Delta Logic AG

konsequent kundenorientiert
solutions focalisées sur le client

"Informationssicherheit in der Rechtspflege"

Chancen, Herausforderungen, praktische Lösungen

Reto Frischknecht, Delta Logic AG
Adolf J. Doerig, Doerig + Partner AG

eJustice.CH, 13. Magglinger Rechtsinformatikseminar, 19. März 2013

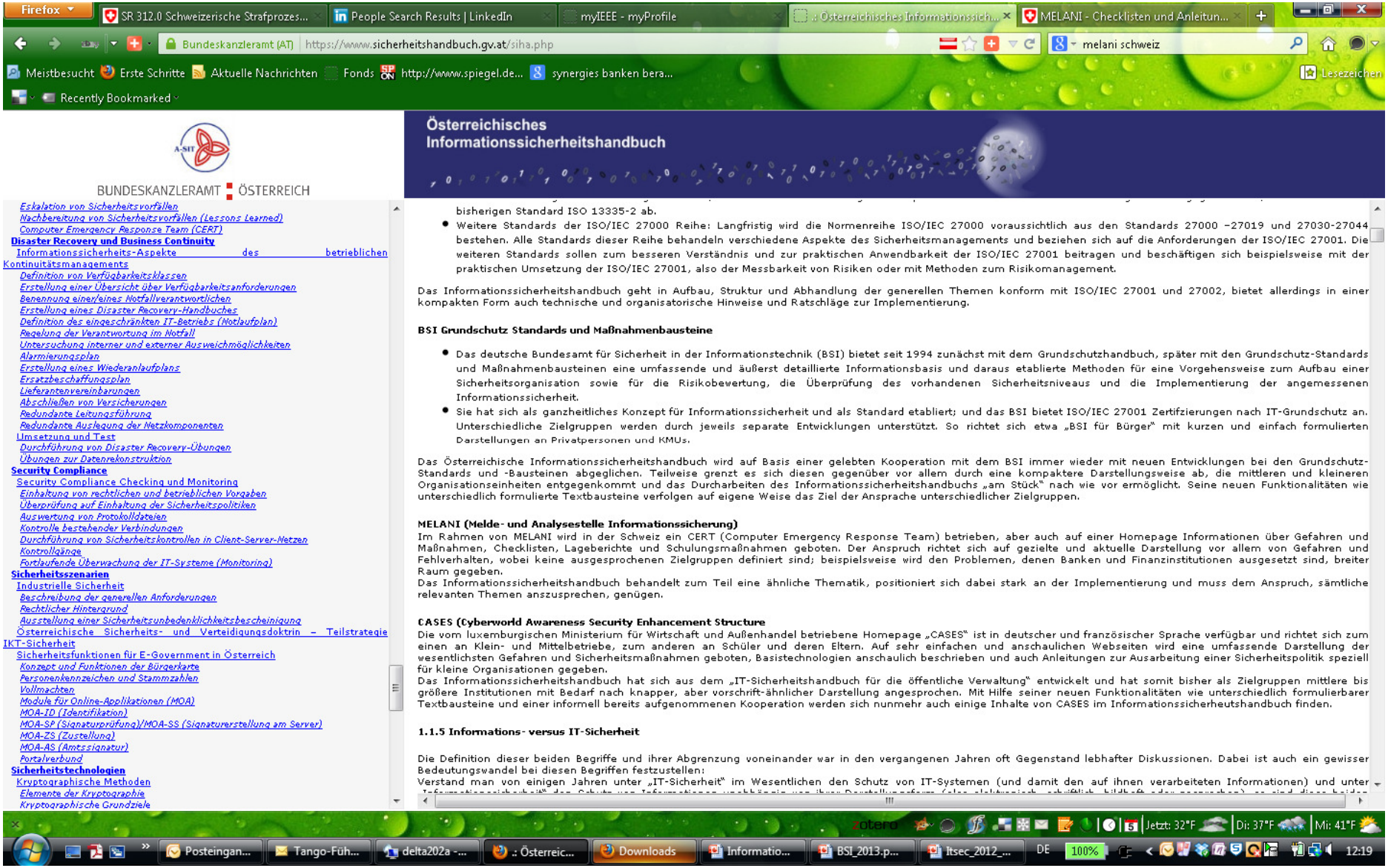
Agenda

- **Ausgangslage**
- Informationssicherheit
- ISO 27001
- Ihre Fragen

Informationssicherheit: Bund wird nervös

Mittwoch, 24.10.2012:

- **„Der kürzliche Datenklau** hat den Bund aufgeschreckt."
- „Der Bundesrat hat heute das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) damit beauftragt **bis Ende Februar 2013 eine Analyse der Gefahren und Lücken im Bereich Informationssicherheit vorzulegen**."


