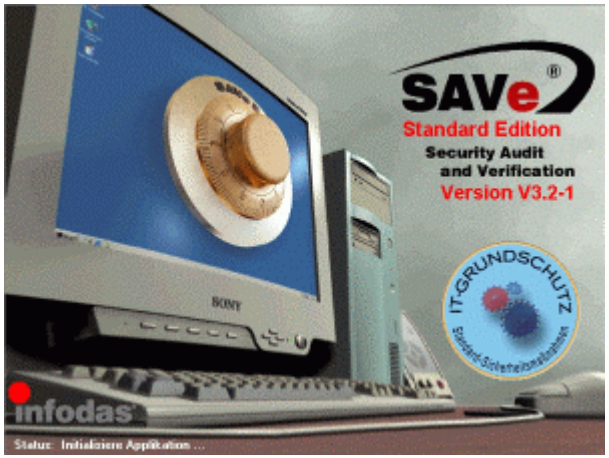
Prozessorientiertes IT-Sicherheitsmanagement auf der Basis von ITIL

Frank Reiländer, Berater IT-Sicherheit/Datenschutz
IT Security & Risk Management, INFODAS GmbH
f.reilaender@infodas.de www.save-infodas.de
☎(0221) 7 09 12-85

Überblick

- ITIL – Motivation
  - Zielsetzung
  - Grundbegriffe
  - Struktureller Aufbau
- Das drei Ebenen-Prozessmodell
  - Business Perspective
  - Service Delivery
  - Service Support
- Integration von IT-Sicherheit mit ITIL
  - Beispiele für einzelne Prozesse
  - Security SLAs
  - Abbildung auf IT-Grundschutzbausteine



Probleme bei der Aufgabenerfüllung von Service-Dienstleistern

- Unklare oder fehlende Zielsetzungen
- Unrealistische Erwartungen; unrealistische Versprechen
- Unterschätzter Zeit- und Personal-aufwand beim Vertragsmanagement
- Unzureichende Definition von Auf-tragsumfang, Servicelevel und Preis
- Qualität und Kundenservice schlecht
- Geschäft und Technologie ändern sich in unvorhergesehener Weise

Intention – Originäres IT -Denken

- Methodische Grundlage für den Aufbau einer prozess- und dienstleistungsorientierten IT–Organisation
- Fokus auf den Themen des IT–Service Managements

ITIL beschreibt, was zu tun ist (und nicht wie) !

ITIL – Grundbegriffe

- ITIL → Information Technologie Infrastructure Library
  - Prozessmodell für die Gestaltung einer dienstleistungsorientierten Informationsverarbeitung
  - Library (Bibliothek) besteht aus 45 Büchern
  - Ziel: Umgestaltung einer produktorientierten IT-Organisation in eine IT-Service-Management-Organisation
  - IT Infrastructure beschreibt Räumlichkeiten, elektrische Versorgung, Telefon, Netze, Hardware, Software, IT Services und Dokumentationen
- Best Practice for IT → Entwicklung Ende der 80er Jahre durch die CCTA (Central Computer and Telecommunications Agency)
  - Zunächst Host-basierter Ansatz
  - Später Qualitätssicherungsstandard auch für Client-Server-Systeme

