Von IT-Governance bis COBIT

Jimmy Heschl

Zur Person

bwin.party, COBIT & Justiz
Stiegl
Wirtschaftsinformatik
KPMG
Ernst & Young

Pragmatische
Governance
auf Basis von Standards,
wie COBIT
sichert
verlässlichkeit.

Agenda

- **Vorstellung und Zielsetzung**
- **Überblick über aktuelle Entwicklungen der IT-Governance**
- **Nationale und Internationale Anforderungen an IT-Compliance**
- **Prozessmanagement**
  - ITIL
  - COBIT
  - ISO 27002
  - weitere Standards
  - Integration von COBIT, ITIL, ISO 2700x, CMMI, etc

Ziele

- **Definition IT Governance**
- **Anforderungen**
- **Verantwortungen**
- **Standards für IT Governance**
  - fordernde
  - helfende

Grundregeln

- Dies ist IHRE Lehrveranstaltung!
- Stellen Sie Fragen!
- Unterbrechen Sie wo notwendig!
- Wichtig ist der Inhalt, den Sie mitnehmen, nicht die Zeit!

Leader in online gaming

- World's leading provider of online Sports Betting
- One of the largest Poker networks
- Integrated gaming portal in 22 languages
- Active in 25 core markets
- Elements of success: brand and technology

World-class performance

- >2.4m active customers (FY09)
- EURm 414 gaming revenues (FY09)
- Daily Page Views: >15m
- Daily Unique Visitors (peak): 980.000
- >70.000 payment transactions per day
- Number of servers: 6.500
- Data Centers: 7

Flagship product: Sportsbetting

- **Europe ‘s largest betting line-up**

  - > 90 different sports covered
  - > 14.000 bets offered simultaneously
  - > 1 million placed bets per day
  - 3,000 live events and 800 hours' live sports programming each month

Poker – Casino – Games

- **Europe's largest poker platform**
  - Up to 45.000 concurrent players
  - Poker platform to handle ~ 250k users
  - bwin offers extensive range of Casino games
  - Constantly adding new games to portfolio

IT-Governance

In den Nachrichten…

OÖNachrichten

Hauptausgabe vom 29.12.2003 - Seite 009

Parmalat-Gründer Tanzi drohen

nach Festnahme bis zu 15 Jahre Haft

nicht versagt - Dewitte: "Habe mir nichts z
kommen lassen"

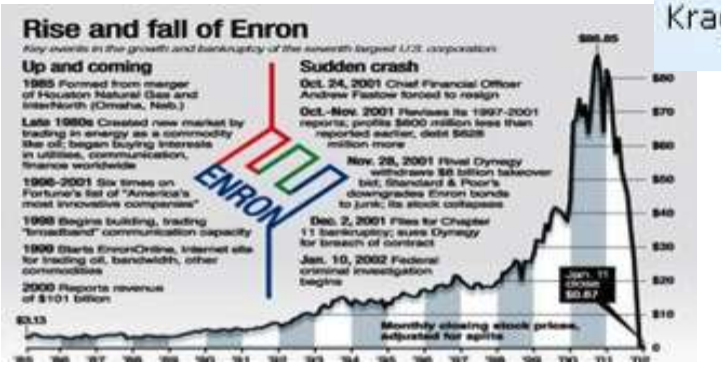
Salzburg - Die Salzburger Landeshauptfrau u
geschäftsführende Präsidentin der Osterfests
Burgstaller, will die Osterfestspiel GmbH in Zu
kontrollieren. Wie am Mittwoch bekanntegegel
künftige Geschäftsführung sämtliche wirtscha

Donnerstag, 14. Juli 2005

Tränen beim Ebbers-Urteil

Zittern in den Chef-Etagen

Gewaltiger Donner krachte vom New Yorker Himmel, als der ehemalige WorldCom-Chef und Millionär Bernard Ebbers (63) am Mittwoch zu 25 Jahren Haft verurteilt wurde – ein dramatischer Backgroundsound zum vorläufigen Höhepunkt der Serie amerikanischer Wirtschaftsprozesse. Es war die höchste Gefängnisstrafe, die bislang gegen Verbrecher "mit weißem Kragen" (white collar), wie es auf Englisch heißt, verhängt wurde.



OÖNachrichten

Bilanzskandal in Japan löste ein weltweites Börse-Beben aus

19.01.2006

TOKIO. Die Betrugsaffäre bei einer japanischen Internet-Firma hat die Anleger in Tokio gestern in Panik versetzt. Die Auswirkungen waren weltweit zu spüren. Auch in Wien gab es kräftige Kursverluste.

Unternehmen auf dem Weg ins 21. Jhd

Ruf nach strengen gesetzlichen Regelungen

Debatte um Corporate Governance

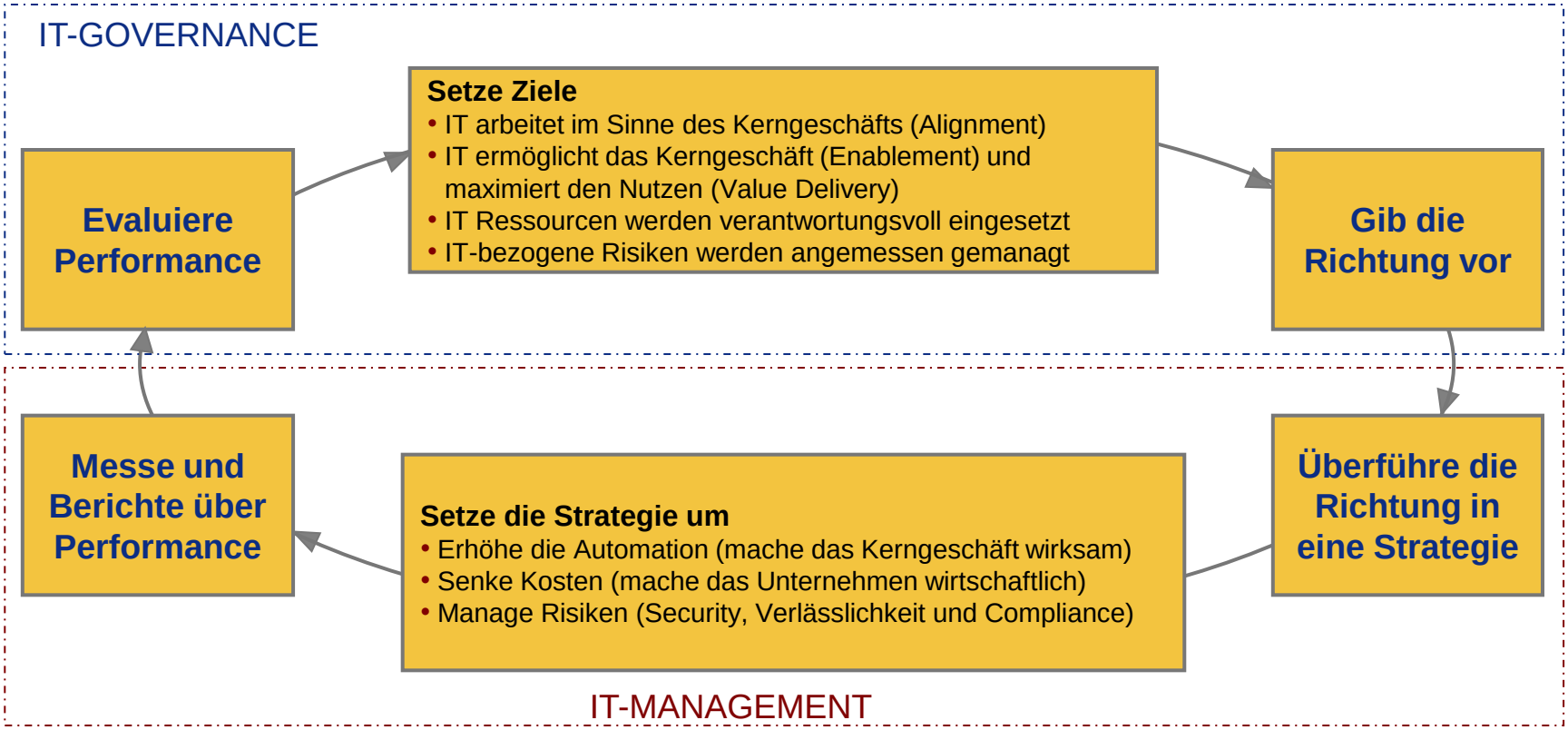
Forderung nach integriertem internem Kontrollsystem

Schlanke / dezentrale Unternehmenseinheiten verlangen systematische interne Kontrollsysteme!

Was ist IT-Governance?

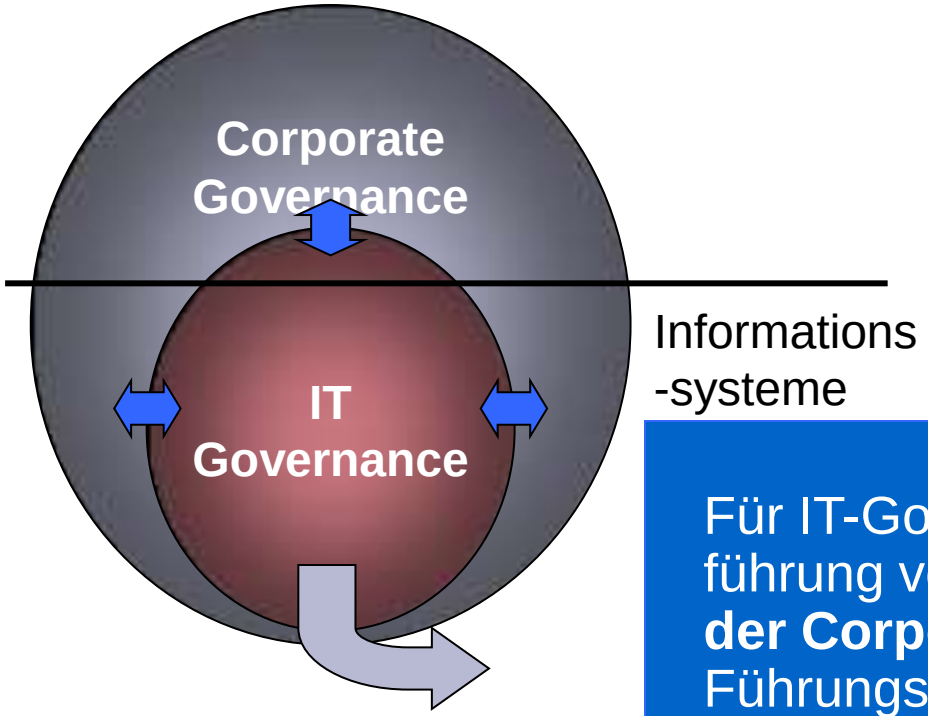
- **Ursprung**
  - griechisch: kybernân
  - Ein Schiff führen / leiten

Was ist IT-Governance?



- Ziel: sicherstellen, dass die IT die Geschäftsstrategien und -ziele unterstützt und vorantreibt
- Methode: Führungs- und Organisationsstrukturen sowie Prozesse
- Verantwortung: Vorstand und Geschäftsführung

IT-Governance: Eine Definition



Für IT-Governance sind Vorstand und Geschäfts-führung verantwortlich. Sie ist **integraler Bestandteil der Corporate Governance** und besteht aus Führungs- und Organisationsstruk-turen sowie Prozessen, die sicherstellen, dass IT die Geschäftsstrategien und -ziele unterstützt und vorantreibt.

— IT Governance Institute

IT-Governance – Warum?

- § 81 AktG: Bericht des Vorstands an den Aufsichtsrat
- § 82 AktG / § 22 GmbHG: Internes Kontrollsystem
- § 131 BAO: Ordnungsmäßigkeit der Buchführung
- § 38 BWG: Bankgeheimnis
- § 39 BWG: Sorgfaltspflicht und ORM
- § 14 DSG: Datensicherheitsmaßnahmen
- § 15 DSG: Anordnung durch den Arbeitgeber
- Emittenten-Compliance-Verordnung – ECV
- Corporate Governance Codex
- KonTraG
- HIPAA
- ...

Gefordert in unterschiedlichen Gesetzen

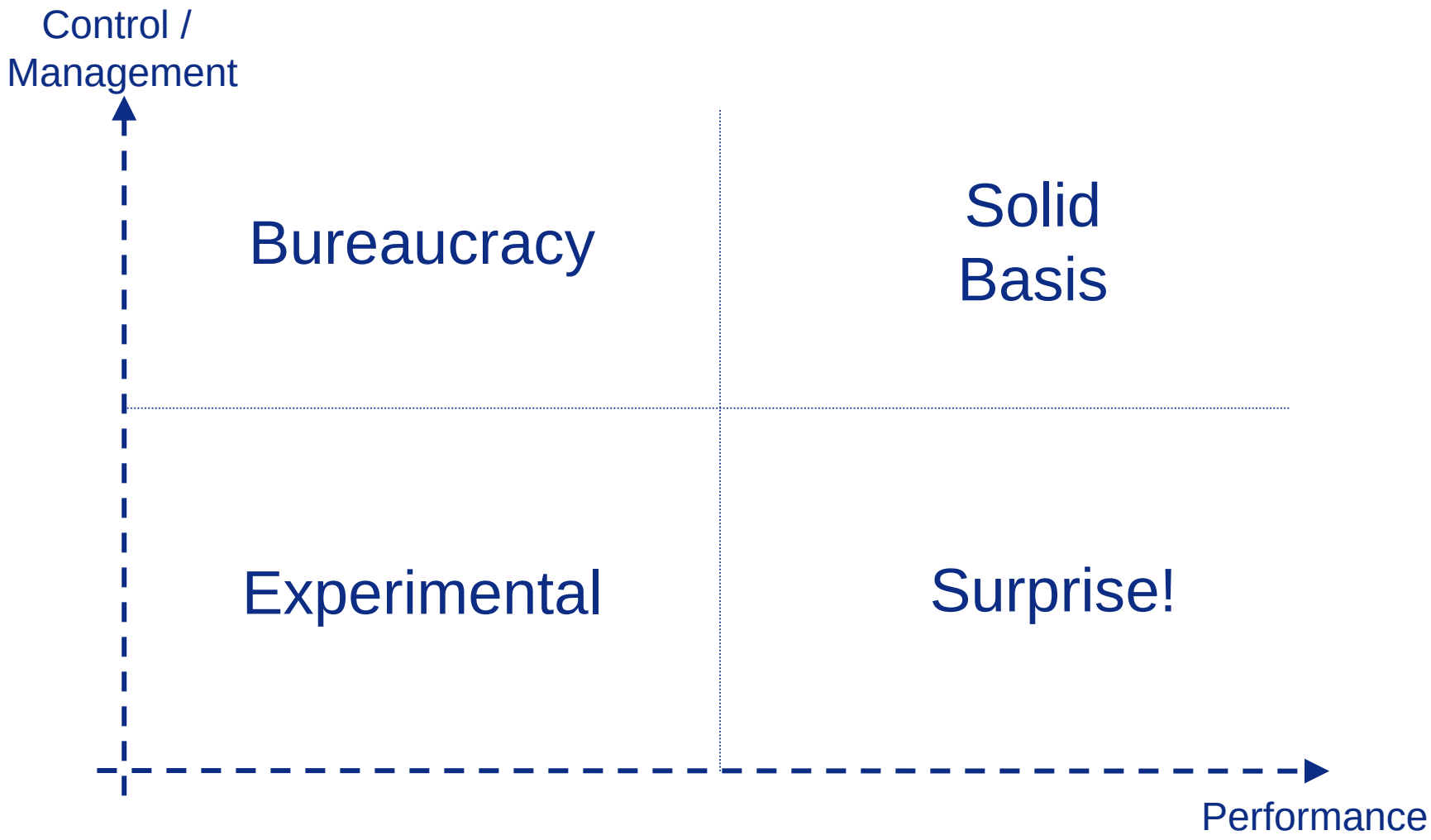
- **§ 82 AktG und § 22 GmbHG fordern die Einführung eines internen Kontrollsystems**
  - „Der Vorstand hat (Die Geschäftsführer haben) dafür zu sorgen, dass ein Rechnungswesen und ein **internes Kontrollsystem** geführt werden, die den Anforderungen des Unternehmens entsprechen.“
- **Sarbanes-Oxley Act (USA)**
  - J-SOX
  - K-SOX
  - CAN-SOX
  - …
- **8. EU Audit-Richtlinie**
- **URÄG (Unternehmens-Rechts-Änderungs-Gesetz**

Nutzen und Bedeutung interner Kontrollsysteme

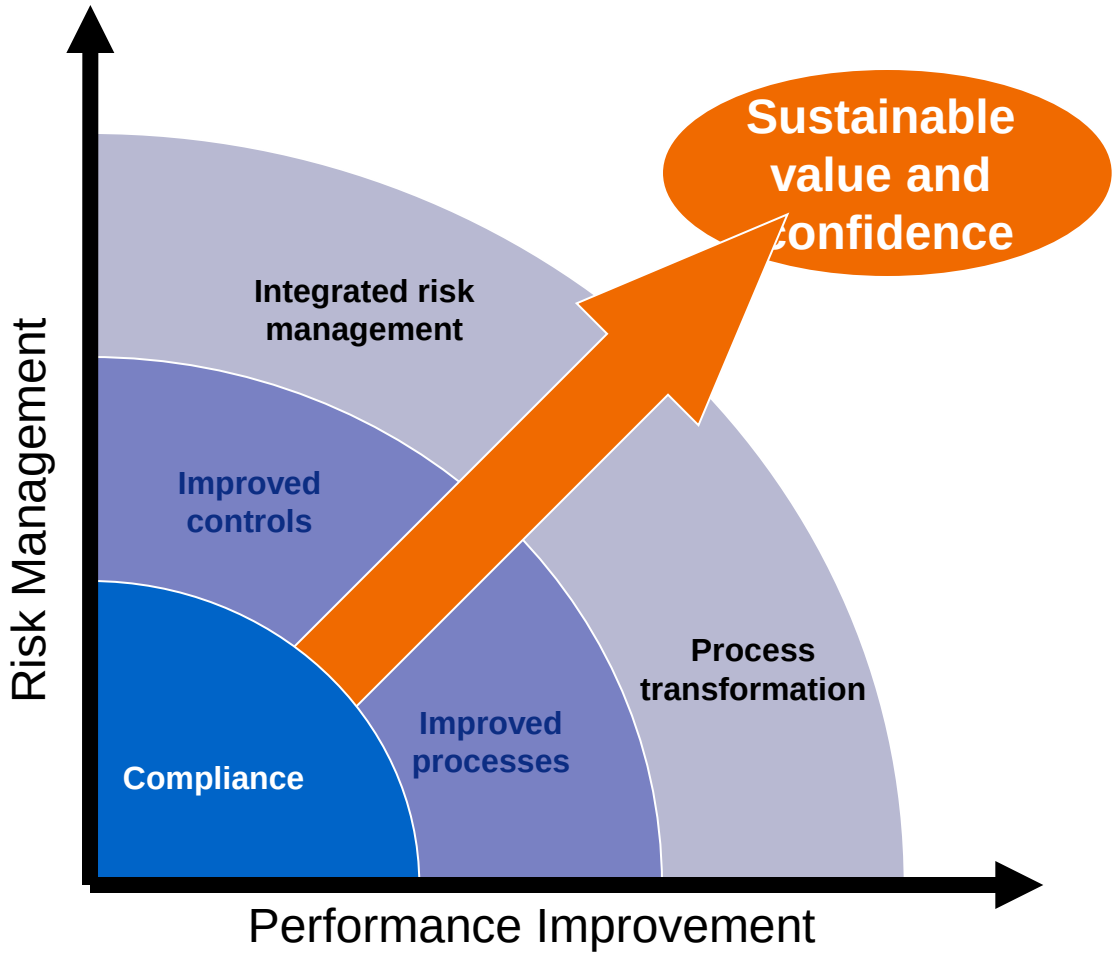
Unter einem **internen Kontrollsystem** wird die Gesamtheit aller Grundsätze, Methoden und Maßnahmen verstanden, die den ordnungsgemäßen Ablauf sämtlicher im Unternehmen stattfindenden Transaktionen und Handlungen sicherstellen soll.