Österreichisches
Informationssicherheitshandbuch
BUNDESKANZLERAMT ÖSTERREICH
Eskalation von Sicherheitsvorfällen
Nachbereitung von Sicherheitsvorfällen (Lessons Learned)
Computer Emergency Response Team (CERT)
Disaster Recovery und Business Continuity
Informationssicherheits-Aspekte des betrieblichen Kontinuitätsmanagements
Definition von Verfügbarkeitsklassen
Erstellung einer Übersicht über Verfügbarkeitsanforderungen
Benennung einer/eines Notfallverantwortlichen
Erstellung eines Disaster Recovery-Handbuches
Definition des eingeschränkten IT-Betriebs (Notlaufplan)
Regelung der Verantwortung im Notfall
Untersuchung interner und externer Ausweichmöglichkeiten
Alarmierungsplan
Erstellung eines Wiederanlaufplans
Ersatzbeschaffungsplan
Lieferantenvereinbarungen
Abschließen von Versicherungen
Redundante Leitungsführung
Redundante Auslegung der Netzkomponenten
Umsetzung und Test
Durchführung von Disaster Recovery-Übungen
Übungen zur Datenrekonstruktion
Security Compliance
Security Compliance Checking und Monitoring
Einhaltung von rechtlichen und betrieblichen Vorgaben
Überprüfung auf Einhaltung der Sicherheitspolitiken
Auswertung von Protokolldateien
Kontrolle bestehender Verbindungen
Durchführung von Sicherheitskontrollen in Client-Server-Netzen
Kontrollgänge
Fortlaufende Überwachung der IT-Systeme (Monitoring)
Sicherheitsszenarien
Industrielle Sicherheit
Beschreibung der generellen Anforderungen
Rechtlicher Hintergrund
Ausstellung einer Sicherheitsunbedenklichkeitsbescheinigung
Österreichische Sicherheits- und Verteidigungsdoktrin – Teilstrategie IKT-Sicherheit
Sicherheitsfunktionen für E-Government in Österreich
Konzept und Funktionen der Bürgerkarte
Personenkennzeichen und Stammzahlen
Vollmachten
Module für Online-Applikationen (MOA)
MOA-ID (Identifikation)
MOA-SP (Signaturprüfung)/MOA-SS (Signaturerstellung am Server)
MOA-ZS (Zustellung)
MOA-AS (Amtssignatur)
Portalverbund
Sicherheitstechnologien
Kryptographische Methoden
Elemente der Kryptographie
Kryptographische Grundziele
bisherigen Standard ISO 13335-2 ab.
Weitere Standards der ISO/IEC 27000 Reihe: Langfristig wird die Normenreihe ISO/IEC 27000 voraussichtlich aus den Standards 27000 -27019 und 27030-27044 bestehen. Alle Standards dieser Reihe behandeln verschiedene Aspekte des Sicherheitsmanagements und beziehen sich auf die Anforderungen der ISO/IEC 27001. Die weiteren Standards sollen zum besseren Verständnis und zur praktischen Anwendbarkeit der ISO/IEC 27001 beitragen und beschäftigen sich beispielsweise mit der praktischen Umsetzung der ISO/IEC 27001, also der Messbarkeit von Risiken oder mit Methoden zum Risikomanagement.
Das Informationssicherheitshandbuch geht in Aufbau, Struktur und Abhandlung der generellen Themen konform mit ISO/IEC 27001 und 27002, bietet allerdings in einer kompakten Form auch technische und organisatorische Hinweise und Ratschläge zur Implementierung.
BSI Grundschutz Standards und Maßnahmenbausteine
Das deutsche Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet seit 1994 zunächst mit dem Grundschutzhandbuch, später mit den Grundschutz-Standards und Maßnahmenbausteinen eine umfassende und äußerst detaillierte Informationsbasis und daraus etablierte Methoden für eine Vorgehensweise zum Aufbau einer Sicherheitsorganisation sowie für die Risikobewertung, die Überprüfung des vorhandenen Sicherheitsniveaus und die Implementierung der angemessenen Informationssicherheit.
Sie hat sich als ganzheitliches Konzept für Informationssicherheit und als Standard etabliert; und das BSI bietet ISO/IEC 27001 Zertifizierungen nach IT-Grundschutz an. Unterschiedliche Zielgruppen werden durch jeweils separate Entwicklungen unterstützt. So richtet sich etwa „BSI für Bürger" mit kurzen und einfach formulierten Darstellungen an Privatpersonen und KMUs.
Das Österreichische Informationssicherheitshandbuch wird auf Basis einer gelebten Kooperation mit dem BSI immer wieder mit neuen Entwicklungen bei den Grundschutz-Standards und -Bausteinen abgeglichen. Teilweise grenzt es sich diesen gegenüber vor allem durch eine kompaktere Darstellungsweise ab, die mittleren und kleineren Organisationseinheiten entgegenkommt und das Durcharbeiten des Informationssicherheitshandbuchs „am Stück" nach wie vor ermöglicht. Seine neuen Funktionalitäten wie unterschiedlich formulierte Textbausteine verfolgen auf eigene Weise das Ziel der Ansprache unterschiedlicher Zielgruppen.
MELANI (Melde- und Analysestelle Informationssicherung)
Im Rahmen von MELANI wird in der Schweiz ein CERT (Computer Emergency Response Team) betrieben, aber auch auf einer Homepage Informationen über Gefahren und Maßnahmen, Checklisten, Lageberichte und Schulungsmaßnahmen geboten. Der Anspruch richtet sich auf gezielte und aktuelle Darstellung vor allem von Gefahren und Fehlverhalten, wobei keine ausgesprochenen Zielgruppen definiert sind; beispielsweise wird den Problemen, denen Banken und Finanzinstitutionen ausgesetzt sind, breiter Raum gegeben.
Das Informationssicherheitshandbuch behandelt zum Teil eine ähnliche Thematik, positioniert sich dabei stark an der Implementierung und muss dem Anspruch, sämtliche relevanten Themen anzusprechen, genügen.
CASES (Cyberworld Awareness Security Enhancement Structure
Die vom luxemburgischen Ministerium für Wirtschaft und Außenhandel betriebene Homepage „CASES" ist in deutscher und französischer Sprache verfügbar und richtet sich zum einen an Klein- und Mittelbetriebe, zum anderen an Schüler und deren Eltern. Auf sehr einfachen und anschaulichen Webseiten wird eine umfassende Darstellung der wesentlichsten Gefahren und Sicherheitsmaßnahmen geboten, Basistechnologien anschaulich beschrieben und auch Anleitungen zur Ausarbeitung einer Sicherheitspolitik speziell für kleine Organisationen gegeben.
Das Informationssicherheitshandbuch hat sich aus dem „IT-Sicherheitshandbuch für die öffentliche Verwaltung" entwickelt und hat somit bisher als Zielgruppen mittlere bis größere Institutionen mit Bedarf nach knapper, aber vorschrift-ähnlicher Darstellung angesprochen. Mit Hilfe seiner neuen Funktionalitäten wie unterschiedlich formulierbarer Textbausteine und einer informell bereits aufgenommenen Kooperation werden sich nunmehr auch einige Inhalte von CASES im Informationssicherheutshandbuch finden.
1.1.5 Informations- versus IT-Sicherheit
Die Definition dieser beiden Begriffe und ihrer Abgrenzung voneinander war in den vergangenen Jahren oft Gegenstand lebhafter Diskussionen. Dabei ist auch ein gewisser Bedeutungswandel bei diesen Begriffen festzustellen:
Verstand man von einigen Jahren unter „IT-Sicherheit" im Wesentlichen den Schutz von IT-Systemen (und damit den auf ihnen verarbeiteten Informationen) und unter