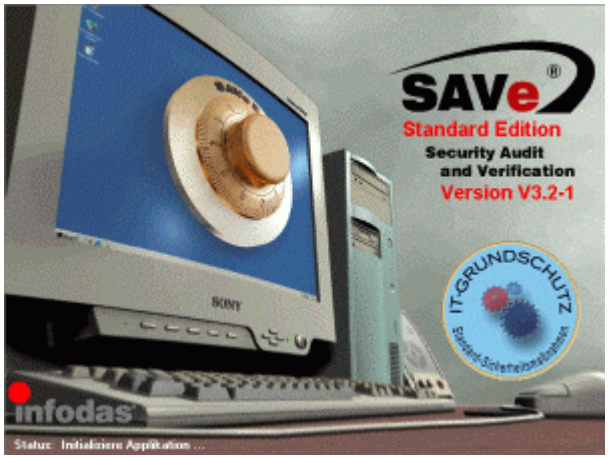
ITIL – Merkmale

- De-facto-Standard
  - Herausgeber: Office of Government Commerce (OGC)
  - Rahmenwerk beschreibt in 7 Bänden 10 Kernprozesse
- Knowledge Management
  - Seit Ende der 80er Jahre kontinuierlich aufgebaut
  - Seit 1985 in Deutschland, Österreich und der Schweiz eingeführt
  - (Hersteller-)Unabhängigkeit
  - Basis für viele andere Referenzmodelle
  - Fachlich fundiert
- Frei verfügbar / nicht proprietär
  - ITIL ist allerdings Eigentum der britischen Regierung