- **Ziele eines internen Kontrollsystems sind**
  - **Sicherung des Vermögens** und **Aufdeckung von Vermögensschädigungen**
  - **Wirtschaftlichkeit** des unternehmerischen Handelns
  - **Ordnungsmäßigkeit aller betrieblichen Abläufe** im Hinblick auf die Einhaltung interner wie externer Regelwerke
- **Ein internes Kontrollsystem**
  - **verringert die Fehleranfälligkeit** von Transaktionen im Unternehmen
  - hält die Möglichkeit für **Betrug** am Unternehmen möglichst gering
  - sichert die **Wirtschaftlichkeit** des unternehmerischen Handelns
  - gewährleistet die **Übereinstimmung** sämtlicher Abläufe im Unternehmen mit der Satzung oder dem Gesellschaftsvertrag, den Unternehmensrichtlinien und den geltenden Gesetzen **(Compliance)**
  - verhindert, dass sich das Unternehmen **unnötigen Risiken** aussetzt

Optionen für IT-Governance



Performance vs. Control



Legislation is forcing the pendulum toward the Risk Management axis

Competition and market pressures are forcing the pendulum toward the Performance Improvement axis

Good IT Governance can help an organization balance risk management and performance improvement forces.

IT Governance – Warum?

- **Fragen des Aufsichtsrat bezüglich IT**
  - Verfolgen wir die richtigen Vorhaben?
  - Verfolgen wir die Vorhaben richtig?
  - Werden die Aufgaben gründlich erledigt?
  - Wird effizient gearbeitet?
  - Bestehen Risiken, die wir nicht kennen?
  - Was passiert mit den Ressourcen, die für IT bereitstehen?
- **Druck auf das Unternehmen und die IT**
  - Kostenkürzung, höhere Profite und Marktanteil
  - Höhere Funktionalität und einfachere Bedienung
  - Höhere Verantwortung bezüglich Datenschutz, etc.)

IT Governance – Warum?

- Ihr Unternehmen ist durchdrungen mit IT
- Die IT ist kritisch für Ihren Unternehmensfortbestand
- Die IT ist Strategischer Erfolgsfaktor
- Die Erwartungen an die IT und die Realität sind diskrepant
- Der Stellenwert der IT ist unterbewertet
- IT bedeutet hohe Investitionen und hohes Risiko

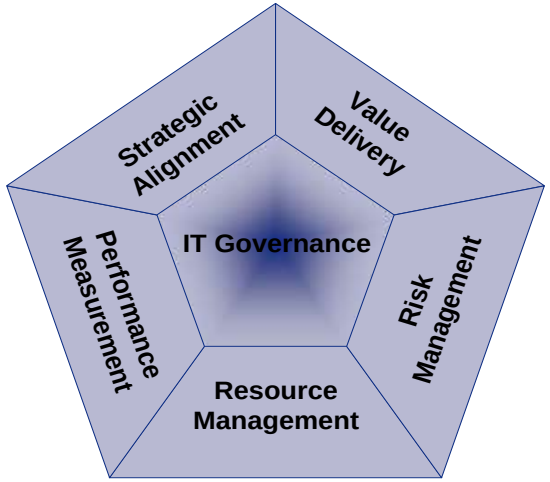
IT Governance – Aufgaben

- **Aufgaben des Vorstandes**
  - Herunterbrechen der Unternehmensstrategie und -ziele für die IT
  - Organisatorische Ausrichtung der IT – Prozessorientierung
  - Aufbau und Unterhalt des internen Kontrollsystems in der IT
  - Messung der Zielerreichung

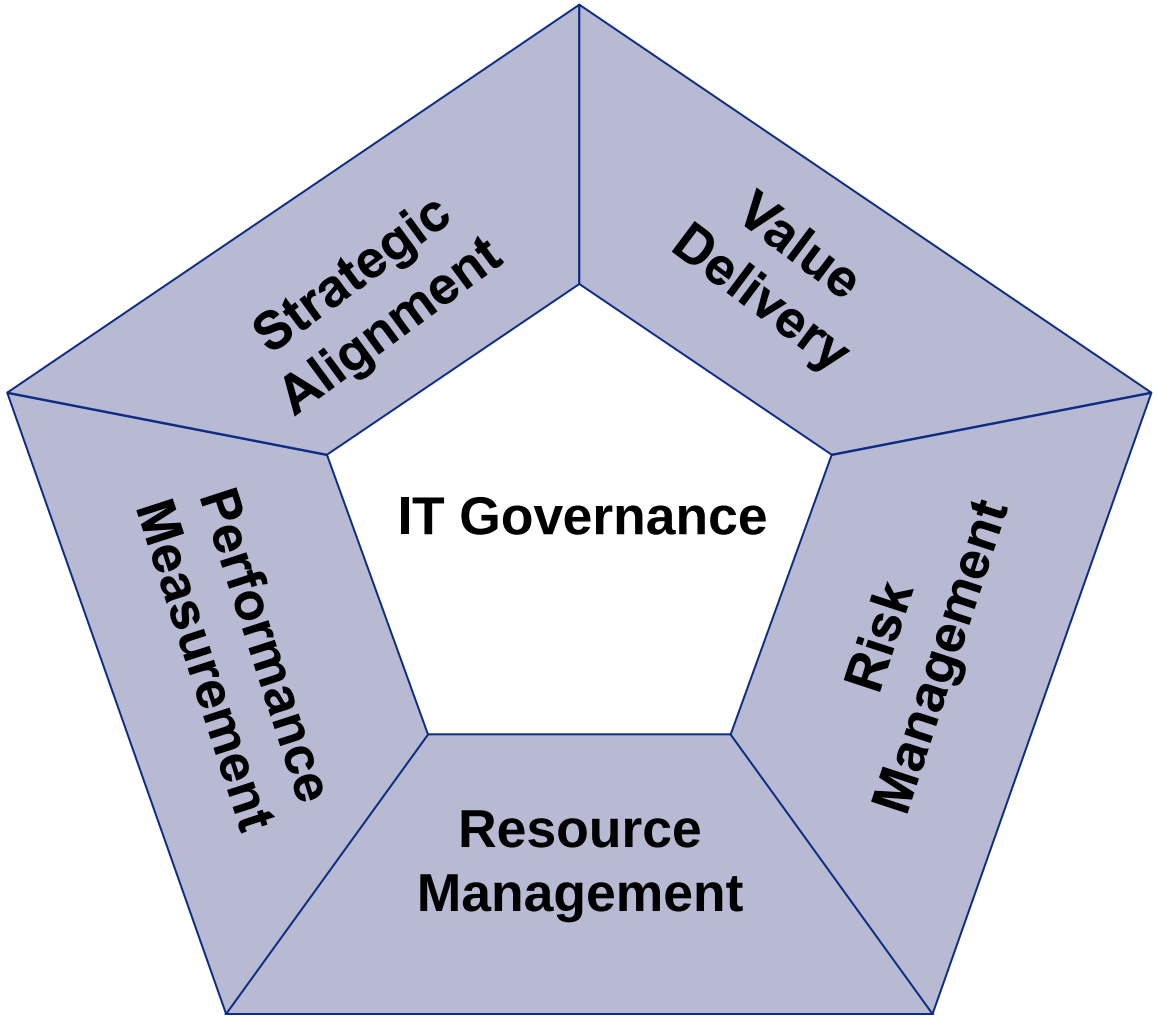
Prioritäten der Analysten

- Gartner
- CSC
- Compass
- Giga
- AICPA/CICA
- CIO Magazine
- Technology Council

- Strategic Alignment
- Value Delivery
- IT Asset Management
- Risk Management
- Performance Measurement

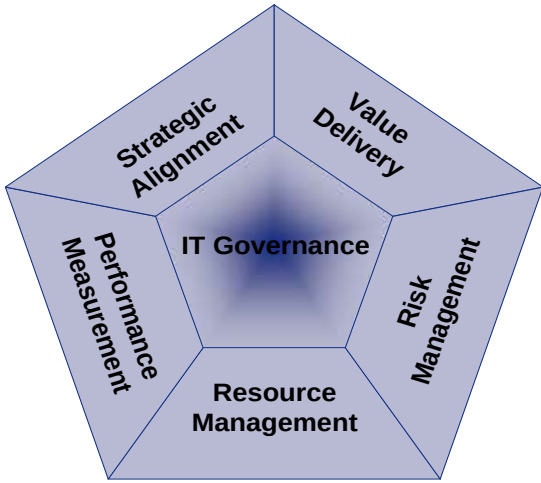


IT Governance Focus Areas



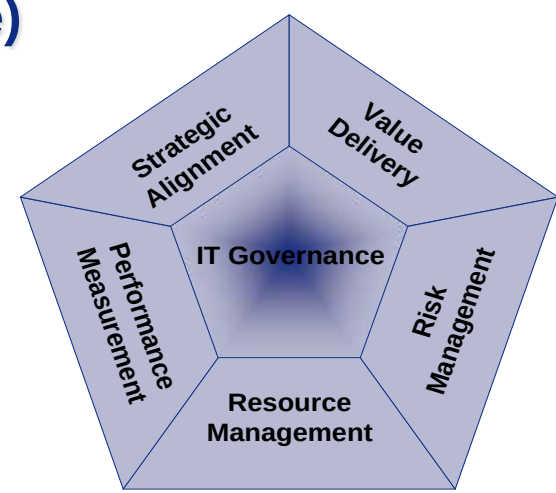
IT Governance Focus Areas (1)

- **Strategic Alignment (Strategische Ausrichtung)**
  - Sicherstellung des Verbunds von Unternehmens- und IT Zielen
  - Festlegung, Beibehaltung und Validierung des Wertbeitrags
  - Abgleich zwischen operativen Betrieb des Unternehmens und jenem der IT
- **Value Delivery (Schaffen von Werten/Nutzen)**
  - Realisierung des Wertbeitrags im Leistungszyklus
  - Sicherstellung, von Generierung des strategisch geplanten Nutzen
  - Kostenoptimierung
  - Erbringung des intrinsischen Nutzen der IT.
- **Resource Management (Ressourcenmanagement)**
  - Optimierung von Investitionen in IT-Ressourcen
  - geregeltes Management von IT-Ressourcen
  - Optimierung von Wissen und Infrastruktur



IT Governance Focus Areas (2)

- **Risk Management (Risikomanagement)**
  - Risiko-Awareness bei der Unternehmensleitung
  - Verständnis über die Risikobereitschaft (engl: risk appetite)
  - Verständnis für Compliance-Erfordernisse
  - Transparenz über die für das Unternehmen wichtigsten Risiken
  - Integration der Verantwortlichkeit für Risikomanagement in der Organisation
- **Performance Measurement (Messen von Performance)**
  - Verfolgen und überwachen der Umsetzung der Strategie und der Umsetzung von Projekten
  - Verwendung von Ressourcen
  - Prozessperformance (Balanced Scorecard)
  - Leistungserbringung (engl: Service Delivery)



Anforderungen

Gesetzestexte

- **§ 190 UGB (ehemals HGB):**
  - Datenträger können verwendet werden…
  - Inhaltsgleiche, vollständige, geordnete Wiedergabe (volle Aufbewahrungsfrist)
- **§ 131 BAO:**
  - Zusammenhang zw. Buchungen und Belegen nachweisbar; Nachweis der Vollständigkeit und Richtigkeit
  - Datenträger können verwendet werden…

Aktiengesetz (AktG)

- **Viele Bestimmungen, die zu Corporate Governance beitragen,**
  - zB § 81 Quartalsberichte und Jahresberichte an den Aufsichtsrat
  - § 92 Ausschüsse für Jahresabschlusserstellung
- **Vorstandsverantwortung für Corporate Governance wird derzeit in § 82 subsummiert:**
  - „Der Vorstand hat dafür zu sorgen [...] dass ein internes Kontrollsystem geführt wird, das den Anforderungen des Unternehmens entspricht“.

GmbHG

- **Bei großen GmbHs gelten die Bestimmungen des AktG über Aufsichtsräte sinngemäß.**
- **Die Verantwortung der Geschäftsführer für Corporate Governance wird in § 22 subsummiert:**
  - „Die Geschäftsführer haben dafür zu sorgen [...] dass ein internes Kontrollsystem geführt wird, das den Anforderungen des Unternehmens entspricht“.

Andere relevante Gesetze

- Datenschutzgesetz
- Fernabsatzgesetz
- BWG / VAG
- Telekommunikationsgesetz
- Signaturgesetz, Signaturverordnung
- eCommerce Gesetz
- eGovernment Gesetz
- Informationssicherheitsgesetz
- Emittenten Compliance Verordnung
- …

DSG-Novelle 2010

- **Umgesetzt**
  - Videoüberwachung
  - Datenschutzkommission
  - Registrierungsverfahren
- **Nicht umgesetzt**
  - Datenschutzbeauftragter
  - Verwendung biometrischer Daten, Ortungssysteme
  - Scoring-Systeme
  - Zutritts- und Prüfrecht für die DSK
  - Rechte von Journalisten
  - Präzisierung der „Datensicherheitsmaßnahmen“ (§14)

DSG § 14 (1) - Datenschutzmaßnahmen

§ 14. (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

DSG § 14 (2) - Datenschutzmaßnahmen

(2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,

1. die **Aufgabenverteilung bei der Datenverwendung** zwischen den Organisationseinheiten und zwischen den Mitarbeitern **ausdrücklich festzulegen**,
2. die Verwendung von Daten an das **Vorliegen gültiger Aufträge** der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
3. jeder **Mitarbeiter** über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu **belehren**,
4. die **Zutrittsberechtigung** zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu **regeln**,
5. die **Zugriffsberechtigung auf Daten und Programme** und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und **jedes Gerät** durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen **gegen die unbefugte Inbetriebnahme abzusichern**,
7. Protokoll zu führen, damit **tatsächlich durchgeführte Verwendungsvorgänge**, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
8. eine **Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen** zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist.

Fachgutachten - Verschiedene herausgebende Organisationen

- **IFAC – International Federation of Accountants**
  - ISA (ISA 402 - Audit Considerations relating to Entities using Service Organizations)
- **AICPA – American Institute of CPAs**
  - SAS (zB SAS 70 - Reports on the Processing of Transactions by Service Organizations)
- **PCAOB – Public Company Accounting Oversight Board**
  - Auditing Standards
- **KFS – Kammer der WT - Fachsenat für Datenverarbeitung**
  - KFS/DV1
  - KFS/DV2
- **IDW – Institut der Wirtschaftsprüfer**
  - PS331 (Serviceorganisationen)
  - FAIT (Fachgutachten für die Prüfung von Informationstechnologie)

KFS/DV 1 – Grundsätze ordnungsgemäßer IT-Buchführungen

- Pflicht zur Führung von Büchern und Aufzeichnungen
- Nachvollziehbarkeit
- Vollständigkeit
- Richtigkeit
- Zeitgerechtheit
- Ordnung
- Unveränderbarkeit
- Inhaltsgleiche, vollständige und geordnete Wiedergabe

vgl. § 190 UGB

+ angemessenes IKS

Was ist relevant?