Motion SR Pirmin Bischof – Chancen nutzen

„Der Bundesrat wird beauftragt,

1. die nötigen rechtlichen, organisatorischen und technischen Vorkehrungen zu treffen, damit der bereits in ZPO, StPO, SchKG und im **Bundesverwaltungsrecht vorgesehene elektronische Rechtsverkehr (ERV)** für den gesamten Behördenverkehr (inkl. Gerichte) in der ganzen Schweiz einheitlich umgesetzt wird und auf allen Stufen funktioniert;

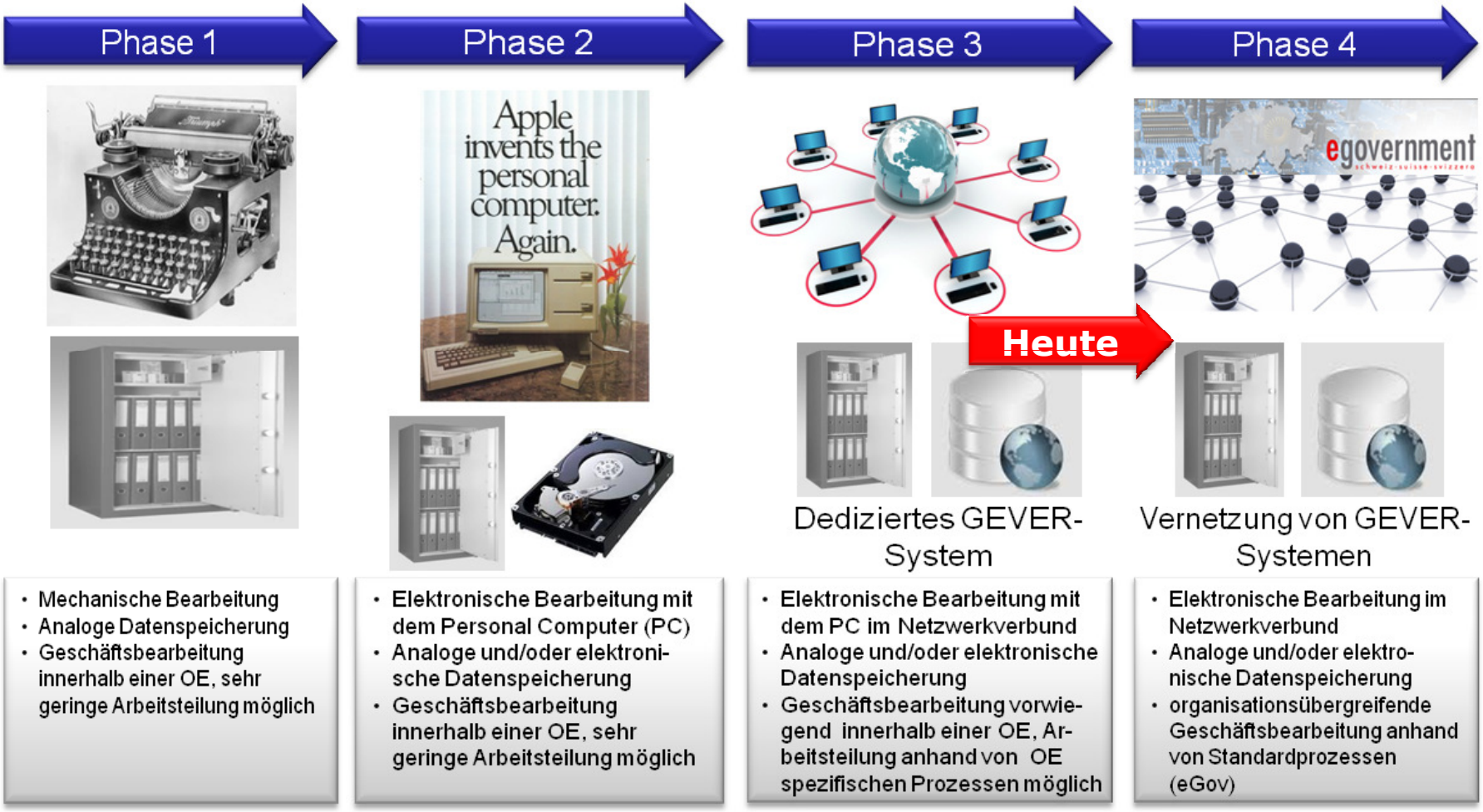