ITIL - Publication Framework

Quelle: OGC

Überblick

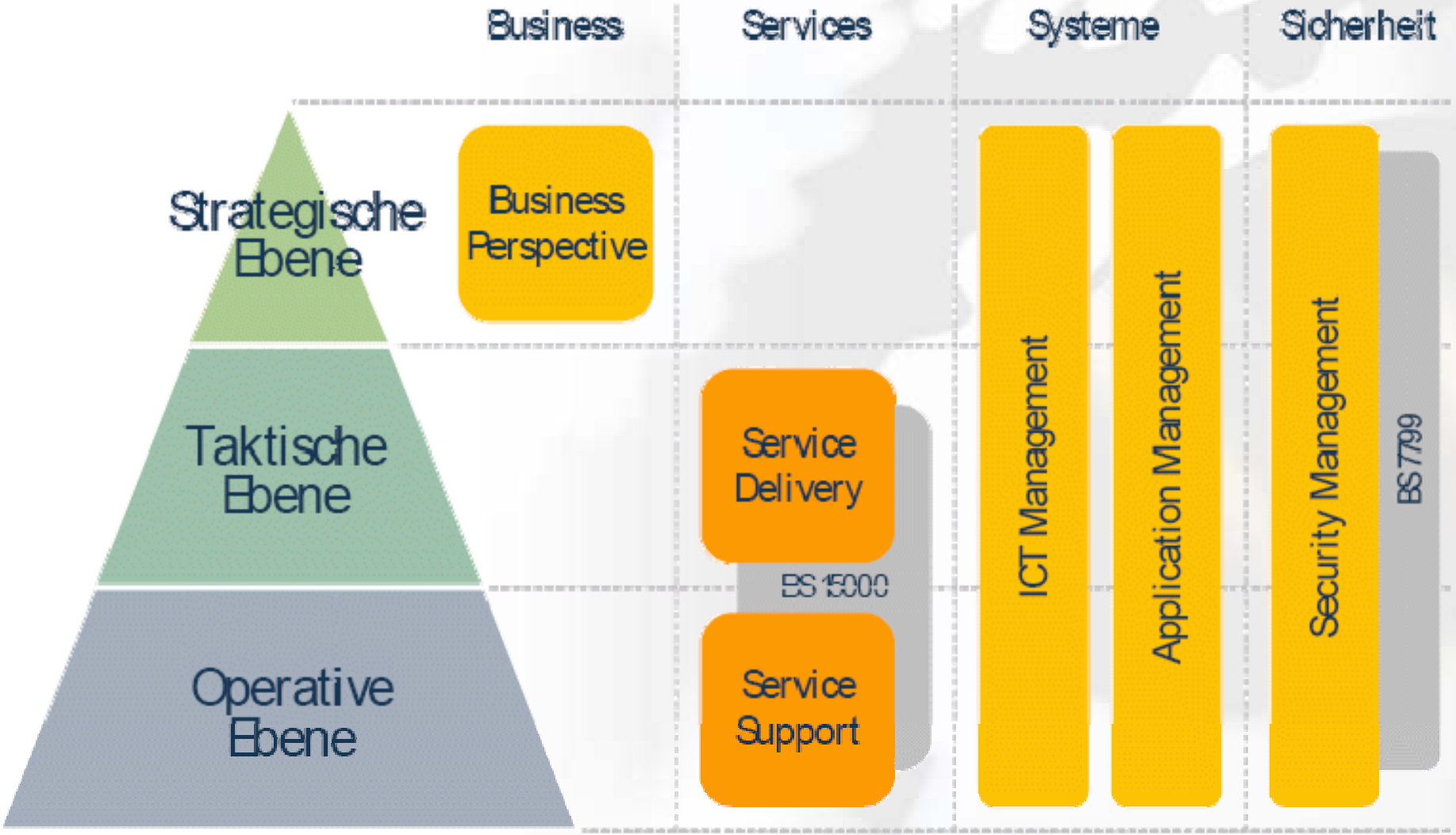


- ITIL – Motivation
  - Zielsetzung
  - Grundbegriffe
  - Struktureller Aufbau
- Das drei Ebenen-Prozessmodell
  - Business Perspective
  - Service Delivery
  - Service Support
- Integration von IT-Sicherheit mit ITIL
  - Beispiele für einzelne Prozesse
  - Security SLAs
  - Abbildung auf IT-Grundschutzbausteine

ITIL – die drei Ebenen

- Management-Ebene (Strategical Layer)
  - Erfolgspotentiale schaffen (Produkte, Marktpotentiale, Mitarbeiter)
    - The Business Perspective
    - Planing to implement Service Management
- Führungs-Ebene (Tactical Layer)
  - Erfolgspotentiale nutzen (Umsetzung der Strategie)
    - Application Management
    - Security Management
    - Service Delivery
- Prozess-Ebene (Operational Layer)
  - Koordination der der Prozesse
    - ITC Infrastructure Management
    - Service Support

ITIL - Gliederungsebenen



Anforderungen an das IT Management – The Business Perspective

- Business Continuity Management (Notfallvorsorge und Notfallmanagement)
- Partnerschaften und Outsourcing
- Änderungsmanagement
- Gestaltung der IT-Service-Organisation
- Planung und Steuerung von IT-Services
- Qualitätsmanagement für IT-Services
- Business- und Management-Fähigkeiten
- Kundenbeziehungsmanagement

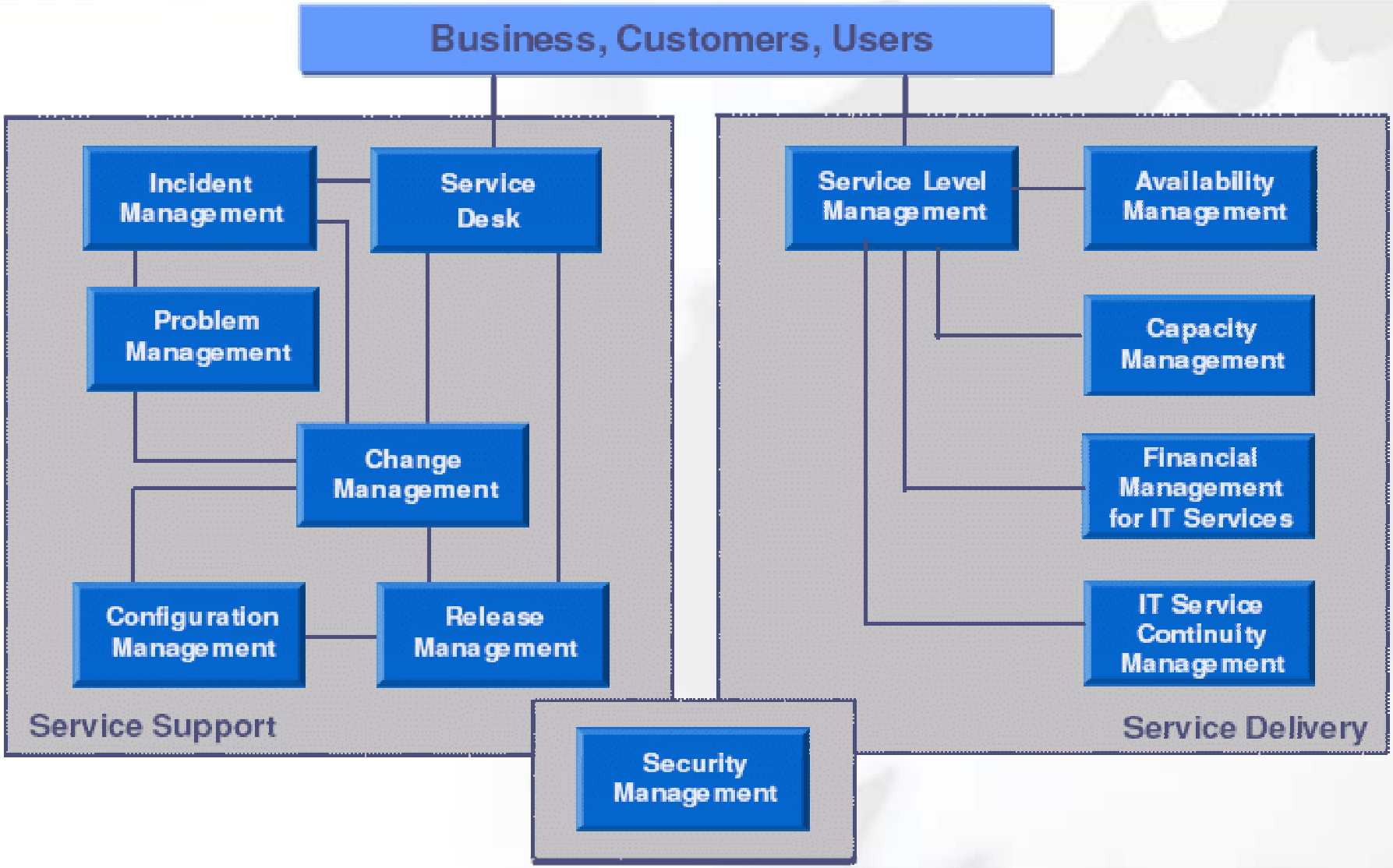
Service Delivery – die taktischen Prozesse