- Buchführung
  - Hauptbuch
  - die Nebenbücher
  - Aufzeichnungen
  - vorgelagerte oder zuliefernde IT-Systeme, soweit diese buchführungsrelevante Daten erzeugen, weiterleiten oder verarbeiten
  - Jahresabschluss (Konzernabschluss)

Funktionen

- Belegfunktion
- Journalfunktion
- Kontenfunktion
- Dokumentation
- Aufbewahrung

Internes Kontrollsystem

- **Kontrollebenen**
  - IT-Kontrollumfeld
    - Organisation, Richtlinien …
  - Generelle IT-Kontrollen
    - Beschaffung, Zugriffsschutz, Betrieb
  - Anwendungskontrollen
    - manuell, automatisch, Mischform
- **Bereiche**
  - IT-Anwendungen
  - IT-Infrastruktur
  - IT-Organisation
  - IT-Prozesse
- **Sonderthemen**
  - Datenmigration
  - Outsourcing

Österreich KFS/DV 1 – Dokumentation

- **Verfahrensdokumentation**
  - Für Programmentwicklungen, Change Management, Zukäufe von SW (inkl. Customizing/Tabellen-Einstellungen) muss verfügbar sein:
    - Anforderung/Aufgabenstellung
    - Datensatzaufbau
      - Verarbeitungsregeln (inkl. Steuerungsparameter, Tabelleneinstellungen) einschl. Kontrolle, Abstimmungsverfahren und Fehlerbehandlung
      - Datenausgabe
      - Datensicherung
      - Verfügbare Programme
    - Art, Inhalt und Umfang der durchgeführten Tests
    - Freigaben (Zeitpunkt, Unterschrift des Auftraggebers)
    - Versionsmanagement
  - Gilt auch für Datenbanken, Betriebssysteme, Netzwerkkomponenten,…
  - Eventuell können Teile davon auch von externen Dritten zur Verfügung gestellt werden
  - …

Überblick Fachgutachten KFS/DV 2

- Fachgutachten „Die Prüfung der IT im Rahmen von Abschlussprüfungen“
- Erarbeitet durch FS DV
- Gemeinsame Überarbeitung durch FS DV und FS HR
- Verabschiedet im November 2004

KFS/DV 2 - Grundsätze

- **Prüfung der IT ist Teil der Prüfung des Internen Kontrollsystems**
- **Geprüft werden die IT Qualitätsmerkmale**
  - Effektivität
  - Vertraulichkeit
  - Verfügbarkeit
  - Integrität
  - Konformität
  - Wartbarkeit
  - Nicht: Effizienz
- **Risikoorientierte Prüfung**
- **Prüfung von Stichproben**
- **Abhängig von Größe und Komplexität des Unternehmens und der eingesetzten Systeme**

KFS/DV 2 – Grobüberblick über IT Prüfungen

- Gewinnung eines Überblicks über Systeme und Abläufe
- Prüfung der IT Prozesse (anwendungsunabhängige IT Kontrollen), orientiert zB an CobIT
- Prüfung der Anwendungen (anwendungsabhängige IT Kontrollen)

Prüfung von Systemen

- **von besonderer Bedeutung für das Finanz- und Rechnungswesen**
  - Buchhaltungssystem
  - vor- und nachgelagerte Systeme
- **Entscheidungsrelevante Systeme**
  - für Management und Steuerung des Unternehmens
  - für Corporate Governance

Minimale Prüfungsgebiete der ITGC

- **Zugriffsschutz**
  - Security Policy
  - Logischer Zugriffsschutz
  - Funktionstrennung
- **Änderungswesen**
  - Programmänderungen
  - Konfigurationsänderungen
  - Inbetriebnahme der Änderungen
  - Software-Entwicklung
- **Betrieb**
  - Datensicherung
  - Incident-Management
  - Automatisierte Systemabläufe
  - Physischer Zugriffsschutz (Rechenzentrum)

Prüfung anwendungsabhängiger Kontrollen

- **Erhebung der Einhaltung der relevanten GoB**
  - Vgl KFS DV/1
- **Prüfung von**
  - Eingabekontrollen
  - Verarbeitungskontrollen
  - Ausgabekontrollen
  - Zugriffsschutz und Funktionstrennung

KFS/DV 2 - Outsourcing

- **Der Abschlussprüfer hat ausreichende Informationen einzuholen, um**
  - das IKS beurteilen zu können
  - die Kontrollrisiken des Unternehmens beurteilen zu können.
- **Gegebenenfalls sind**
  - vom Prüfer der Service-Organisation Informationen einzuholen oder
  - Prüfungshandlungen vor dem Dienstleistungsunternehmen durchzuführen.
- **Externe Reports dann, wenn nach ISA402 berichtet und ausreichende Qualität**
  - Nicht ausreichend:
    - ISO-Zertifikate (27002, 20000, 9000, …)
    - Selbstbeurteilungen
    - Beurteilungen von nicht ausreichend unabhängigen Organisationen

Sarbanes Oxley

Allgemeines

- **Sarbanes-Oxley; namensgebend sind Senator Paul Sarbanes und der Kongressabgeordnete Michael Oxley**
  - 2002 durch George W. Bush in Kraft gesetzt
  - Initiative als Folge des Zusammenbruchs von Enron und Worldcom
- **Adressaten sind alle US-amerikanischen und ausländischen Unternehmungen inklusive deren Töchter, die an einer US-Börse notieren**
- **Ziel: Vertrauen der Anleger in die Richtigkeit und Verlässlichkeit der veröffentlichten Finanzdaten von Unternehmen wiederherzustellen**

Sarbanes-Oxley (SOX) Paragraph 404

- **Section 404 des Sarbanes-Oxley Act fordert:**
  - Unternehmensleitung beurteilt das Interne Kontrollsystem (IKS) im Unternehmen für Finanzreporting (ICOFR) und berichtet darüber
  - Der externe, unabhängige Prüfer gibt ein Testat über den Management-Test
- **Prüfer berichtet direkt über die Wirksamkeit des IKS**
- **Seit 2004 für US-Unternehmen, die SEC gelistet sind, erforderlich**
- **Seit 2006 für andere Unternehmen (foreign issuers) erforderlich**

Relevante Bestimmungen

- 302 – unternehmerische Verantwortung
  - Durch CEO und CFO zu tragen
  - Eidesstattliche Erklärung
  - Korrekte Darstellung der finanziellen Situation des Unternehmens
  - Erfolgte kritische Durchsicht aller veröffentlichungspflichtigen Dokumente

- 906 – strafrechtliche Bestimmungen
  - Für CEO und CFO
  - Bis zu 1 Mio USD und/oder 10 Jahre Haft bei Kenntnis
  - Bis zu 5 Mio USD und/oder 20 Jahre Haft bei Vorsatz

Auswirkungen

- **Fokussiert auf Finanzberichte**
- **Festlegung des IKS durch das Management**
- **Festlegung von Prozessen**
- **Festlegung der Prozessverantwortung**
- **Identifikation von Risiken, die Prozesse abdecken**
- **Festlegung der Kontrollverantwortung**
- **Identifikation oder Neudefinition von entsprechenden Kontrollaktivitäten**
  - Wer, Was, Wie oft, Womit, Was passiert, wenn…
- **Regelmäßige Tests der Kontrollaktivitäten durch Management**
  - Design: Art der Kontrolle, Anordnung im Prozess
  - Wirksamkeit: Prüfung an Hand von Stichproben, erfordert die Nachvollziehbarkeit der Durchführung von Kontrollen
    - Eine nicht dokumentierte Kontrolle ist keine Kontrolle!
- **Einleitung und Umsetzung von Verbesserungsmaßnahmen**

8. EU-Audit-Richtlinie
(RL 2006/43/EG)

8. EU-Richtlinie (Europa)

- **Vollständige Bezeichnung:**
  „Richtlinie 2006/43/EG des Europäischen Parlaments und des Rates vom 17. Mai 2006 über Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen, zur Änderung der Richtlinien 78/660/EWG und 83/349/EWG des Rates und zur Aufhebung der Richtlinie 84/253/EWG des Rates“
- **Einführung: Am 17. Mai 2006 im Amtsblatt der Europäischen Union veröffentlicht (somit in Kraft getreten)**
- **Von den Mitgliedsstaaten der EU bis 29. Juni 2008 umzusetzen**
- **Umsetzung in Österreich: URÄG2008**
- **Adressaten:**
  - Abschlussprüfer
  - Unternehmen von öffentlichem Interesse
    - (Unternehmen, die unter das Recht eines Mitgliedstaats der EU fallen und deren übertragbare Wertpapiere zum Handel auf einem geregelten Markt eines Mitgliedstaats […] zugelassen sind, Kreditinstitute […] und Versicherungs-unternehmen […]. Die Mitgliedstaaten können auch andere Unternehmen zu Unternehmen von öffentlichem Interesse bestimmen (zB. aufgrund der Art ihrer Tätigkeit, ihrer Größe oder der Zahl ihrer Beschäftigten)

Inhalt der Richtlinie

- Kapitel I: Gegenstand und Bestimmungen
- Kapitel II: Zulassung, kontinuierliche Fortbildung und gegenseitige Anerkennung von Wirtschaftsprüfern
- Kapitel III: Registrierung von Wirtschaftsprüfern
- Kapitel IV: Berufsgrundsätze, Unabhängigkeit, Unparteilichkeit, Verschwiegenheit und Berufsgeheimnis des Wirtschaftsprüferberufs
- Kapitel V: Prüfungsstandards und Bestätigungsvermerk bei Abschlussprüfungen
- Kapitel VI: Qualitätssicherung für Wirtschaftsprüfer
- Kapitel VII: Untersuchungen bei mangelhaften Prüfungen und Sanktionen für Wirtschaftsprüfer
- Kapitel VIII: Öffentliche Aufsicht und gegenseitige Anerkennung der mitgliedsstaatlichen Regelungen
- Kapitel IX: Bestellung und Abberufung des Wirtschaftsprüfers
- Kapitel X: Besondere Bestimmungen für die Abschlussprüfung bei Unternehmen von öffentlichem Interesse
  (insb. Artikel 41 – Prüfungsausschuss)
- Kapitel XI: Internationale Aspekte zu Wirtschaftsprüfern
- Kapitel XII: Übergangs- und Schlussbestimmungen

Ziele und relevante Teile

- Ziele der Richtlinie
  - Begrenzung von finanziellen und betrieblichen Risiken und Vorschriftenverstößen und Verbesserung der Rechnungslegung durch Prüfungsausschüsse und wirksame interne Kontrollsysteme
  - Sicherung hoher Prüfungsqualität durch regelmäßige Kontrollen und Qualitätssicherungssysteme
  - Harmonisierung der Anforderungen an die Abschlussprüfung auf hohem Niveau

Ziele und relevante Teile

- Artikel 41
  - Verpflichtung von Unternehmen von öffentlichem Interesse zur Ein-richtung eines Prüfungsausschusses mit folgenden Aufgaben (u. a.):
    - den Rechnungslegungsprozess zu überwachen;
    - die Wirksamkeit des internen Kontrollsystems, gegebenenfalls des internen Revisionssystems und des Risikomanagementsystems des Unternehmens zu überwachen;
    - die Abschlussprüfung des Jahres- und des konsolidierten Abschlusses zu überwachen;
  - Der Abschlussprüfer oder die Prüfungsgesellschaft berichten dem Prüfungsausschuss über die wichtigsten bei der Abschlussprüfung gewonnenen Erkenntnisse, insbesondere über wesentliche Schwä-chen bei internen Kontrollen des Rechnungslegungsprozesses
  - Nicht börsennotierte Unternehmen von öffentlichem Interesse sowie deren Prüfer können von der Pflicht des Kapitel X ausgenommen werden, die Bedingungen dafür sind derzeit nicht definiert

Notwendige Maßnahmen

- Einrichtung eines eigenen **Prüfungsausschusses** und Zuweisung von umfangreichen Kontrollverantwortlichkeiten.
- Aufnahme, Analyse des **Rechnungslegungsprozesses** im Hinblick auf die Funktionsfähigkeit und stetige Überwachung desselben
- Wirksamkeit des **internen Kontrollsystems**, **internen Revisionssystems** und des **Risikomanagementsystems** muss durch den Prüfungsausschuss sichergestellt werden
- Explizite Pflicht des **Abschlussprüfers** über **wesentliche Schwächen der internen Kontrollen des Rechnungslegungs-prozesses an den Prüfungsausschuss** zu berichten. **Prüfungsmaßstab** sind die anerkannten Grundsätze der **Ordnungsmäßigkeit, Sicherheit und Effizienz**.

Ein umfangreiches System an internen Steuerungs- und Überwachungsmechanismen (IKS) muss im Unternehmen implementiert, angewandt und entsprechend überwacht werden.

URÄG

Umsetzung in Österreich

- **“Bundesgesetz, mit dem das Unternehmensgesetzbuch, das Aktiengesetz, das GmbHGesetz, das SE-Gesetz, das Genossenschaftsgesetz, das Genossenschaftsrevisionsgesetz, das Spaltungsgesetz und das Luftfahrtgesetz geändert werden (Unternehmensrechts-Änderungsgesetz 2008 – URÄG 2008)”**
- **Anforderungen der EU-RL grundsätzlich vollständig übernommen**
  - In Kraft: 30.6.2008
  - Gültig für Geschäftsjahre beginnend nach 31.12.2008
- **Unternehmen von öffentlichem Interesse (Betroffene)**
  - Kapitalmarktorientierte Unternehmen
    - Aktien oder Wertpapiere an geregeltem Markt oder anerkannten, offenen Markt in OECD-Staat notieren
  - Versicherungen, Banken
  - „Sehr“ große Unternehmen
    - 96,25 Millionen Euro Bilanzsumme
    - 192,5 Millionen Euro Umsatzerlöse
  - Unternehmen mit Aufsichtsrat aus mehr als 5 (gewählten) Mitgliedern

Umsetzung in Österreich (2)

- **Unternehmen müssen (zusätzlich zur Bilanz und zum Lagebericht) einen Corporate Governance Bericht verfassen**
  - Welcher Codex
  - Abweichungen vom Codex müssen erklärt werden
- **Abschlussprüfungen müssen die internationalen Prüfungsstandards (ISA) beachten**
- **Auswahl des Abschlussprüfers durch den Aufsichtsrat**
- **Ausschließungsgründe und Unabhängigkeits-bedingungen für Prüfer**

Umsetzung in Österreich (3)

- **Der Aufsichtsrat hat einen Prüfungsausschuss mit folgenden Aufgaben zu bilden:**
  - die Überwachung der Rechnungslegung;
  - die Überwachung der Wirksamkeit des internen Kontrollsystems;
  - die Überwachung der Abschlussprüfung und Konzernabschlussprüfung;
  - die Prüfung und Überwachung der Unabhängigkeit des Abschlussprüfers, insbesondere im Hinblick auf die für das geprüfte Unternehmen erbrachten zusätzlichen Leistungen;
  - …
- **Fristen (§ 906 UGB)**
  - Änderungen treten mit 1. Juni 2008 in Kraft
  - „… auf Geschäftsjahre anzuwenden, die nach dem 31. Dezember 2008 beginnen“

Auswirkungen 8. EU-RL

- **8. EU-RL wendet sich kaum direkt an Unternehmen, ABER**
- **Der Benchmark von SOX bezüglich IKS wird abfärben**
  - Über den Prüfungsausschuss
    - Überwachungsaufgaben (IKS, Risikomanagement, etc.)
  - Über den Prüfer
    - Die Ausbildung von Prüfern greift IKS und Risikomanagement auf
    - Der Prüfer muss über das IKS berichten
  - Über die Verantwortlichkeiten des Vorstands
  - Über den Markt
- **Wie und woher bekommt der Vorstand / Prüfungsausschuss seine Informationen über das IKS?**

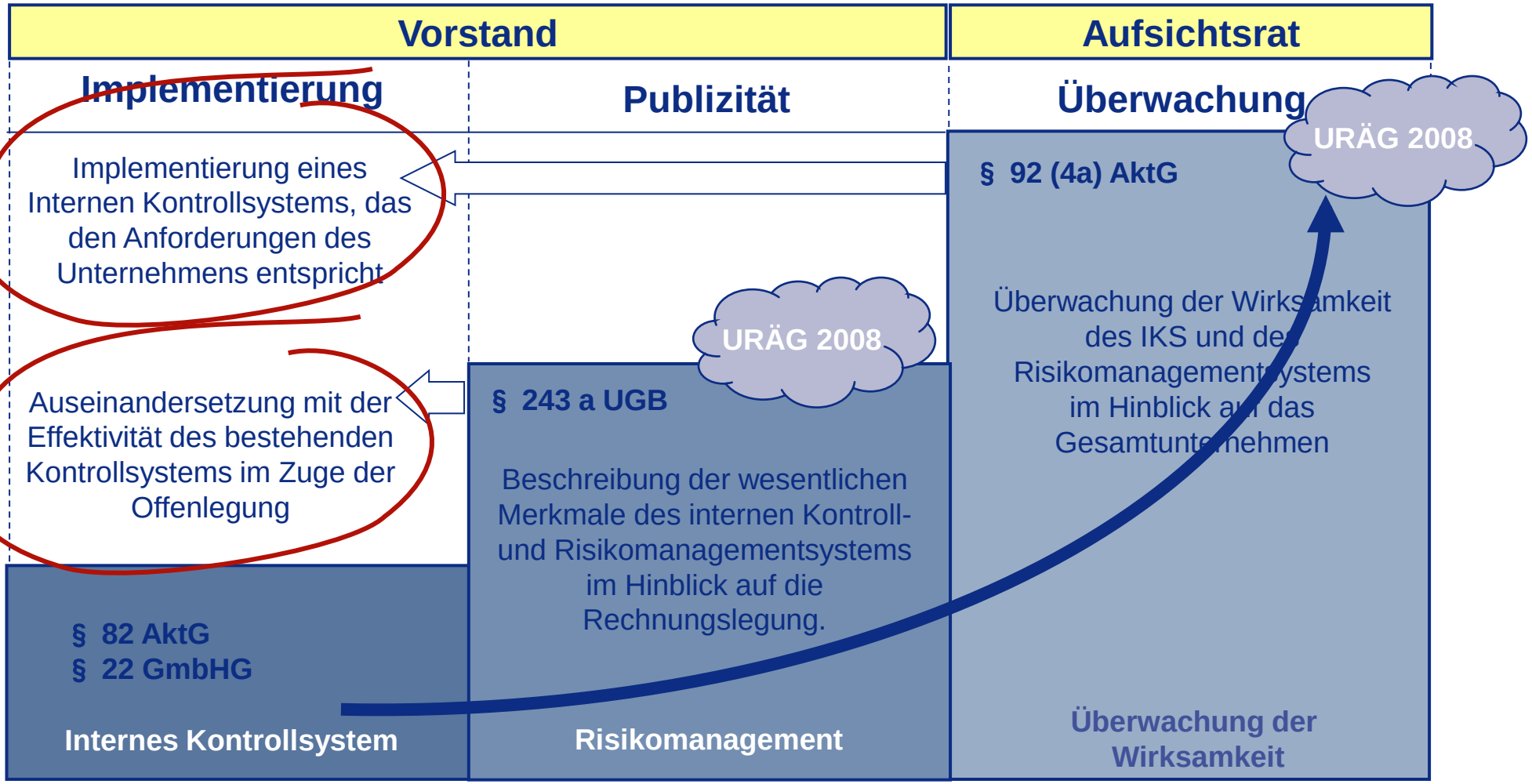
Auswirkungen auf Gremien

- **Vorstand / GF**
  - Verantwortet IKS, interne Revision, RM-System
  - Stellt Lagebericht und CG-Bericht auf und unterschreibt diesen
- **Prüfungsausschuss**
  - Überwacht IKS, RM-System, interne Revision
  - Prüft Lagebericht, CG-Bericht (darin: IKS, RM-System)
- **Abschlussprüfer**
  - Prüft Einhaltung relevanter Gesetze (Lagebericht, Erstellung CG-Bericht, IKS,…)
  - Berichtet über Beanstandungen
- **Geschäftsführung**
  - Setzt das IKS um
- **Abteilungs-/Bereichsleiter**
  - Setzen das IKS in Ihrem Bereich um
  - Beurteilen die Wirksamkeit
- **Revision**
  - Unterstützt in der Beurteilung der Wirksamkeit