Quelle: http://www.parlament.ch/d/suche/seiten/geschaefte.aspx?gesch_id=20124139

eGovernment-Strategie Schweiz

- Die **Wirtschaft** wickelt den Verkehr mit den Behörden elektronisch ab
- Die **Behörden** modernisieren ihre Geschäftsprozesse und verkehren untereinander elektronisch
- Die **Bevölkerung** wickelt die wichtigen Geschäfte mit den Behörden elektronisch ab

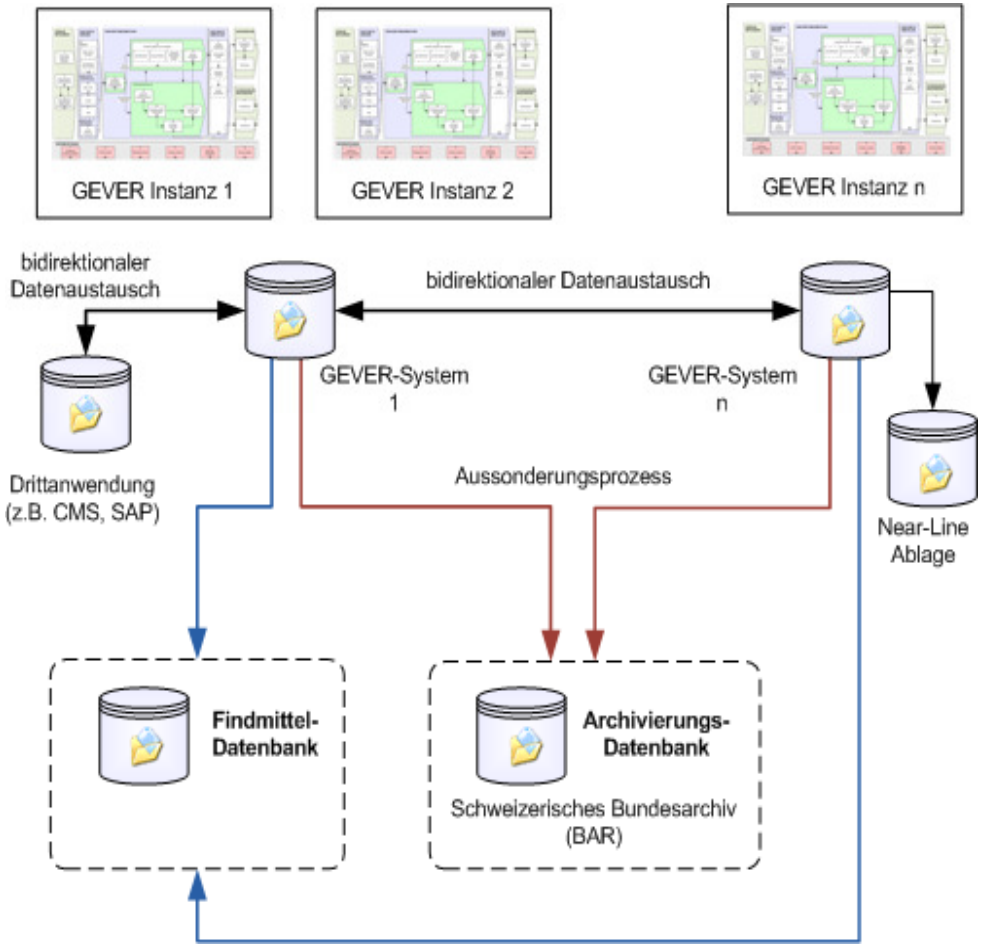
Quelle: E-Government-Strategie Schweiz vom 24. Januar 2007

Die Evolution in der Arbeitsverrichtung und ihre Auswirkungen.