- Service Level Management
  - Service-Kataloge, Vertragsmanagement, Reporting
- Finanzmanagement (Financial Management for IT-Services)
  - Kostentransparenz, Zuordnungen (TCO), Profit Center
- Verfügbarkeitsmanagement (Availability Management)
  - Einhaltung der Zusagen, Abstimmung mit dem Kunden
- Kapazitätsmanagement (Capacity Management)
  - Ökonomische Planung, Prognosen, Konfliktmanagement bei gemeinsamer Nutzung von Ressourcen
- Kontinuitätsmanagement (IT Service Continuity Management)
  - Identifikation von Risiken, Notfallvorsorge

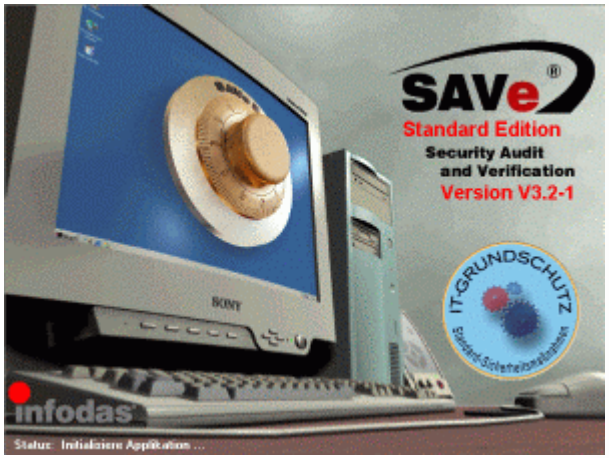
Service Support – die operativen Prozesse

- Störungsmanagement (Incident Management)
  - Wiederherstellen des vereinbarten Services
- Problemmanagement (Problem Management)
  - Fehler gering halten
  - Wiederholtes Auftreten von Störungen verhindern
- Änderungsmanagement (Change Management)
  - Aufeinander abgestimmte Änderungen mit standardisierten Methoden
- Versionsmanagement (Release Management)
  - Einspielen von getesteter Hard- und Software
- Konfigurationsmanagement (Configuration Management)
  - Erfassung, Kontrolle und Verifikation der IT-Komponenten