Konsequenzen / Aufgaben

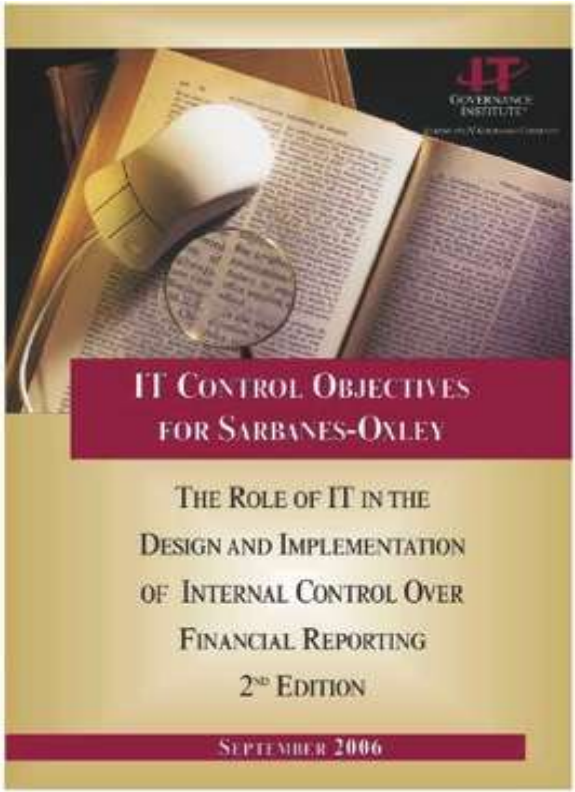
- **Umsetzung eines Internen Kontrollsystems für die Gesellschaft**
- **Beurteilung IKS durch das Management (Management Assessment)**
- **Bericht über die Wirksamkeit im Corporate Governance Bericht des Konzerns**
- **Abschlussprüfer stellt die Existenz und die Angemessenheit des IKS sicher**
  - Nicht: Prüfung des Management Assessment (vgl. SOX)
- **Zusätzlich empfohlen:**
  - ISA402/SAS 70 für Konzerngesellschaften

URÄG 2008
Zusammenfassung



Auswirkungen auf die IT

- Massive Auswirkungen
- Kontrollen müssen dokumentiert und geprüft werden
- große Teile der Kontrollen in der IT (oft 50 bis 70 %)
- Im Regelfall mehrere hundert Kontrollen
- Wesentliche Kontroll-Schwachstellen sind oft in der IT
- Unterscheidung in Anwendungskontrollen und General IT Controls
- COBIT als Standard für General IT Controls anerkannt
- Überleitung von COSO auf COBIT in einer Veröffentlichung vom IT Governance Institute



SAS 70 → SSAE16
ISA402 → ISAE3402
IWP-PE 14

Überblick SSE 16 (SAS70)

- **Standard für die Prüfung von Outsourcing-Dienstleistern (und deren Kontrollumfeld)**
- **Definiert die Prüfung und die Berichterstattung, allerdings NICHT den Inhalt**
- **Anzuwenden bei (Teil-) Outsourcing der IT**
- **Mittlerweile weltweiter De-Facto Standard für Prüfungen von und für Wirtschaftsprüfern bei (IT-) Service-Organisationen**
- **Unterschiedliche Versionen**
  - International: ISAE 3402 der IFAC
  - PS 331 in Deutschland
  - IWP-PE 14 in Österreich
- **Sarbanes Oxley – vom PCAOB vorgeschrieben**
- **Auch in Österreich bei (fast) allen RZ in Umsetzung**

Möglichkeiten der Prüfer

- **Prüfer von RZ-Kunden müssen (lt. KFS/DV2)**
  - Report des RZ einholen oder
  - selbst das RZ prüfen oder
  - jemanden beauftragen, das RZ nach SAS 70 zu prüfen oder
  - Bestätigungsvermerk einschränken oder versagen

Berichterstattung

- Standard-Text für Bestätigungsvermerk definiert
- Bei Typ II Report sind die vorhandenen Kontrollen, deren Prüfung und die Ergebnisse der Prüfung im Detail dazustellen
- Die Verantwortungen von Kunde und RZ sind klar abzugrenzen
- Bei wesentlichen Mängeln ist der Bestätigungs-vermerk zu ergänzen, einzuschränken oder zu versagen

Readiness

- **Beschreibung der wesentlichen IT-Prozesse**
- **Identifikation von**
  - Risiken
  - Control Objectives (COBIT, ITIL, ISO27002)
  - Kontrollaktivitäten
- **Dokumentation der Kontrolldurchführung**

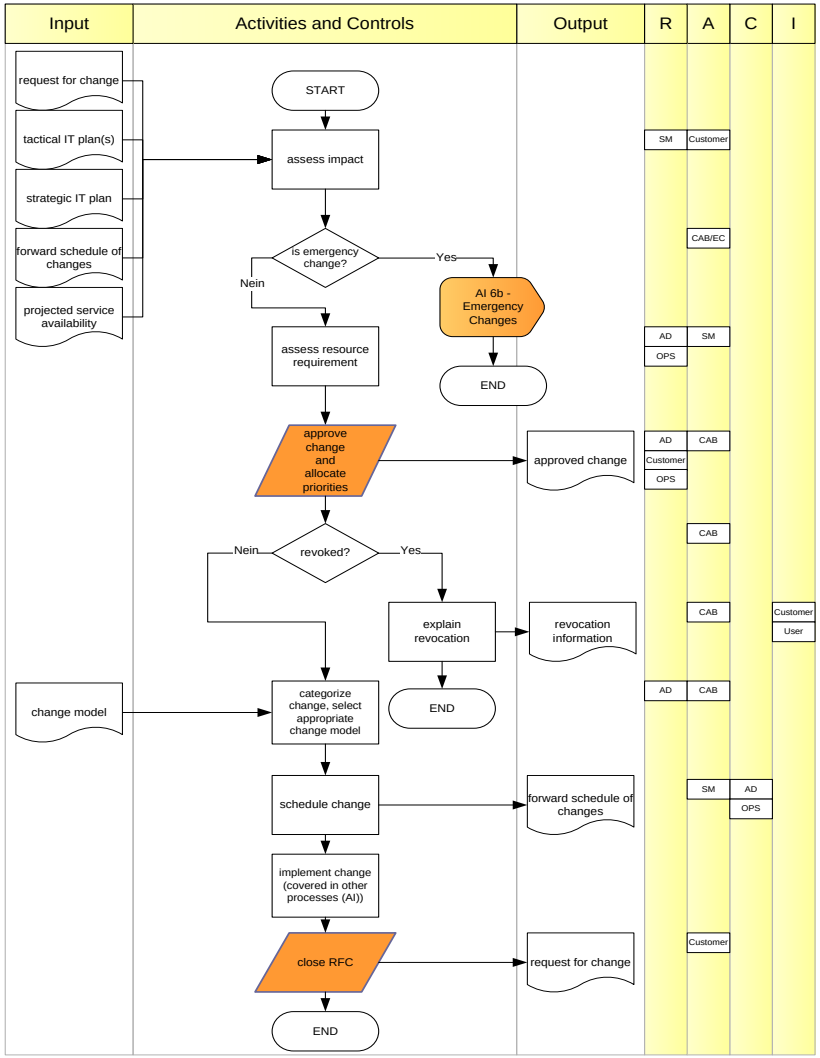
Prüfung

- **Beweisführung, dass die Control Objectives durch die Kontrollaktivitäten erreicht werden und damit die Risiken abgedeckt werden.**
- **Vorgehen**
  - Test of Design (ToD)
    - Bewertung des prinzipiellen Kontrolldesigns des IKS
  - Test of Operating Effectiveness (ToE)
    - Ziehen von statistisch relevanten Stichproben
    - Prüfung von Kontrollen
- **Berichterstattung**
  - Detaillierte Informationen
    - Prozess und Control Objective
    - Kontrollaktivität
    - Prüfungsvorgehen
    - Prüfungsergebnis

Berichtsausschnitt (Beispiel)

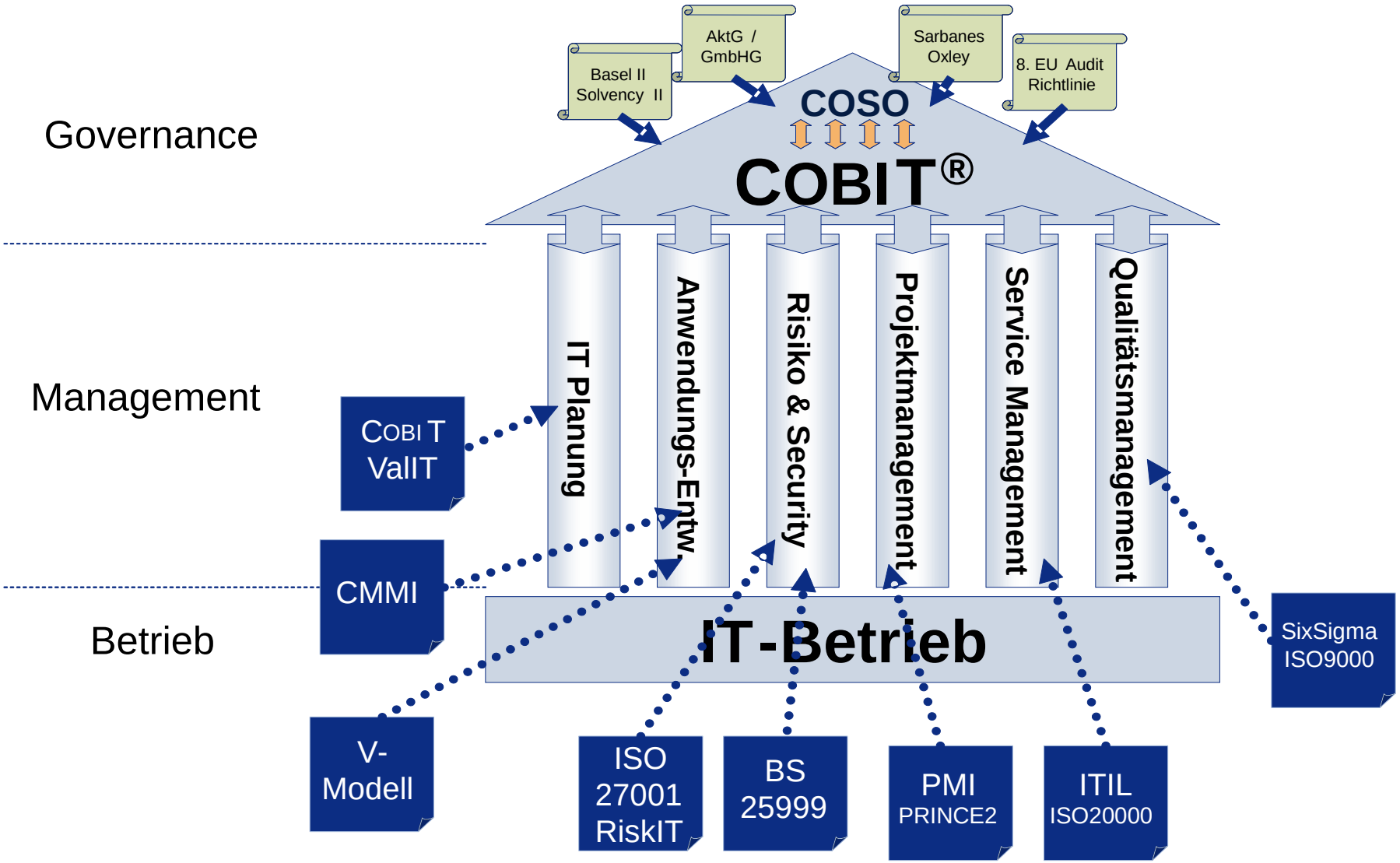
Bereitgestellt vom Unternehmen	Geprüft (zB durch KPMG, EY, D&T, PWC)	
Kontrollaktivität	Test über effiziente Durchführung von Kontrollen	Testergebnisse
1. Anforderungen für die Anlage, Änderung oder Löschung eines Zugang zum Unternehmensnetzwerk werden durch einen Key User initialisiert und zur Bearbeitung schriftlich an den IT Helpdesk des Unternehmens weitergeleitet.	**Prüfung von einer Stichprobe von 20 Eintritten, ob für diese entsprechende Anforderungsformulare vorhanden sind**	**Formular bei 19 von 20 Eintritten vollständig, einmal großteils ausgefüllt, daher Kontrolle insgesamt als wirksam beurteilt**
2. In der Anwendung XXX gelten folgende Anforderungen an Passworte: Mindestlänge 8 Zeichen; Änderungen zumindest alle 90 Tage etc. Änderungen dieser Einstellungen werden protokolliert und die Protokolle wöchentlich von xyz überprüft	**Prüfung des Nachweises der Prüfung und der diesbezüglichen Protokolle der letzten 6 Monate**	**Nachweis der Protokolle fehlt für 5 von 26 Wochen; daher wird die Kontrolle als unwirksam beurteilt**

Prozessbeispiel - Kontrollen



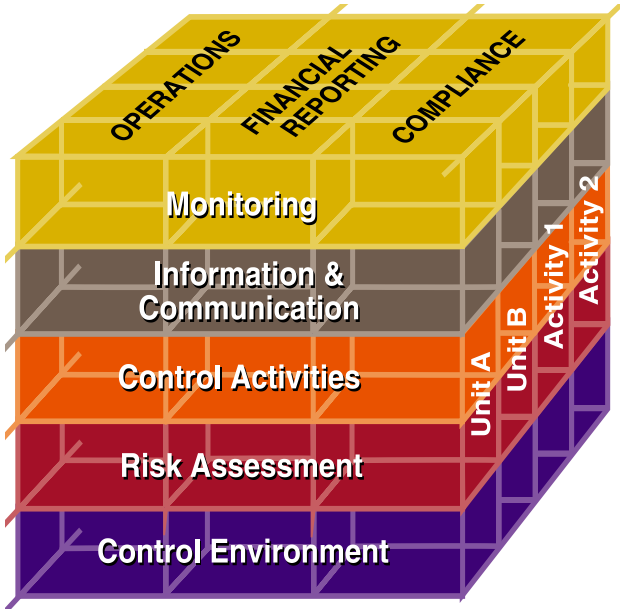
Standards

Standards und Good-Practices



COSO (Internal Control - Integrated Framework)

- 1992 durch „The **C**ommittee **o**f **S**ponsoring **O**rganizations of the Treadway Commission" veröffentlicht
- Gemeinsame Sprache über Kontrollen, Definitionen, Modelle
- **Unternehmensziele** im Rahmen von COSO sind
  - Operations (Effektivität und Effizienz der Tätigkeiten der Unternehmung)
  - Financial Reporting (Erstellung von zuverlässigen Jahresabschlüssen)
  - Compliance (Einhaltung von Gesetzen und Regulationen)
- Zielerreichung über die Ausgestaltung der **Komponenten** des Frameworks
  - Control Environment (Kontrollumfeld)
  - Risk Assessment (Risikobewertung)
  - Control Activities (Kontrollaktivitäten)
  - Information & Communication (Information & Kommunikation)
  - Monitoring (Überwachung)
- **Benchmark für interne Kontrollen** und Verweis in SOX
- Weiterentwicklungen:
  - September 2004: Enterprise Risk Management (COSO II)
  - Juni 2006: Guidance for Smaller Public Companies Reporting on Internal Control over Financial Reporting"



AS8015
ISO36500

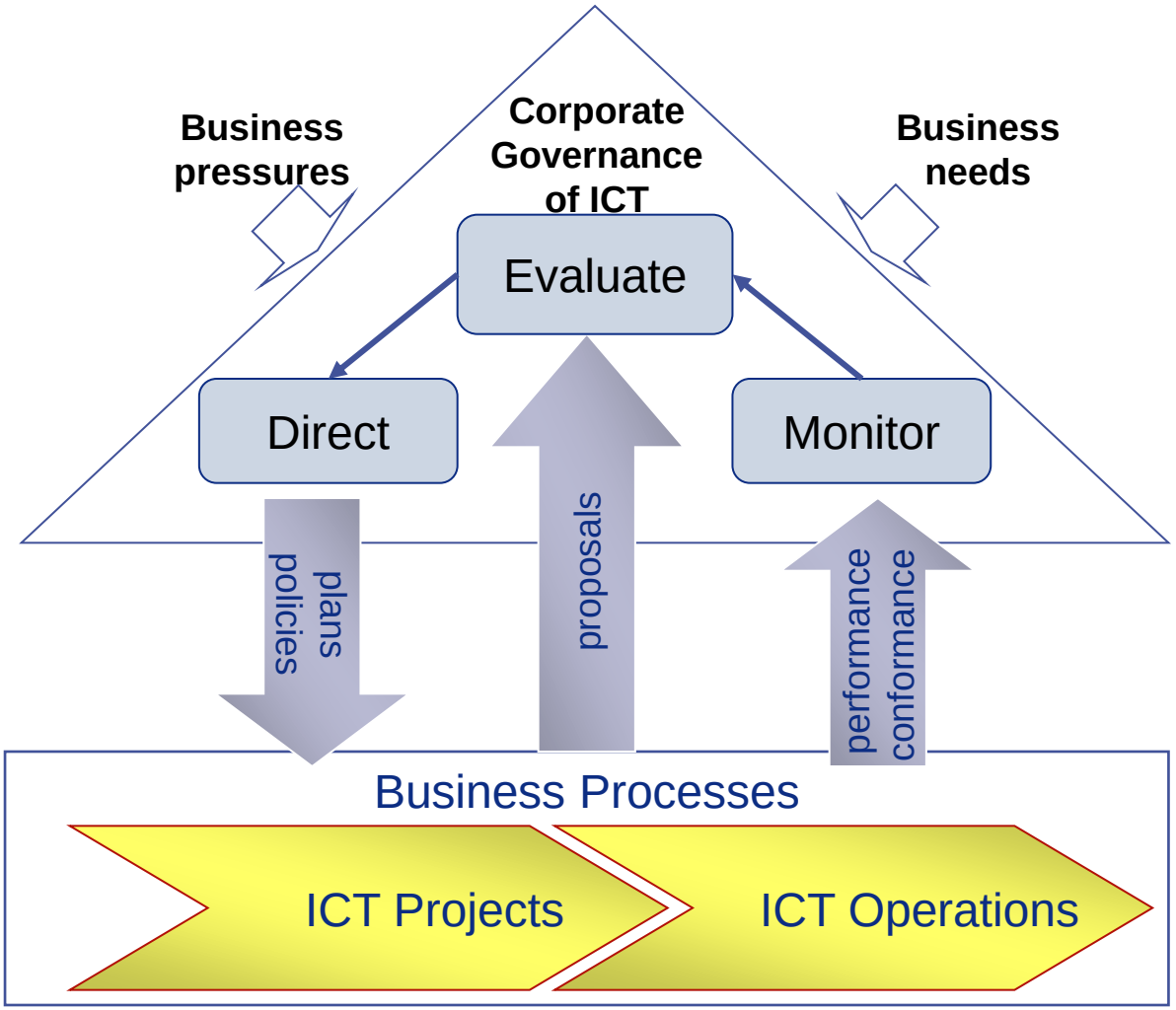
AS8015

- **AS8015-2005 - Australian Standard for Corporate Governance of Information and Communication Technology (ICT)**
- **First Standard on ITG internationally**
- **Will be used as a basis for an ISO Standard**
  - ISO/IEC36500
- **Not requirements based, but principles based**

Principles

- **Principle 1: Responsibility.**
  - Individuals and groups within the organization understand and accept their responsibilities in respect of both supply of, and demand for IT. Those with responsibility for actions also have the authority to perform those actions.
- **Principle 2: Strategy.**
  - The organization's business strategy takes into account the current and future capabilities of IT; the strategic plans for IT satisfy the current and ongoing needs of the organization's business strategy.
- **Principle 3: Acquisition.**
  - IT acquisitions are made for valid reasons, on the basis of appropriate and ongoing analysis, with clear and transparent decision making. There is appropriate balance between benefits, opportunities, costs, and risks, in both the short term and the long term.
- **Principle 4: Performance.**
  - IT is fit for purpose in supporting the organization, providing the services, levels of service and service quality required to meet current and future business requirements.
- **Principle 5: Conformance.**
  - IT complies with all mandatory legislation and regulations. Policies and practices are clearly defined, implemented and enforced.
- **Principle 6: Human Behaviour.**
  - IT policies, practices and decisions demonstrate respect for Human Behaviour, including the current and evolving needs of all the 'people in the process'.