Quelle: Beat Siegrist, Programm GEVER Bund

Vision von GEVER als Gesamtsystem im Endausbau

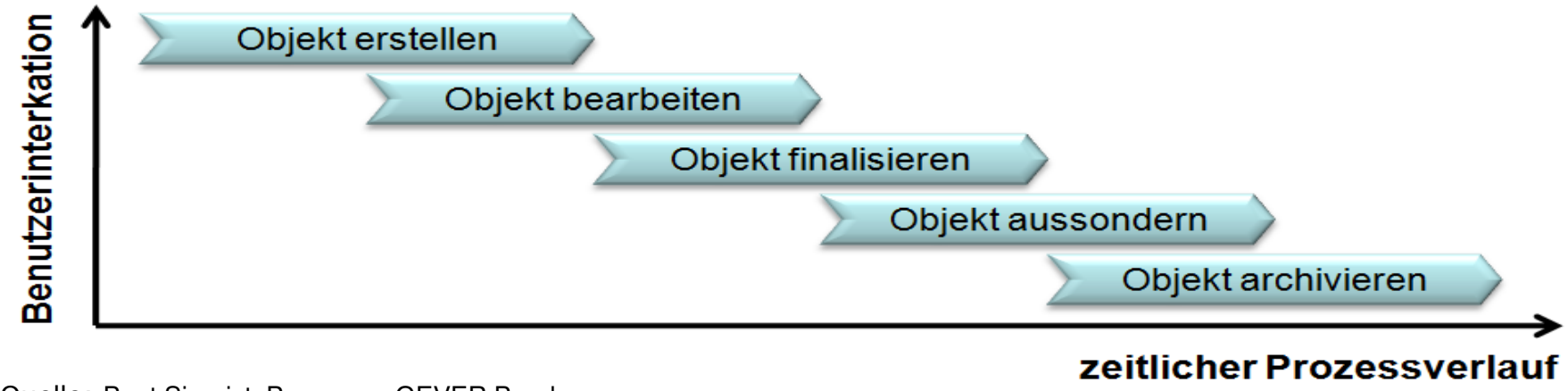


Eine vollständige system-technische **Vernetzung** von unterschiedlichen GEVER-Systemen und Drittanwen-dungen. Einbezug von **Online Business Services** für eine nahtlose, zuver-lässige und wirtschaftliche **Prozessorientierung**, ein-schliesslich Automatisierung entlang der Wertschöpfungs-prozesse über die Organi-sationseinheiten hinaus