Service Management und Security Management



Überblick



- ITIL – Motivation
  - Zielsetzung
  - Grundbegriffe
  - Struktureller Aufbau
- Das drei Ebenen-Prozessmodell
  - Business Perspective
  - Service Delivery
  - Service Support
- Integration von IT-Sicherheit mit ITIL
  - Beispiele für einzelne Prozesse
  - Security SLAs
  - Abbildung auf IT-Grundschutzbausteine

Beispiele für ein IT-Sicherheitsmanagement in ITIL

- Availability Management
  - Verfügbarkeit der IT-Komponenten als Globalanforderung
- Business Continuity Planing
  - Notfallplanung (in Abhängigkeit der Verfügbarkeitsanforderungen)
- Performance and Capacity Management
  - z.B. Analyse der Monitoring Daten unter Sicherheitsgesichtspunkten
- Financial Management
  - Kosten von Sicherheitsmaßnahmen (Firewalls, Virenschutz, ...) [ROSI]
- Configuration and Asset Management / Change Management
  - Sicherheitsbewertung sämtlicher CIs (Configuration Items) [IT-GSHB]
- Incident Management

Sicherheitsanforderungen definiert als Security-SLAs

- Zugriffsmethoden und –management (User-ID, Passwort)
- Audits und Logging
- Dokumentation sicherheitsrelevanter Ereignisse
- Verantwortlichkeiten und Pflichten
  - Einhaltung von Bestimmungen
  - Datenschutz
  - Installations- und Wartungsaspekte
  - Rückgabe von Arbeitsmitteln
- Ansprechpartner und Eskalationspfade bei Sicherheitsverletzungen
- Reporting und Verfolgung von Sicherheitsvorfällen
- Sicherheitsschulungen für Administratoren und Benutzer

Abbildung der ITIL-Prozesse auf die IT-Grundschutzbausteine

Baustein	Konfigurations-management	Störungs-management	Service Desk	Problem-management	Änderungs-management	Versions-management	Service Level Management	Verfügbarkeits-management	Kapazitäts-management	IT-Service Continuity	Finanz-management
IT-Sicherheitsmanagement	X					X	X	X			
Organisation	X	X		X	X	X	X	X	X		
Notfallvorsorge-Konzept		X		X			X	X	X	X	
Datensicherungskonzept								X			
Computer-Virenschutzkonzept	X				X	X		X			
Behandlung von Sicherheits-vorfällen		X		X							
Hard- u. Software-Management	X	X	X	X	X	X	X	X	X	X	
Outsourcing	X				X	X	X	X	X	X	
Verkabelung								X	X	X	
Serverraum								X		X	
Heterogene Netze								X		X	
Datenträgeraustausch						X		X			
Standardsoftware	X				X	X					
Archivierung								X	X		
Schutzbedarfsfeststellung[1]	X							X			

Fazit

- ITIL bietet die Möglichkeit, den Sicherheitsprozess nachhaltig zu machen
  - Tätigkeiten werden geregelt (statt Ad-hoc) durchgeführt
  - Sicherheit kann als Service gegenüber Kunden und Mitarbeitern definiert werden
  - SecSLAs beschreiben bspw. die Benutzerverwaltung als Prozess
  - Audit-Prozesse können sich ISMS-Überprüfungen abstützen
- ITIL kann den Sicherheitsprozess zur Chefsache machen
  - Strategische Prozesse werden durch das Management überwacht
  - ITIL liefert ökonomische Begründungen für IT-Sicherheitsmaßnahmen

SAVe® Security Services
Leistungsangebot der INFODAS

Innovative Beratung und Lösungen

- Security Management
- Security Policies und -konzepte
- Datenschutzberatung, externer DSB
- Business Continuity Planning
- IT-Sicherheitsdatenbank
- Schwachstellen- / Penetrationstests
- Sicherheitsaudits / Zertifikatsaudits
  BSI-Grundschutz, Security for Business

Prozessorientiertes IT-Sicherheitsmanagement auf der Basis von ITIL

Vielen Dank für Ihre Aufmerksamkeit!
Ihre Fragen sind unsere Herausforderungen...

INFODAS GmbH, Rhonestraße 2, D-50765 Köln
info@save-infodas.de oder www.save-infodas.de