A model for corporate governance of IT



Evaluate

the use of IT

Direct

preparation and implementation of plans and policies

Monitor

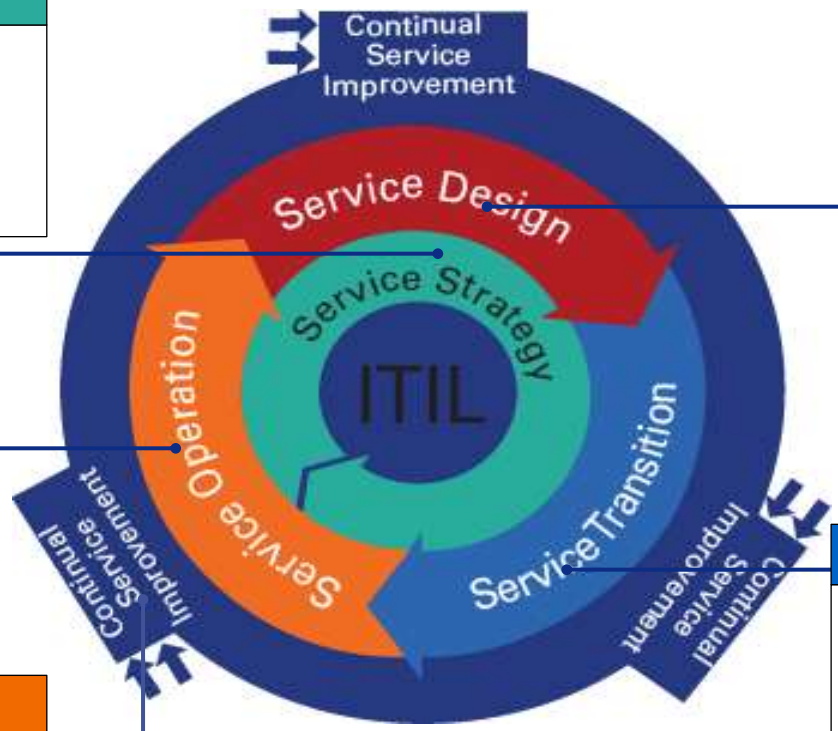
conformance to policies, and performance against the plans

ITIL
IT Infrastructure Library

ITIL –Version 3

SERVICE STRATEGY

- Financial Management
- Return on Investment
- Service Portfolio Mgmnt
- Demand Management



SERVICE DESIGN

- Service Catalogue Management
- Service Level Management
- Capacity Management
- Availability Management
- IT Service Continuity Management
- Information Security Management
- Supplier Management

SERVICE OPERATION

- Event Management
- Incident Management
- Request Fulfilment
- Problem Management
- Access Management

CONTINUAL SERVICE IMPROVEMENT

- 7-Step Improvement Process

SERVICE TRANSITION

- Transition Planning and Support
- Change Management
- Service Asset & Configuration Management
- Release & Deployment Management
- Service Validation
- Evaluation
- Knowledge Management

COBIT

COBIT 5
AN ISACA® FRAMEWORK

Der Anspruch

- Provide a **renewed and authoritative** governance and management **framework** for enterprise information and related technology (**GEIT & MEIT**).
- **Linking** together and reinforcing all other major **ISACA frameworks** and guidance such as:
  COBIT, Val IT, Risk IT, BMIS, ITAF, Board Briefing, TGF
- **Connect to other major frameworks** and standards in the marketplace (COSO, ITIL, ISO standards, etc.).

COBIT 5 - Entwicklung

- Gruppen
  - Task Force „Future Framework“ (2008 – 2009)
  - COBIT 5 Task Force 2010 – 2011
  - Core Development Team
  - Professional Support Team (PwC)
  - Researcher
- Vorgehen
  - Design durch Task Force
  - Ausarbeitung durch Development Team
  - Development Workshops
  - Public Exposure Drafts
  - Stress Tests
  - SME Reviews

Was ist neu?

Fokus	Enterprise Governance over IT
Scope	Business & IT
Methode	Enabler
Produkt	Knowledge Base & Views

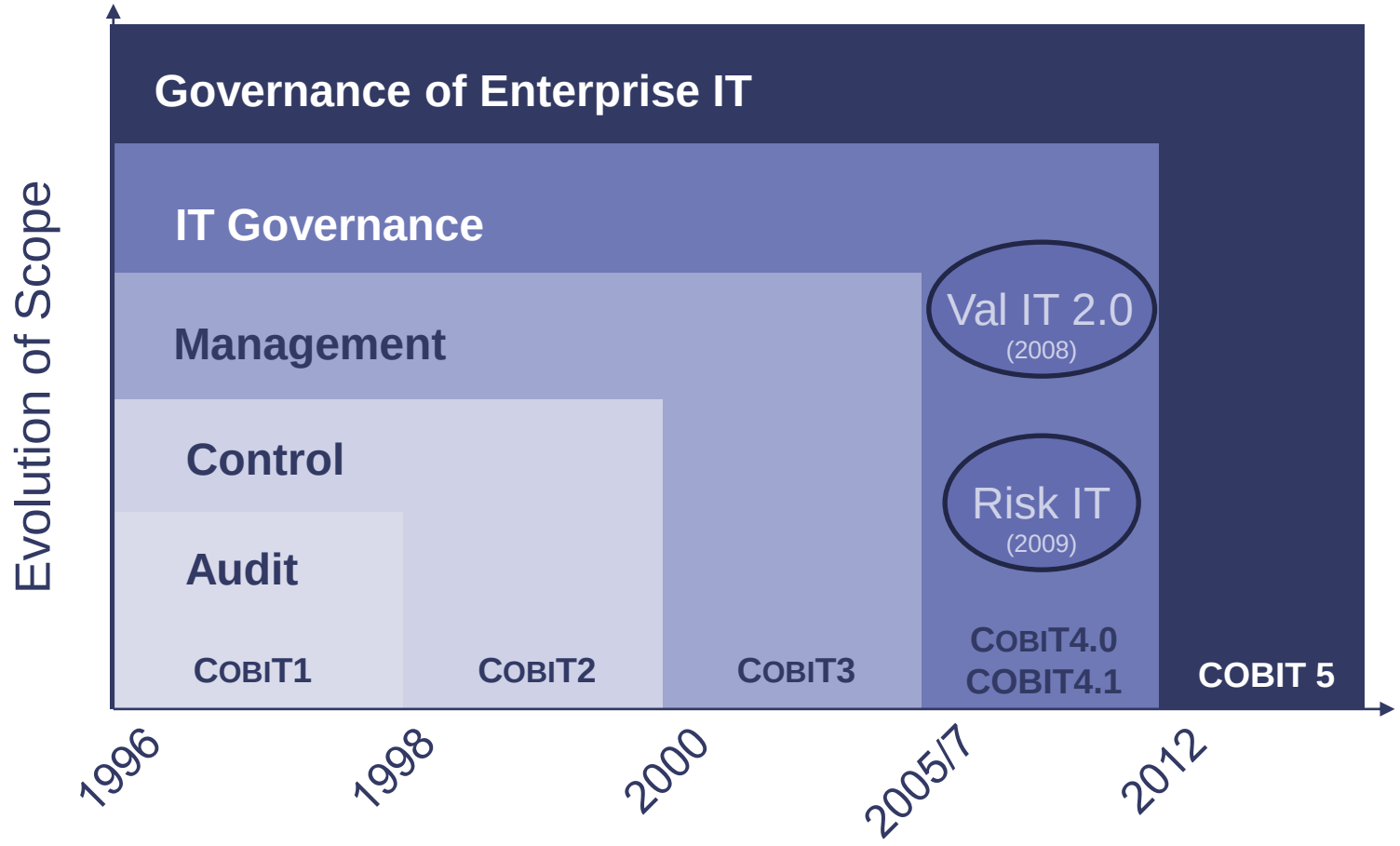
… und einiges mehr.

Publikationen

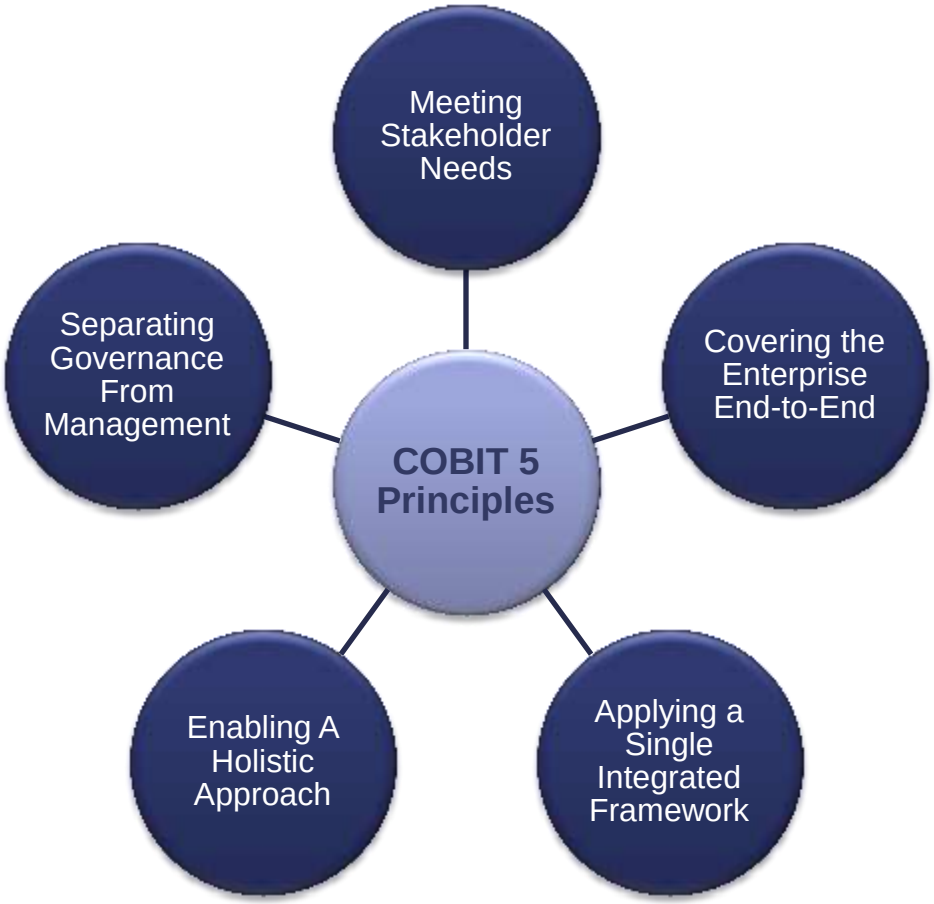
- Zum Release (10. April 2012)
  - COBIT Framework
  - Enabling Processes
  - Implementation Guide

- In Entwicklung
  - COBIT 5 for Security
  - COBIT 5 for Risk
  - COBIT 5 for Assurance
  - COBIT Online Replacement
  - COBIT 5 Assessment Programme
- In Planung
  - COBIT 5 for Performance
  - COBIT 5: Enabling Information (Enabler Guide)
  - More to come …
- COBIT Trainings
  - Ab Mai erste Kurse

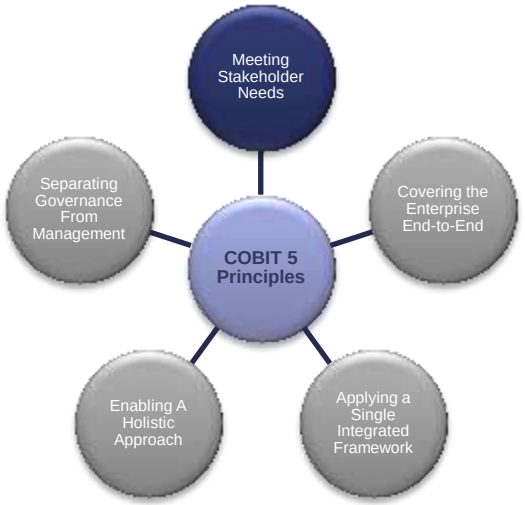
COBIT 5
AN ISACA® FRAMEWORK



COBIT 5 - Principles



COBIT 5
AN ISACA® FRAMEWORK



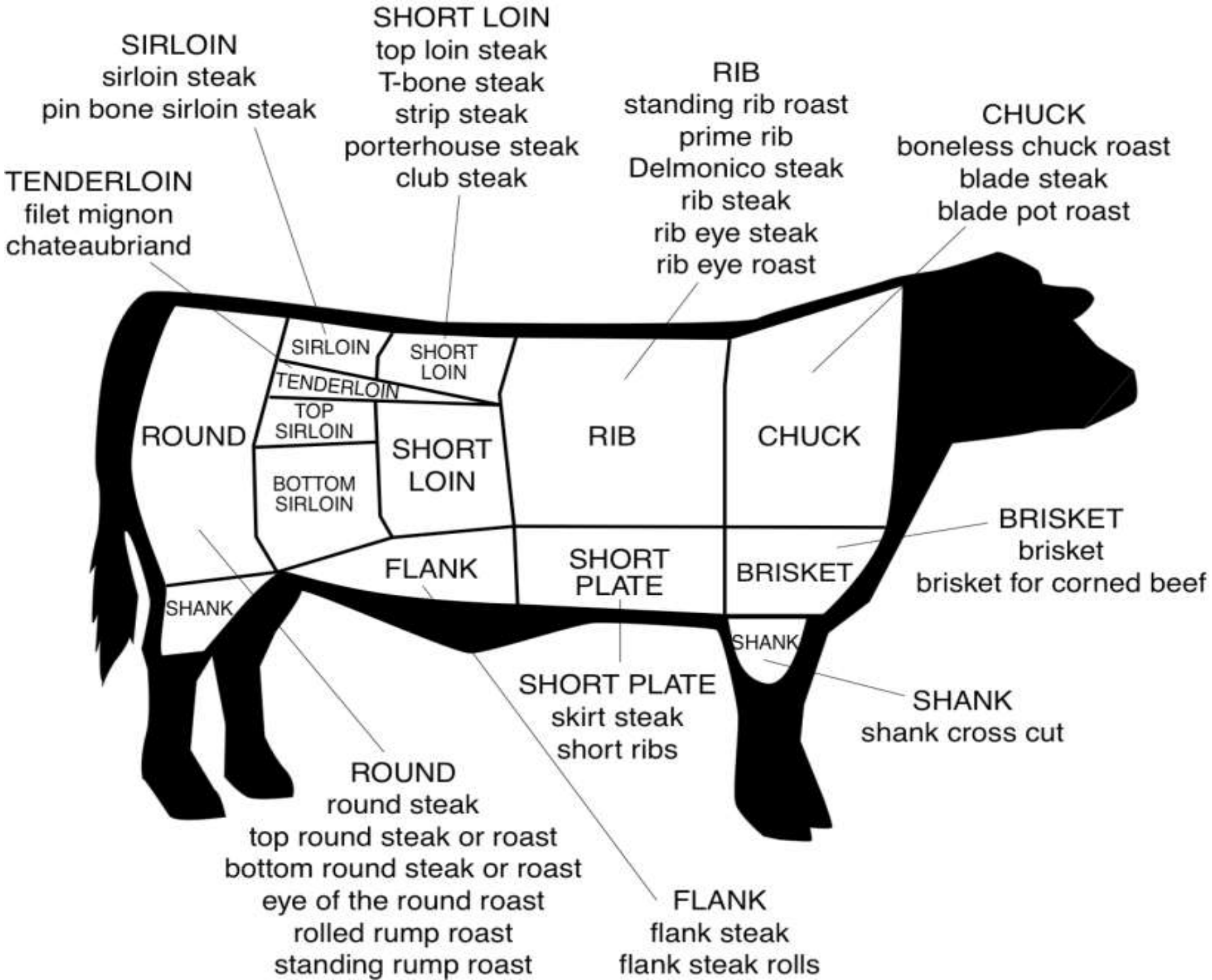
Meeting Stakeholder‘s Needs

Stakeholder Drivers
(Environment, Technology, Evolution, …)

Drive

Governance Objective: Value Creation

- Benefits Realisation
- Resource Optimisation
- Risk Optimisation


SIRLOIN
sirloin steak
pin bone sirloin steak
SHORT LOIN
top loin steak
T-bone steak
strip steak
porterhouse steak
club steak
RIB
standing rib roast
prime rib
Delmonico steak
rib steak
rib eye steak
rib eye roast
CHUCK
boneless chuck roast
blade steak
blade pot roast
TENDERLOIN
filet mignon
chateaubriand
SIRLOIN
SHORT LOIN
TENDERLOIN
TOP SIRLOIN
ROUND
SHORT LOIN
RIB
CHUCK
BOTTOM SIRLOIN
BRISKET
brisket
brisket for corned beef
FLANK
SHORT PLATE
BRISKET
SHANK
SHANK
SHORT PLATE
skirt steak
short ribs
SHANK
shank cross cut
ROUND
round steak
top round steak or roast
bottom round steak or roast
eye of the round roast
rolled rump roast
standing rump roast
FLANK
flank steak
flank steak rolls

COBIT 5
AN ISACA® FRAMEWORK

Internal Stakeholders

IT Manager

How do we deliver IT services, as required by the business and directed by the board?