Quelle: Beat Siegrist, Programm GEVER Bund

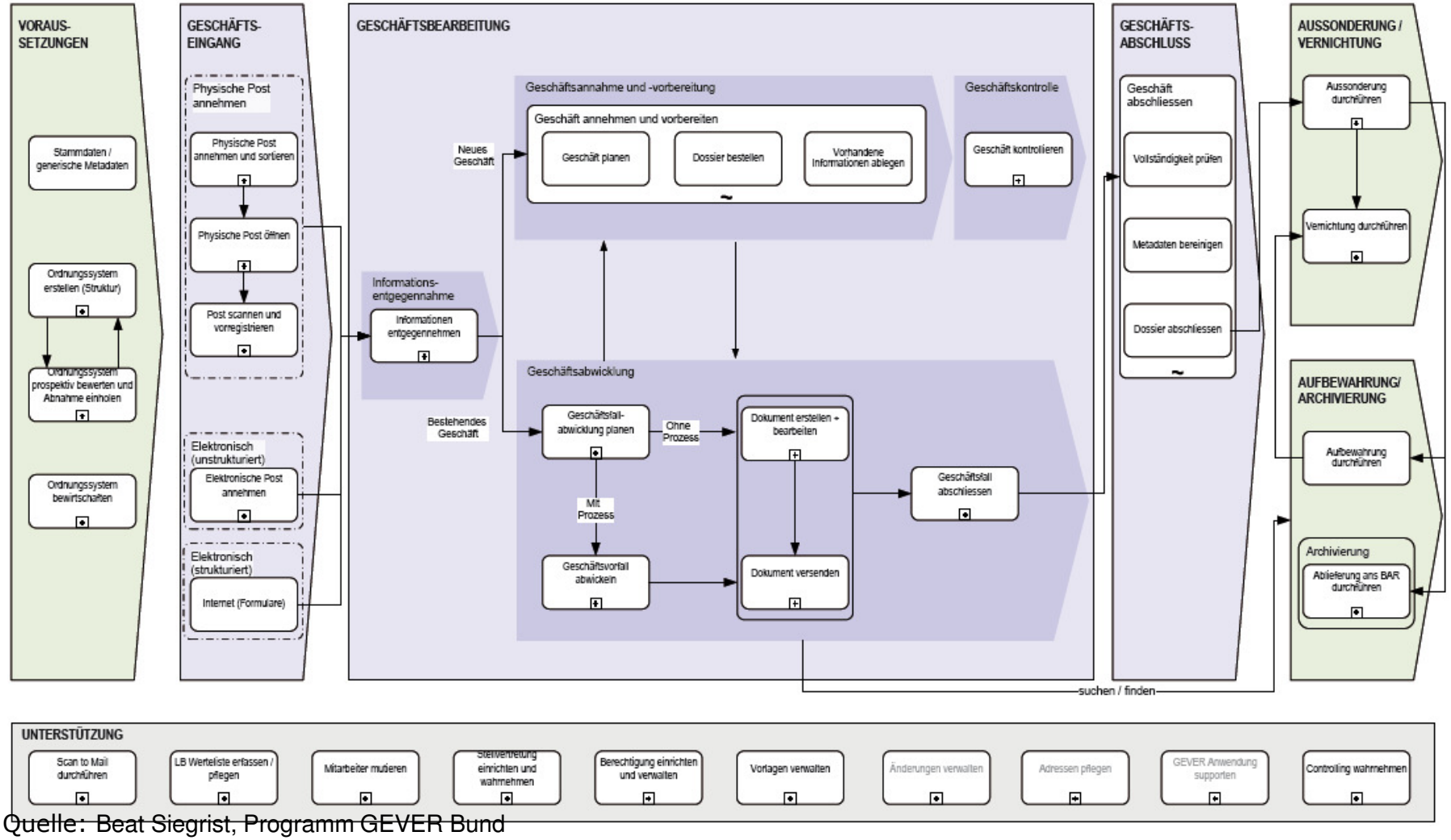
Integrale Sicherheit entlang des gesamten Lebenszyklus eines „Geschäfts“

- Unterschiedlich **klassifizierte Geschäfte** sollen unter Berücksichtigung bestehender Regularien und Standards **sicher** und **nachvollziehbar** in einem GEVER-System bearbeitet werden können
- Die **Informationssicherheit** bestehend aus der **Datensicherheit** sowie dem **Daten- und Informationsschutz** ist über den ganzen **Lebenszyklus** eines Geschäfts zu gewährleisten



Quelle: Beat Siegrist, Programm GEVER Bund

Informationssicherheit ist vital ! - Das GEVER-Verfahren oder die Geschäftsarchitektur.



Quelle: Beat Siegrist, Programm GEVER Bund

"eCH-0039" - Sicherheit im Transportmittel

- Das Transportmittel muss die sichere Übermittlung einer Nachricht gewährleisten. Insbesondere müssen:
  - die **Authentizität des Absenders**
  - die **Integrität des Inhaltes** der Nachricht (Unveränderbarkeit, unbefugte Einsichtnahme) sowie
  - der **Nachweis der Umstände des Austauschvorganges** (z.B. Zeitpunkt des Versandes resp. der Entgegennahme) garantiert oder nachgewiesen werden können

Agenda

- Ausgangslage
- **Informationssicherheit**
- ISO 27001
- Ihre Fragen

Schutz von Informationen

Informationen…

- … **sind Werte**, die (wie auch die übrigen Geschäftswerte) wertvoll für eine Organisation sind und deshalb in geeigneter Weise geschützt werden müssen.

- … sollten deshalb - unabhängig von ihren Erscheinungsform sowie Art der Nutzung und Speicherung - immer angemessen geschützt werden.

Quelle: ISO/IEC 17799:2005, Einleitung

Informationssicherheit

- Eigenschaften von informationsverarbeitenden und -lagernden Systemen, die die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** sicherstellen.

- Informationssicherheit dient dem **Schutz** vor Gefahren bzw. Bedrohungen, der **Vermeidung** von Schäden und der **Minimierung** von Risiken.

- In der Praxis orientiert sich die Informationssicherheit heute unter anderem an der ISO/IEC Standard-Reihe 2700x aber auch zunehmend an ISO/IEC 15408 bzw. Gemeinsame Kriterien zur Evaluierung von IT-Sicherheit (bzw. Common Criteria).

Informationssicherheit ist gefährdet ...

