssueSSP
Gruppe 11: SysSSP
Gruppe 12: Guideline