Board, Executive, and Business Manager

How do we define business direction for IT, deliver value, and manage risks?

Risk and Compliance Manager

How do we ensure that policies, regulations, and laws are complied with and new risks identified?

IT Auditor

How do we provide independent assurance of IT value delivery and risk mitigation?

External Stakeholders

External Auditor

I need to know whether the figures reported are correct and the control system is reliable?

Customers

I need you to keep my private information secure on your computer system.

Regulator

How can we be assured that the organization has a business continuity plan? Remains in the country? Pays taxes? Keeps an employer of choice? Protects data and knowledge?

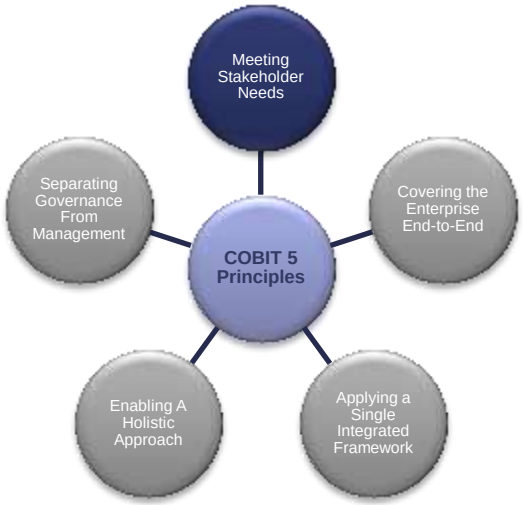
Suppliers

Do we have assurance that confidential information about our company is not sent to our competitors?

Anonymous

How can I get access to the data?

COBIT 5
AN ISACA® FRAMEWORK



Stakeholder Drivers
(Environment, Technology Evolution, …)

Stakeholder Needs

- **Benefits Realisation**
- **Resource Optimisation**
- **Risk Optimisation**

Cascade to

Enterprise Goals

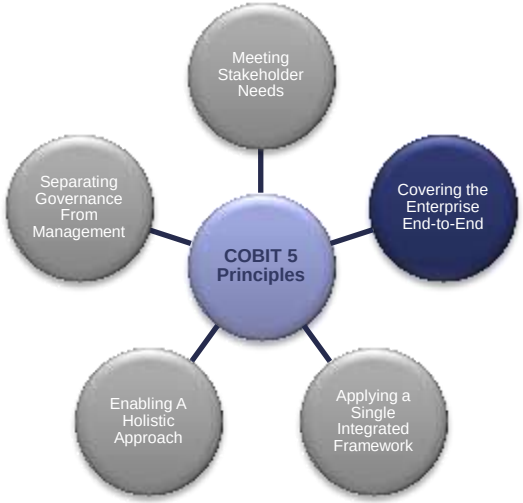
Cascade to

IT Related Goals

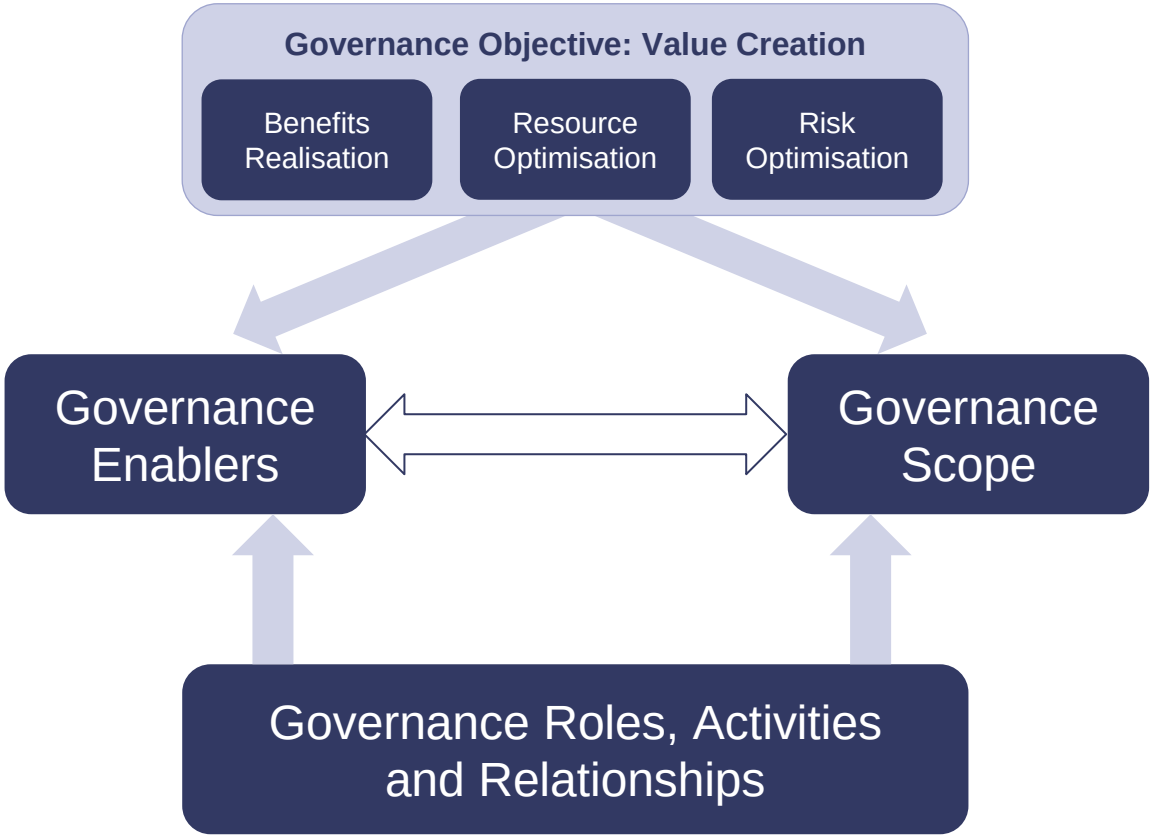
Cascade to

Enabler Goals

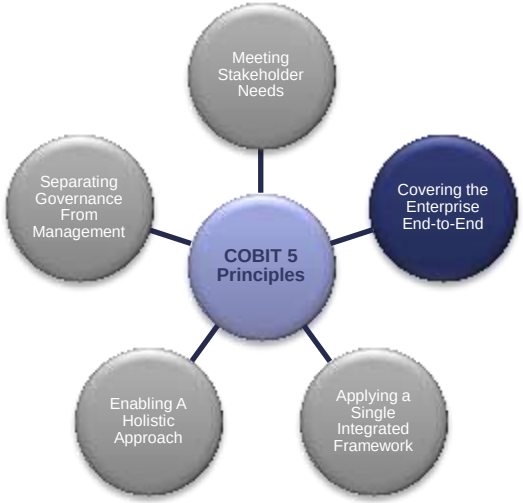
COBIT 5
AN ISACA® FRAMEWORK



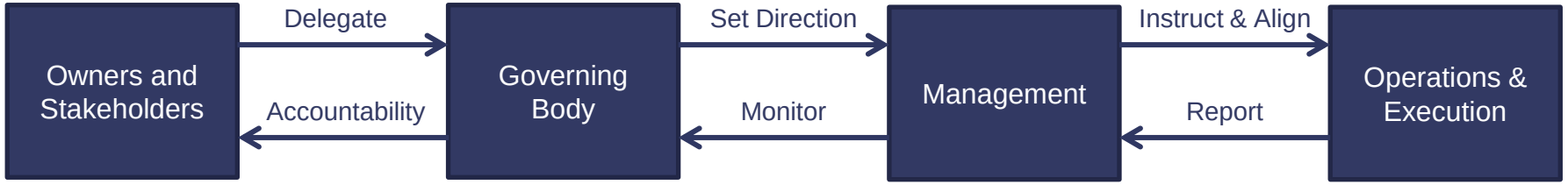
Covering the Enterprise End-to-End



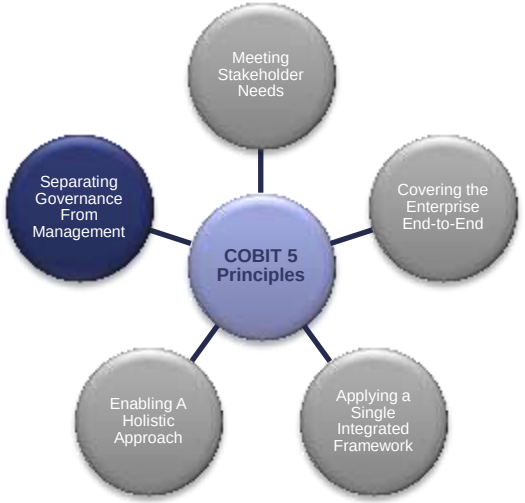
COBIT 5
AN ISACA® FRAMEWORK



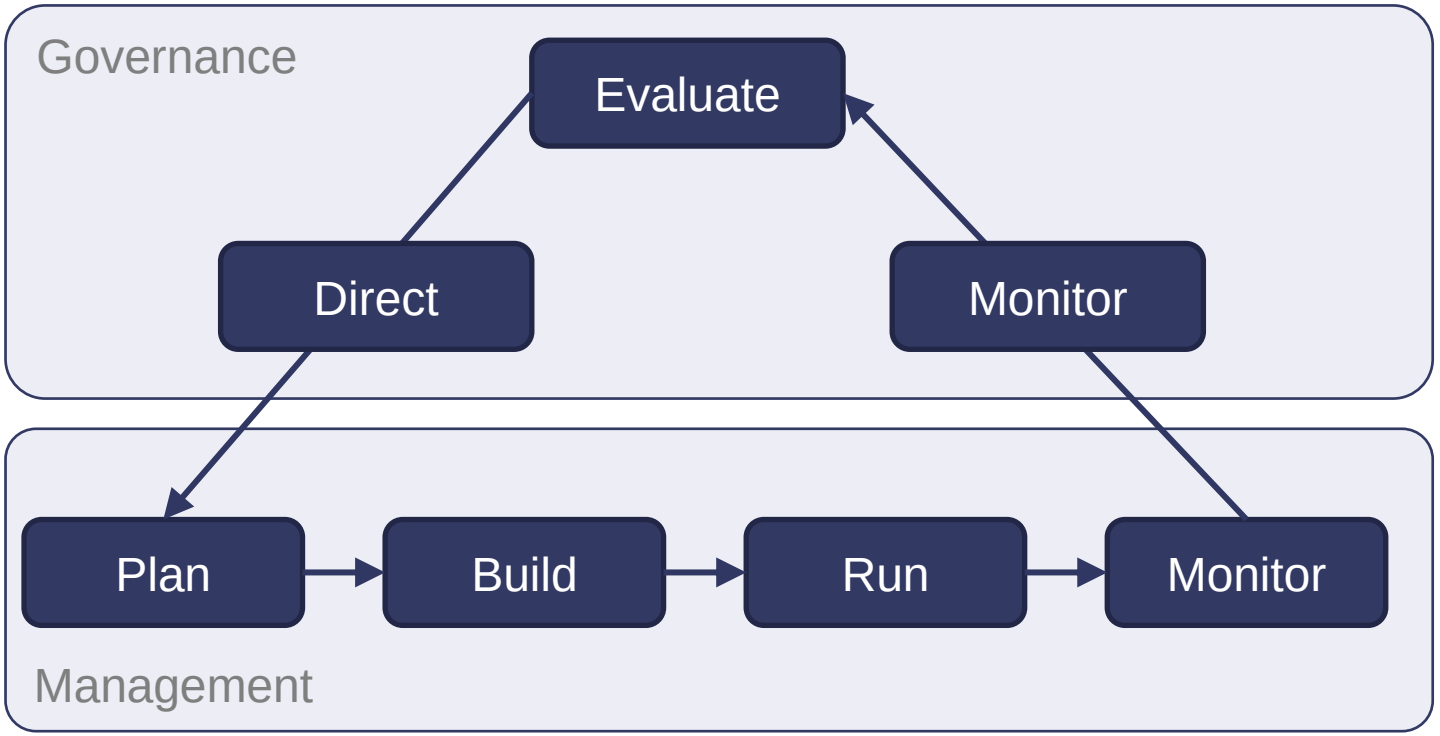
Governance Roles, Activities and Relationships



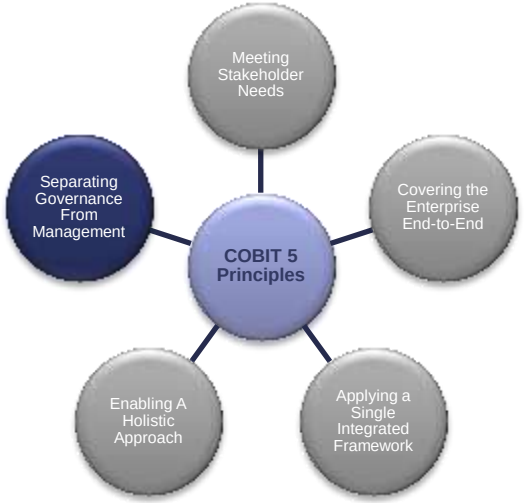
COBIT 5
AN ISACA® FRAMEWORK



Separating Governance from Management



COBIT 5
AN ISACA® FRAMEWORK



Aktualisierte Definitionen

Governance

by
evaluating stakeholder needs, conditions and options;
setting **direction** through prioritisation and decision making; and
monitoring performance, compliance and progress against plans.

Management

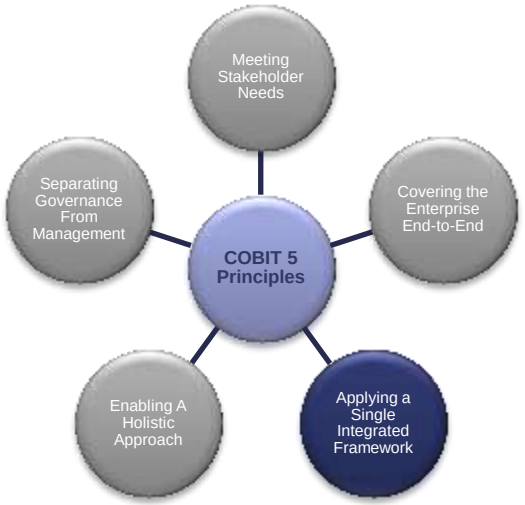
Management **plans, builds, runs** and **monitors activities** in alignment with the direction set by the governance body to achieve the enterprise objectives.

COBIT 5
AN ISACA® FRAMEWORK

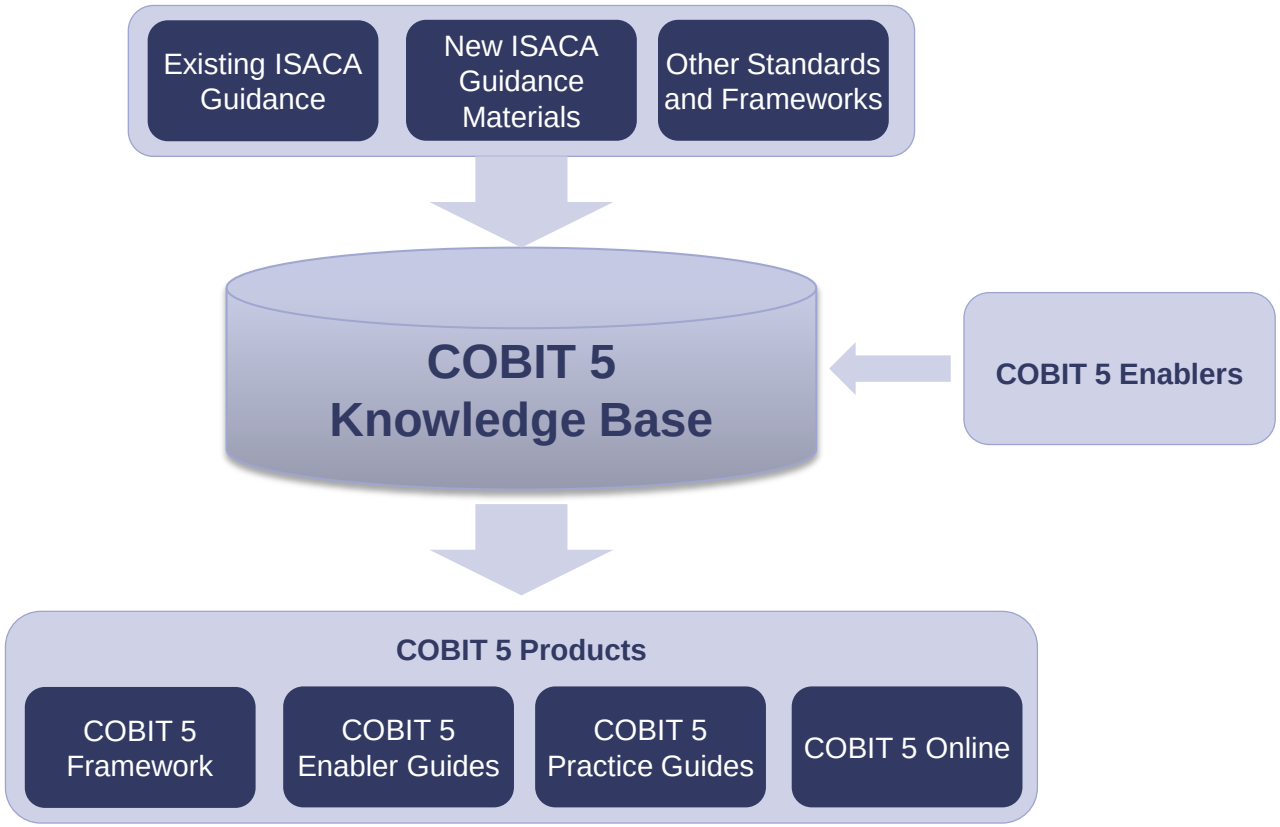
GRC - Three **Different** Areas (often mixed up)

	Governance	Risk	Compliance
Scope	Evaluate, direct and monitor risk, value and resources.	Probability of uncertain future events.	Conforming to a rule.
Question	Are we getting the benefits?	Are things going wrong?	Are we doing things in accordance to requirements? (And: Can we prove it or shall we hide it?)