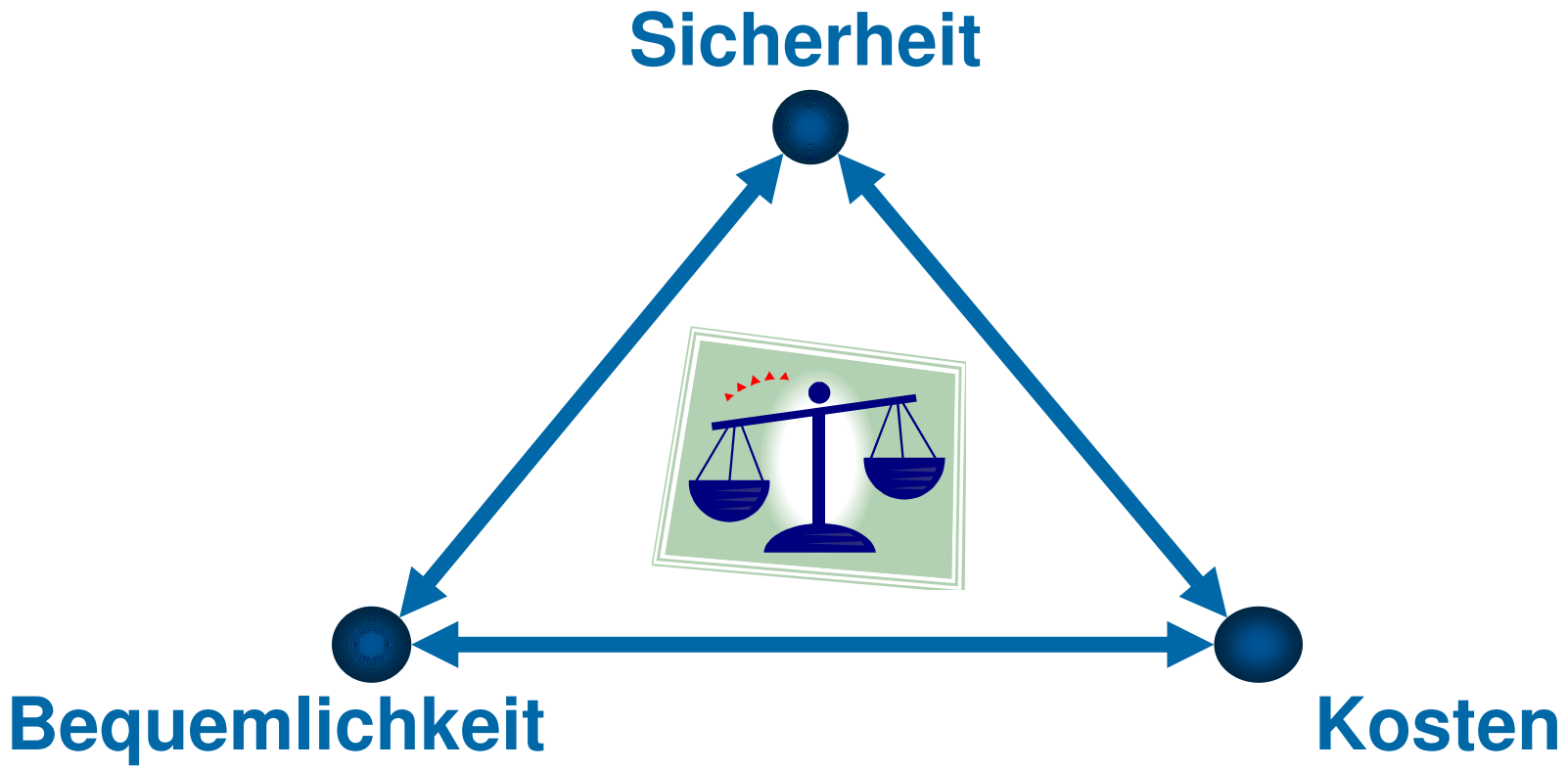
- **Höhere Gewalt**:
  - Feuer, Wasser, Blitzschlag, Krankheit, …
- **Organisatorische Mängel**:
  - Fehlende oder unklare Regelungen, fehlende Konzepte, ...
- **Menschliche Fehlhandlungen**:
  - "Die größte Sicherheitslücke sitzt oft vor der Tastatur„
- **Technisches Versagen**:
  - Systemabsturz, Plattencrash, ...
- **Vorsätzliche Handlungen**:
  - Hacker, Viren, Trojaner, ...

Informationssicherheit lohnt sich ...

- **Optimierung der internen Prozesse** führt zu einem geordneten, effektiven und effizienten Betrieb
  - ➔mittelfristige Kosteneinsparungen
- **Erhöhung der Attraktivität** für Kunden und Geschäftspartner mit hohen Sicherheitsanforderungen
- **Mitarbeiter** identifizieren sich mit Sicherheitszielen und sind stolz auf das Erreichte
- **Versicherungen** honorieren zunehmend Sicherheit

Informationssicherheit im Spannungsfeld unterschiedlicher Interessen

„Suchen Sie sich zwei davon aus!“



Informationssicherheit bedeutet...

- **Wissen**
  - Vitale Prozesse und Daten, Anwendungen, Systeme, Schlüsselpersonen, Kommunikationsverbindungen, Räume
  - Ziele, Schutzbedarf
- **Management und Organisation**
  - Sicherheitsmanagement
  - Sicherheitskonzept
  - Organisation
  - Personal
  - Notfallvorsorge
- **Technik**
  - Sicherung der Infrastruktur
  - Standardsicherheitsmaßnahmen für Standardkomponenten

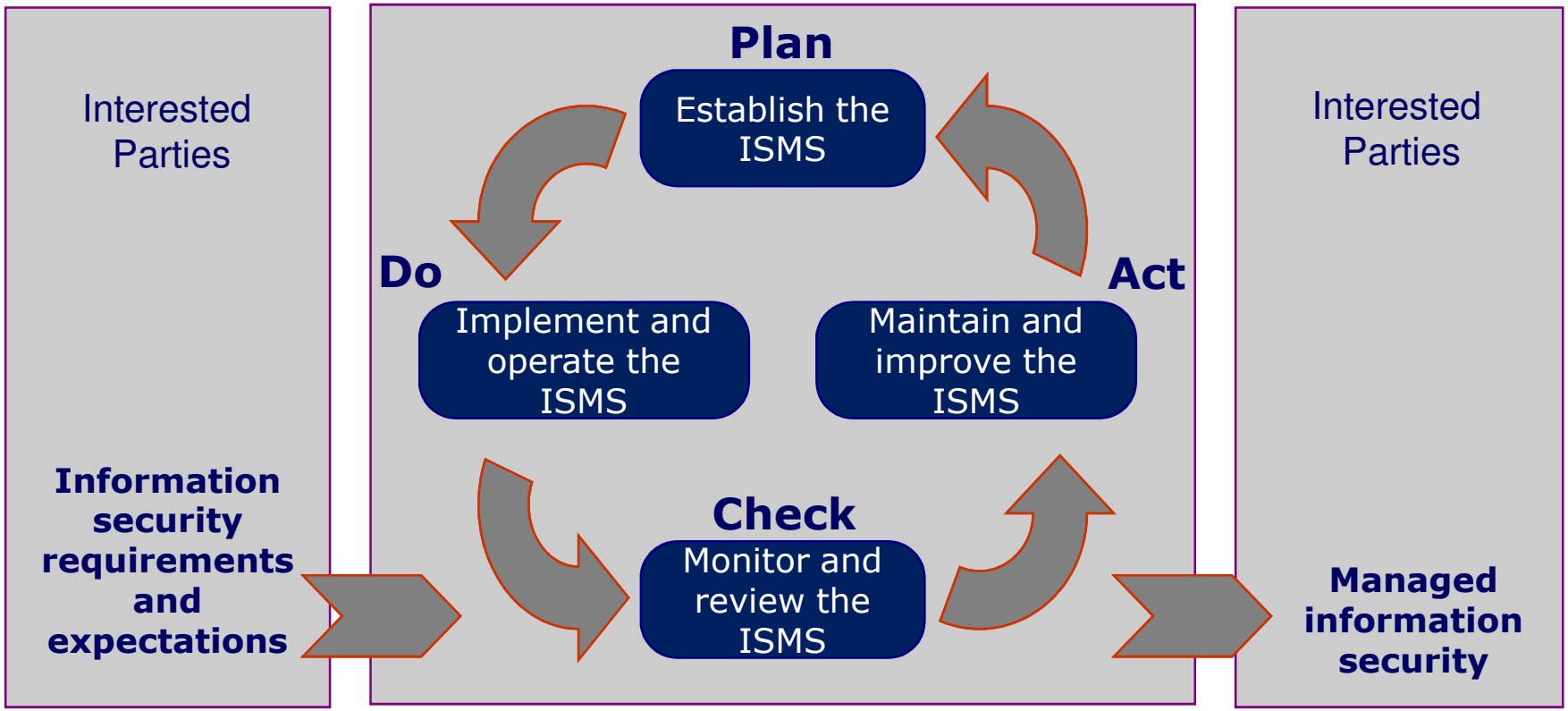
Agenda

- Ausgangslage
- Informationssicherheit
- **ISO 27001**
- Ihre Fragen

ISO/IEC 27001 auf einen Blick

- "Information Security Management Systems – Requirements"
  - spezifiziert Anforderungen an Informationssicherheits-Managementsysteme (ISMS)
  - ist anwendbar in Organisationen jeglicher Art, Ausprägung und Größe
  - kann als Grundlage für Vertragsbeziehungen zwischen Organisationen benutzt werden
  - erlaubt die Implementierung und den Betrieb von integrierten Managementsystemen für Informationssicherheit (ISO 27001), Qualität (ISO 9001), Umwelt (ISO 14001) und Risikomanagement (ISO 31000)

ISO/IEC 27001 in der Praxis Projektablauf



ISMS : Information Security Management System

ISO/IEC 27001 in der Praxis

"We don't pay much attention to information security.
We're hoping our competitors will steal our ideas
and become as unsuccessful as we are."

Quelle: Cartoon @ Randy Glasbergen

Agenda

- Ausgangslage
- Informationssicherheit
- ISO 27001
- **Ihre Fragen**