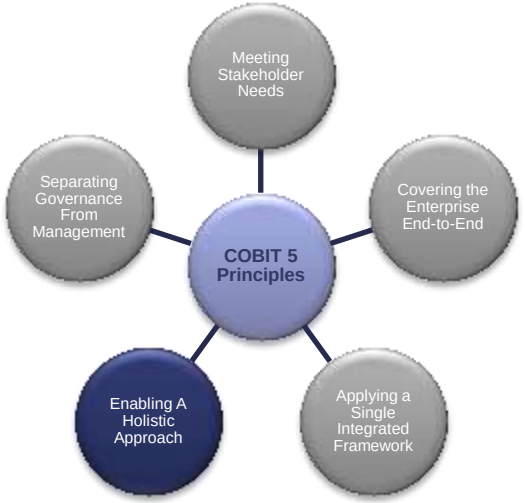
COBIT 5
AN ISACA® FRAMEWORK



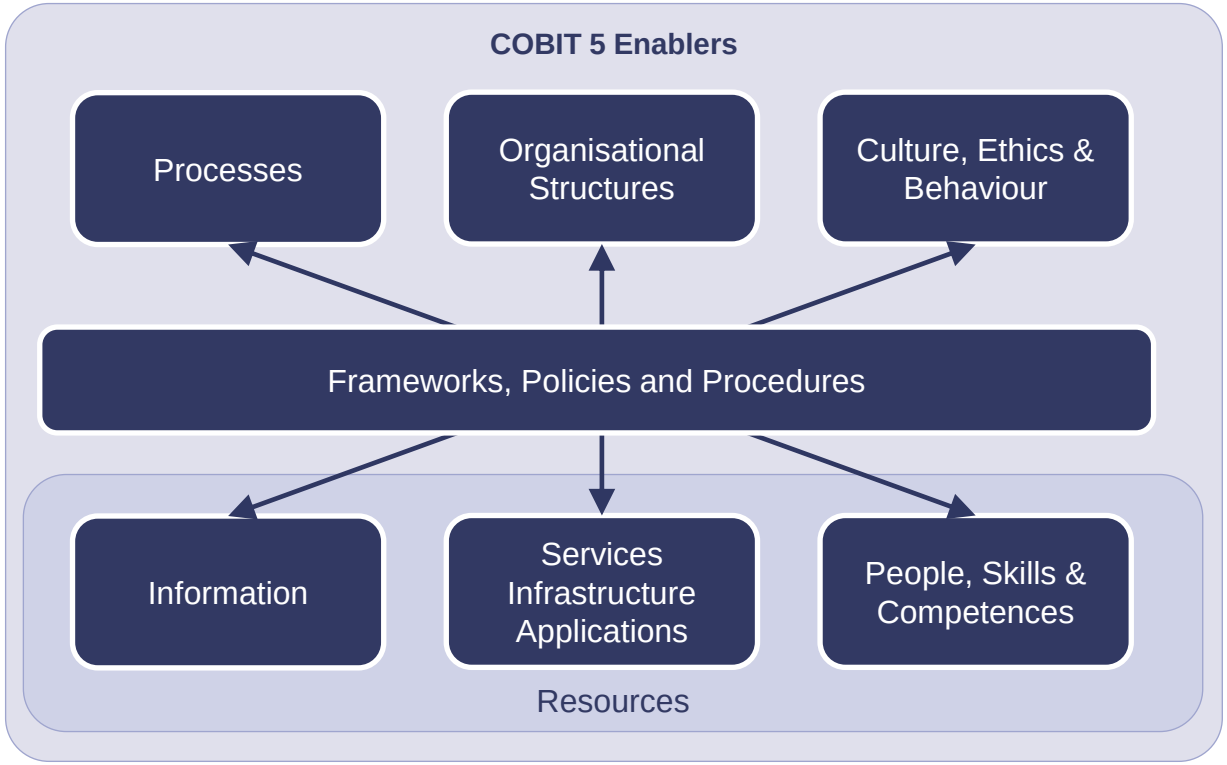
Applying a Single Integrated Framework



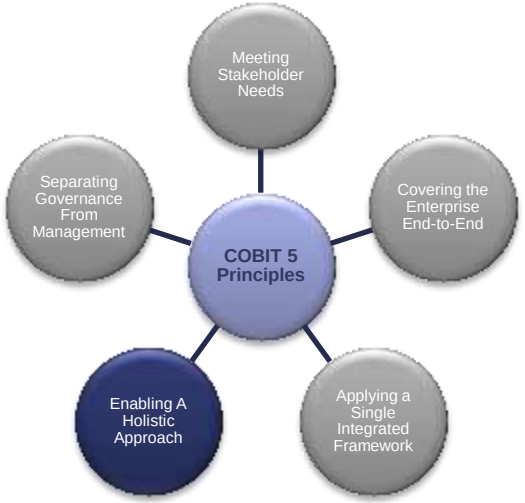
COBIT 5
AN ISACA® FRAMEWORK



Enabling a Holistic Approach



COBIT 5
AN ISACA® FRAMEWORK



Enabler Structure

Enabler Dimension

Stakeholders
- Internal Stakeholders
- External Stakeholders

Goals
- Intrinsic Quality
- Contextual Quality (Relevance, Effectiveness)
- Accessibility and Security

Life Cycle
- Plan
- Design
- Build/Acquire/ Create/Implement
- Use/Operate
- Evaluate/Monitor
- Update/Dispose

Good Practices
- Practices, Activities, Detailed Activities
- Work Products (Inputs/Outputs)

Enabler Performance Management

Metrics for Achievement of Goals (Lag Indicators)

Metrics for Application of Practice (Lead Indicators)

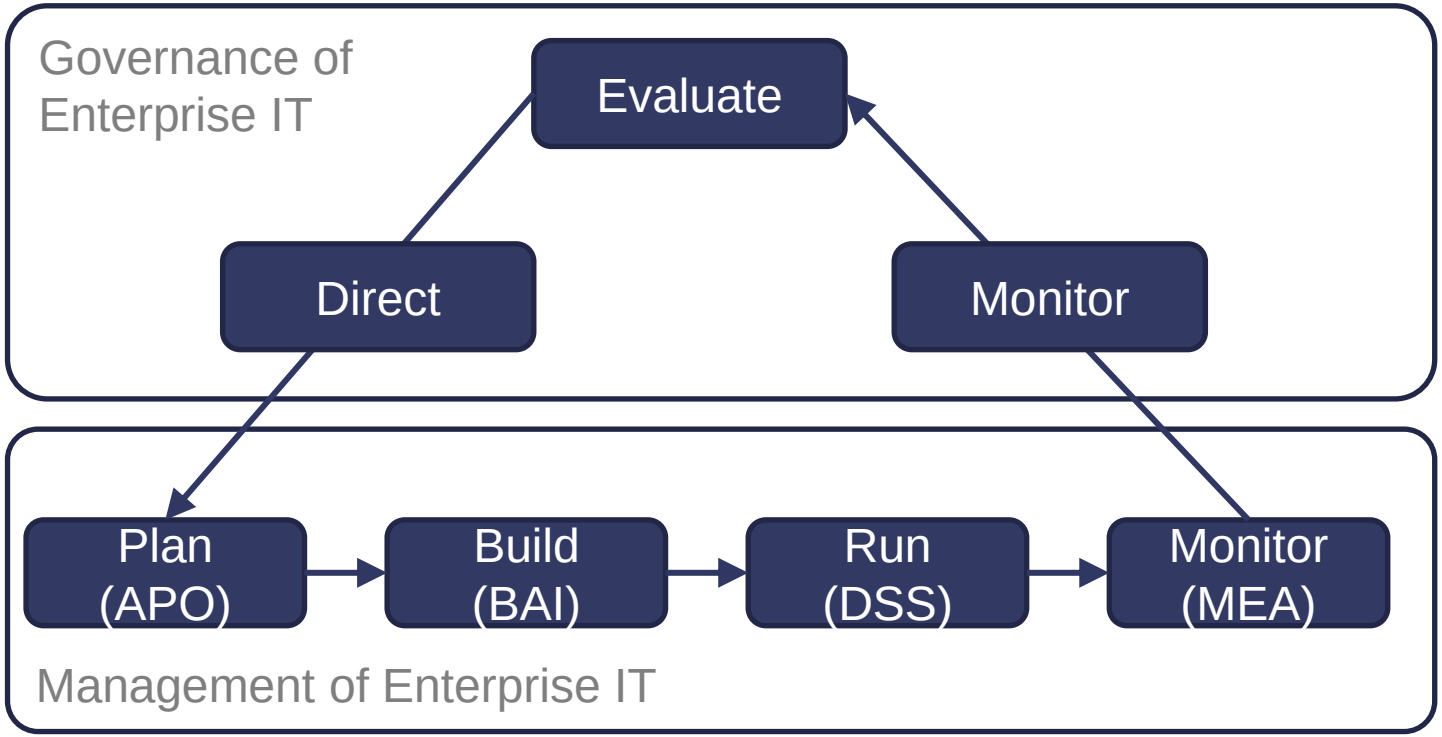
Are Stakeholder Needs Addressed?

Are Enabler Goals Achieved?

Is Life Cycle Managed?

Are Good Practices Applied?

Key Enabler: Processes



Processes for Governance of Enterprise IT

Evaluate, Direct & Monitor

- EDM1 – Set and Maintain the Governance Framework
- EDM2 – Ensure Benefits Delivery
- EDM3 – Ensure Risk Optimisation
- EDM4 – Ensure Resource Optimisation
- EDM5 – Ensure Stakeholder Transparency

Processes for Management of Enterprise IT

Align, Plan & Organise

- APO1 – Define the Management Framework for IT
- APO2 – Manage Strategy
- APO3 – Manage Enterprise Architecture
- APO4 – Manage Innovation
- APO5 – Manage Portfolio
- APO6 – Manage Budget & Costs
- APO7 – Manage Human Resources
- APO8 – Manage Relationships
- APO9 – Manage Service Agreements
- APO10 – Manage Suppliers
- APO11 – Manage Quality
- APO12 – Manage Risks
- APO13 – Manage Security

Build, Acquire & Implement

- BAI1 – Manage Programmes and Projects
- BAI2 – Define Requirements
- BAI3 – Identify & Build Solutions
- BAI4 – Manage Availability & Capacity
- BAI5 – Enable organisational Change
- BAI6 – Manage Changes
- BAI7 – Accept & Transition Changes
- BAI8 – Manage Knowledge
- BAI9 – Manage Assets
- BAI10 – Manage Configuration

Deliver, Service & Support

- DSS1 – Manage Operations
- DSS2 – Manage Service Requests & Incidents
- DSS3 – Manage Problems
- DSS4 – Manage Continuity
- DSS5 – Manage Security Administration
- DSS6 – Manage Business Process Controls

Monitor, Evaluate & Assess

- MEA1 – Monitor & Evaluate Performance and Conformance
- MEA2 – Monitor System of Internal Control
- MEA3 – Monitor and Assess Compliance with External Requirements

Processes for Governance of Enterprise IT

Evaluate, Direct & Monitor (DEM)

1. Governance Framework
2. Benefits Delivery
3. Risk Optimisation
4. Resource Optimisation
5. Stakeholder Transparency

Processes for Management of Enterprise IT

Align, Plan & Organise (APO)

1. Management Framework
2. Strategy
3. Enterprise Architecture
4. Innovation
5. Portfolio
6. Budget & Costs
7. Human Resources
8. Relationships
9. Service Agreements
10. Suppliers
11. Quality
12. Risks
13. Security Mgmt.

Build, Acquire & Implement (BAI)

1. Programs & Projects
2. Define Requirements
3. Identify & Build Solutions
4. Availability & Capacity
5. Organi-sational Change
6. Manage Changes
7. Accept & Transition
8. Knowledge
9. Assets
10. Configuration

Deliver, Service & Support (DSS)

1. Operations
2. Requests & Incidents
3. Problems
4. Continuity
5. Security Admin.
6. Business Controls

Monitor, Evaluate & Assess

1. Performance Conformance
2. System of Internal Control
3. Compliance

Prozesse für die Chefs

Behaupten, bestimmen, motzen (Evaluate, Direct & Monitor)

Wohin, sog I.
(EDM1 - Set and Maintain the Governance Framework)

Wos bringts?
(EDM2 - Ensure Benefits Delivery)

Aufpassen!
(EDM3 - Ensure Risk Optimisation)

Des geht mit weniger!
(EDM4 - Ensure Resource Optimisation)

Vastehst?
(EDM5 - Ensure Stakeholder Transparency)

Prozesse für die Hackler

Hinbiegen, raunzen und amoi schau'n (Align, Plan & Organise)

Wia, sog I.
(APO1 - Define the Management Framework for IT)

Heats zua.
(APO2 - Manage Strategy)

Wos, des ois?
(APO3 - Manage Enterprise Architecture)

Wos neigs.
(APO4 - Manage Innovation)

So vü arbeit!
(APO5 - Manage Portfolio)

Vü z'teia !
(APO6 - Manage Budget & Costs)

G'frasta.
(APO7 - Manage Human Resources)

De scho wieder!
(APO8 - Manage Relationships)

So weit und mehr ned.
(APO9 - Manage Service Agreements)

Mehr G'frasta.
(APO10 - Manage Suppliers)

Bla Bla.
(APO11 - Manage Quality)

Feig!
(APO12 - Manage Risks)

Finger weg!
(APO13 - Manage Security)

Probieren, erschleichen, hinstell'n (Build, Acquire & Implement)

Wo fang ma an?
(BAI1 - Manage Programmes and Projects)

Wos woits?
(BAI2 - Define Requirements)

Schau ma moi!
(BAI3 - Identify & Build Solutions)

Wie vü denn no?
(BAI4 - Manage Availability & Capacity)

Tats ihr amoi wos!
(BAI5 - Enable organisational Change)

Fang' ma uns net an!
(BAI6 - Manage Changes)

Fang!
(BAI7 - Accept & Transition Changes)

Sog I da ned!
(BAI8 - Manage Knowledge)

Meins!
(BAI9 - Manage Assets)

A Meins!
(BAI10 - Manage Configuration)

Gleich selber machen, helf'n und wurscht'ln (Deliver, Service & Support)

Auf geht's.
(DSS1 - Manage Operations)

Gschamster Diener.
(DSS2 - Manage Service Requests & Incidents)

Ned scho wieder.
(DSS3 - Manage Problems)

Oha!
(DSS4 - Manage Continuity)

Finger weg, wirkli!
(DSS5 - Manage Security Administration)

's Eingmochte.
(DSS6 - Manage Business Process Controls)

Motzen, raunzen, g'scheit reden (Monitor, Evaluate & Assess)

Passt scho.
(MEA1 - Monitor & Evaluate Performance and Conformance)

Na geh!
(MEA2 - Monitor System of Internal Control)

Jo eh!
(MEA3 - Monitor and Assess Compliance with External Requirements)

COBIT 5 - Österreich-Ausgabe

Jimmy Heschl

COBIT 5
AN ISACA® FRAMEWORK

Process Model

Descriptive

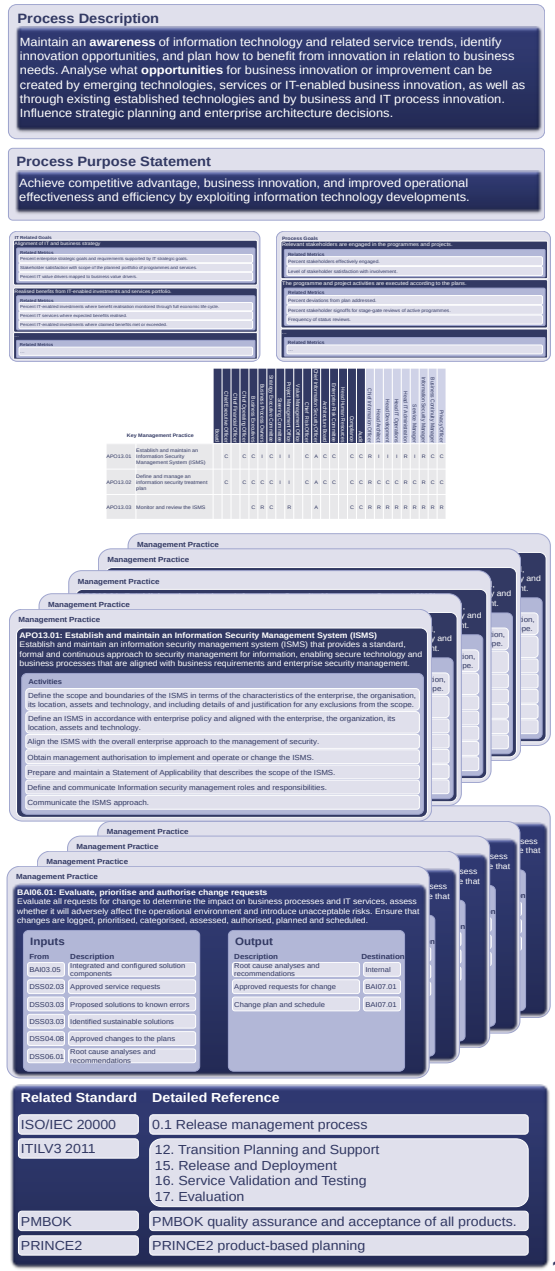
- Domain, Number, Name
- Process Description
- Process Purpose Statement

Process Management

- IT Related Goals & Metrics
- Process Goals & Metrics
- Roles & Responsibilities

Process Design & Operation

- Management Practices
- Activities
- Inputs & Outputs
- Related Guidance



Process Model

IT Stakeholder

IT Professionals

COBIT 5
AN ISACA® FRAMEWORK

Process Description &
Process Purpose Statement

Process Description

Maintain an **awareness** of information technology and related service trends, identify innovation opportunities, and plan how to benefit from innovation in relation to business needs. Analyse what **opportunities** for business innovation or improvement can be created by emerging technologies, services or IT-enabled business innovation, as well as through existing established technologies and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.

Process Purpose Statement

Achieve competitive advantage, business innovation, and improved operational effectiveness and efficiency by exploiting information technology developments.

Example from APO4 – Manage Innovation

IT Related Goals and Metrics

IT Related Goals

Alignment of IT and business strategy

Related Metrics

- Percent enterprise strategic goals and requirements supported by IT strategic goals.
- Stakeholder satisfaction with scope of the planned portfolio of programmes and services.
- Percent IT value drivers mapped to business value drivers.

Realised benefits from IT-enabled investments and services portfolio.

Related Metrics

- Percent IT-enabled investments where benefit realisation monitored through full economic life cycle.
- Percent IT services where expected benefits realised.
- Percent IT-enabled investments where claimed benefits met or exceeded.

…

Related Metrics

- …

Example from:
BAI01 – Manage Programmes and Projects

COBIT 5
AN ISACA® FRAMEWORK

Process Goals and Metrics

Process Goals

Relevant stakeholders are engaged in the programmes and projects.

Related Metrics

- Percent stakeholders effectively engaged.
- Level of stakeholder satisfaction with involvement.

The programme and project activities are executed according to the plans.

Related Metrics

- Percent deviations from plan addressed.
- Percent stakeholder signoffs for stage-gate reviews of active programmes.
- Frequency of status reviews.

…

Related Metrics

- …

Is good practice applied?

Example from:
BAI01 – Manage Programmes and Projects

RACI Chart

Key Management Practice		Board	Chief Executive Officer	Chief Financial Officer	Chief Operating Officer	Business Executives	Business Process Owners	Strategy Executive Committee	Steering Committee	Project Management Office	Value Management Office	Chief Risk Officer	Chief Information Security Officer	Architecture Board	Enterprise Risk Committee	Head Human Resources	Compliance	Audit	Chief Information Officer	Head Architect	Head Development	Head IT Operations	Head IT Administration	Service Manager	Information Security Manager	Business Continuity Manager	Privacy Officer
APO13.01	Establish and maintain an Information Security Management System (ISMS)		C		C	C	I	C	I	I		C	A	C	C		C	C	R	I	I	I	R	I	R	C	C
APO13.02	Define and manage an information security treatment plan		C		C	C	C	C	I	I		C	A	C	C		C	C	R	C	C	C	R	C	R	C	C
APO13.03	Monitor and review the ISMS					C	R	C		R			A				C	C	R	R	R	R	R	R	R	R	R

Who?

Example from APO13 – Manage Security

RACI: Who is **R**esponsible (Zuständig)
Accountable (Verantwortlich)
Consulted (Befragt)
Informed (Informiert)

COBIT 5
AN ISACA® FRAMEWORK

Management Practice & Activities

Management Practice

APO13.01: Establish and maintain an Information Security Management System (ISMS)
Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management.

Activities

- Define the scope and boundaries of the ISMS in terms of the characteristics of the enterprise, the organisation, its location, assets and technology, and including details of and justification for any exclusions from the scope.
- Define an ISMS in accordance with enterprise policy and aligned with the enterprise, the organization, its location, assets and technology.
- Align the ISMS with the overall enterprise approach to the management of security.
- Obtain management authorisation to implement and operate or change the ISMS.
- Prepare and maintain a Statement of Applicability that describes the scope of the ISMS.
- Define and communicate Information security management roles and responsibilities.
- Communicate the ISMS approach.

Good Practice

Example from APO13 – Manage Security

Inputs & Outputs

Management Practice

BAI06.01: Evaluate, prioritise and authorise change requests

Evaluate all requests for change to determine the impact on business processes and IT services, assess whether it will adversely affect the operational environment and introduce unacceptable risks. Ensure that changes are logged, prioritised, categorised, assessed, authorised, planned and scheduled.

Inputs

From	Description
BAI03.05	Integrated and configured solution components
DSS02.03	Approved service requests
DSS03.03	Proposed solutions to known errors
DSS03.03	Identified sustainable solutions
DSS04.08	Approved changes to the plans
DSS06.01	Root cause analyses and recommendations

Output

Description	Destination
Root cause analyses and recommendations	Internal
Approved requests for change	BAI07.01
Change plan and schedule	BAI07.01

Resources

Results

Example from BAI06 – Manage Changes

COBIT 5
AN ISACA® FRAMEWORK

Related Guidance

Related Standard	Detailed Reference
ISO/IEC 20000	0.1 Release management process
ITILV3 2011	12. Transition Planning and Support 15. Release and Deployment 16. Service Validation and Testing 17. Evaluation
PMBOK	PMBOK quality assurance and acceptance of all products.
PRINCE2	PRINCE2 product-based planning

Example from APO07 – Accept and Transition Changes

COBIT 5
AN ISACA® FRAMEWORK

COBIT 5 Implementation Guide

- Positioning GEIT within an enterprise
- Taking the first steps towards improving GEIT
- Implementation challenges and success factors
- Enabling GEIT- related organisational and behavioural change
- Implementing continual improvement that includes change enablement and programme management
- Using COBIT 5 and its components

ISO/IEC 27002:2005

ISO/IEC 27002:2005

- **Historie:**
  - CoP for Security Management
  - BS7799 Part 1
  - ISO 17799:2000, 2005
- **Best Practice für Informations-Sicherheit**
- **Herausgegeben von der ISO**
- **Zeitweise im Konflikt mit BSI - Grundschutzhandbuch**
- **Zertifizierung nach ISO/IEC 27001:2005 (BS7799 Part 2)**

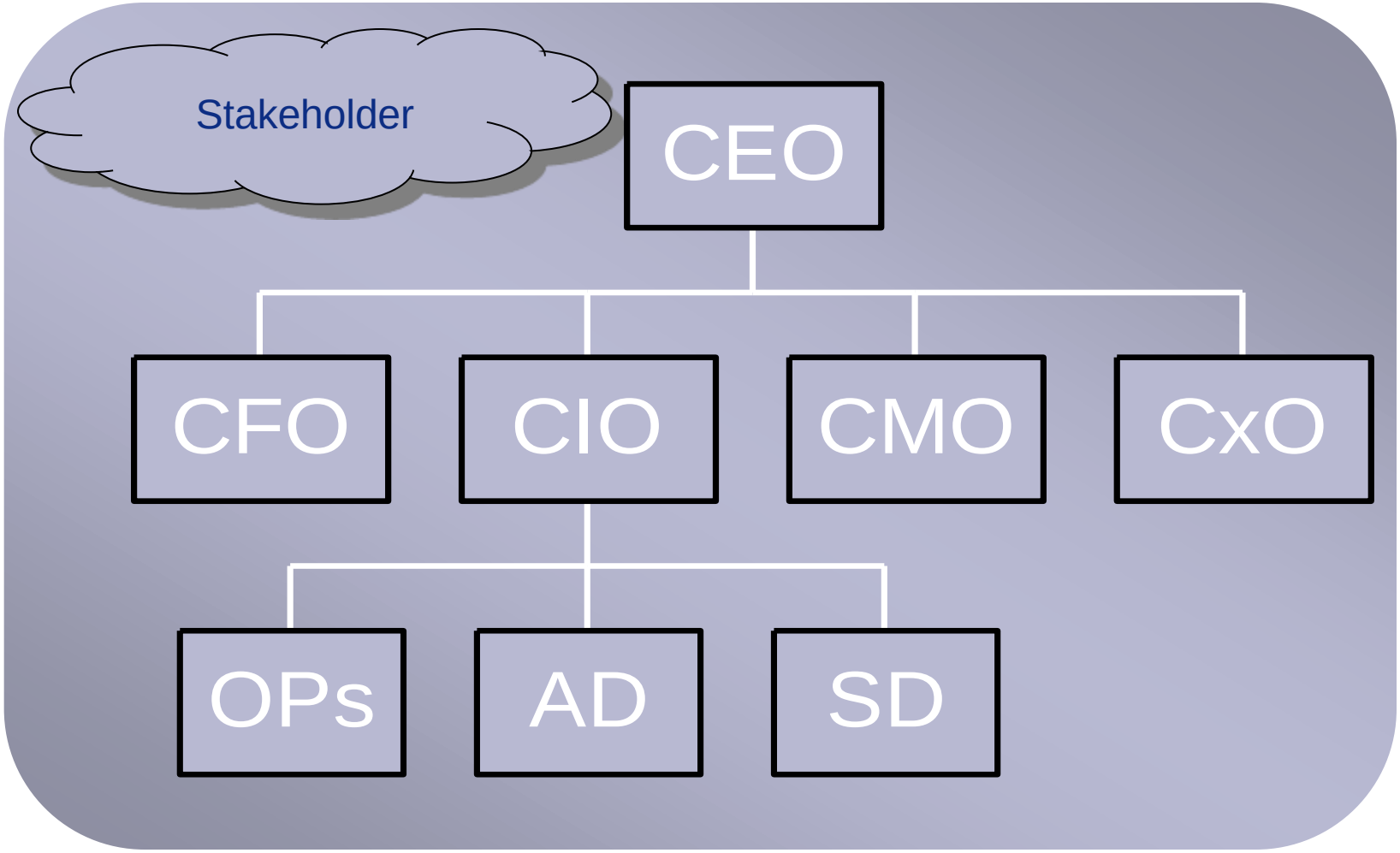
Integration von Standards

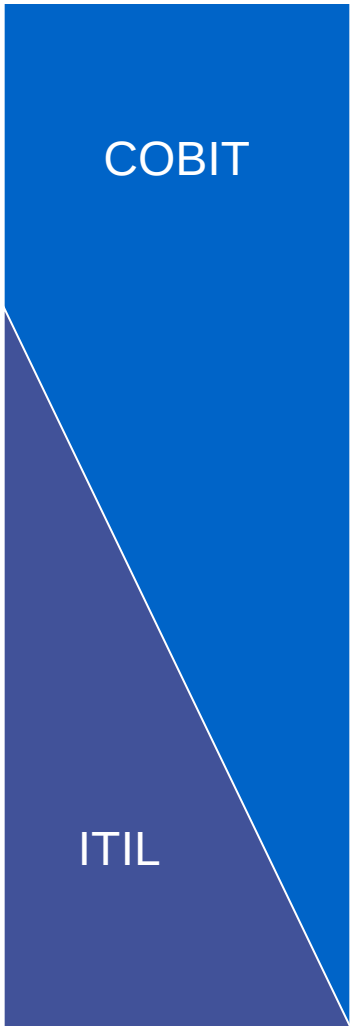
Die Stimme der anderen …

- **Establish frameworks to ease Governance Implementation**
  - First COBIT for overall governance
  - Then ITIL for service delivery and management
  - Then ISO 17799 for information security
  - Balanced Scorecard for measurement and communication

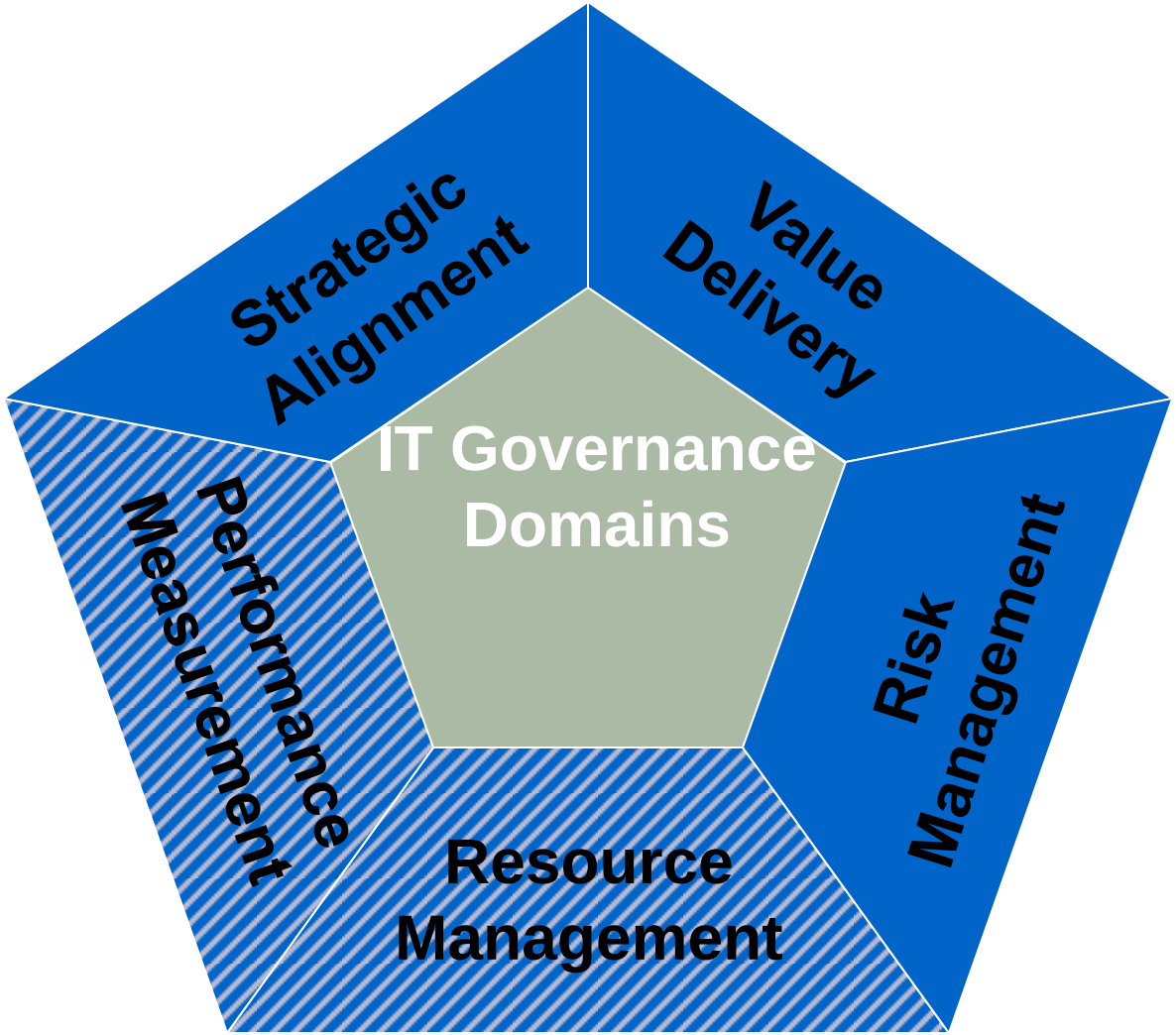
Quelle: Forrester
Helping Business Thrive On Technology Change
A Road Map To Comprehensive IT Governance
by Craig Symons, Jan 2006

Potential COBIT & ITIL





Potential COBIT & ITIL

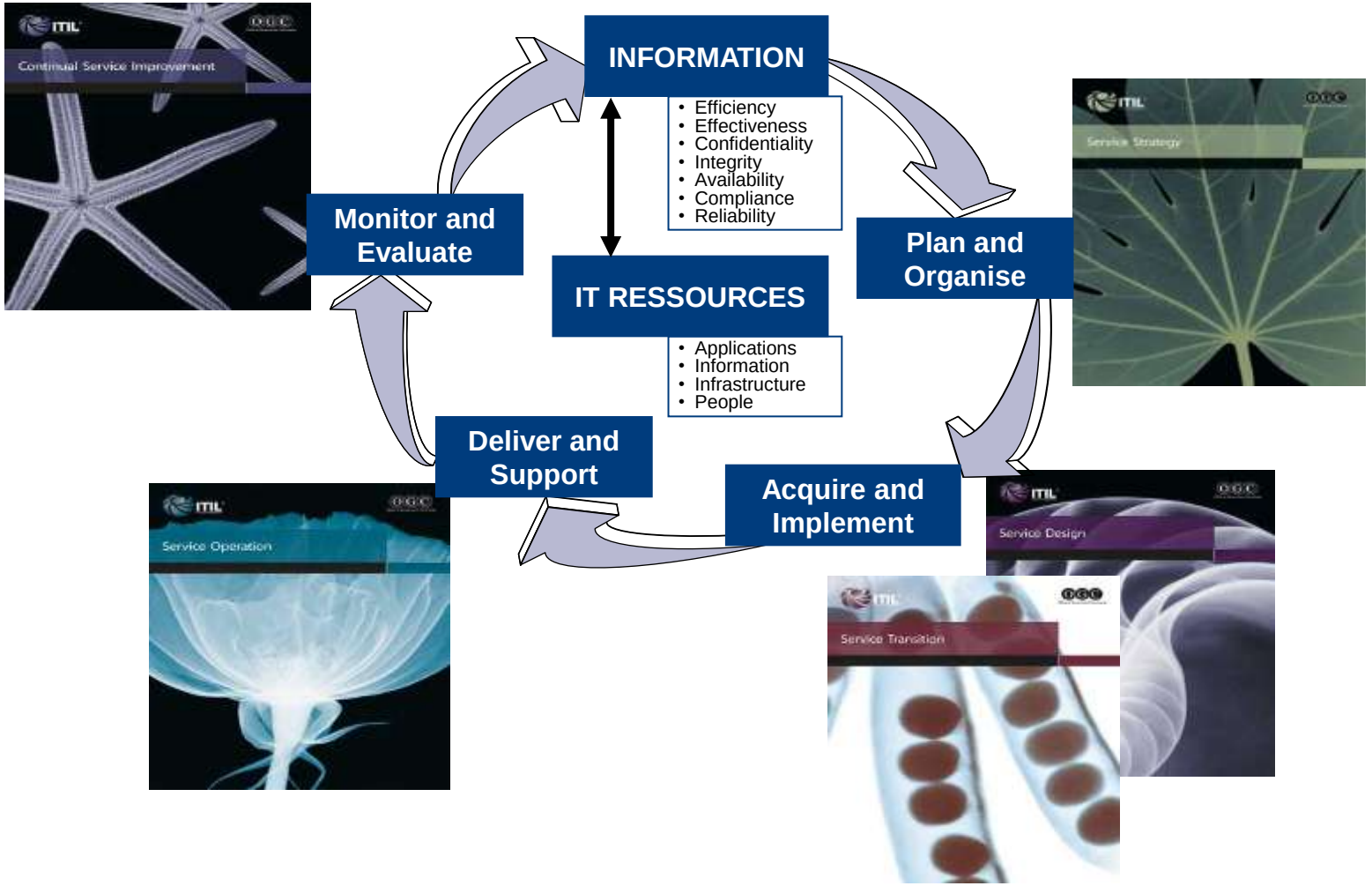


COBIT

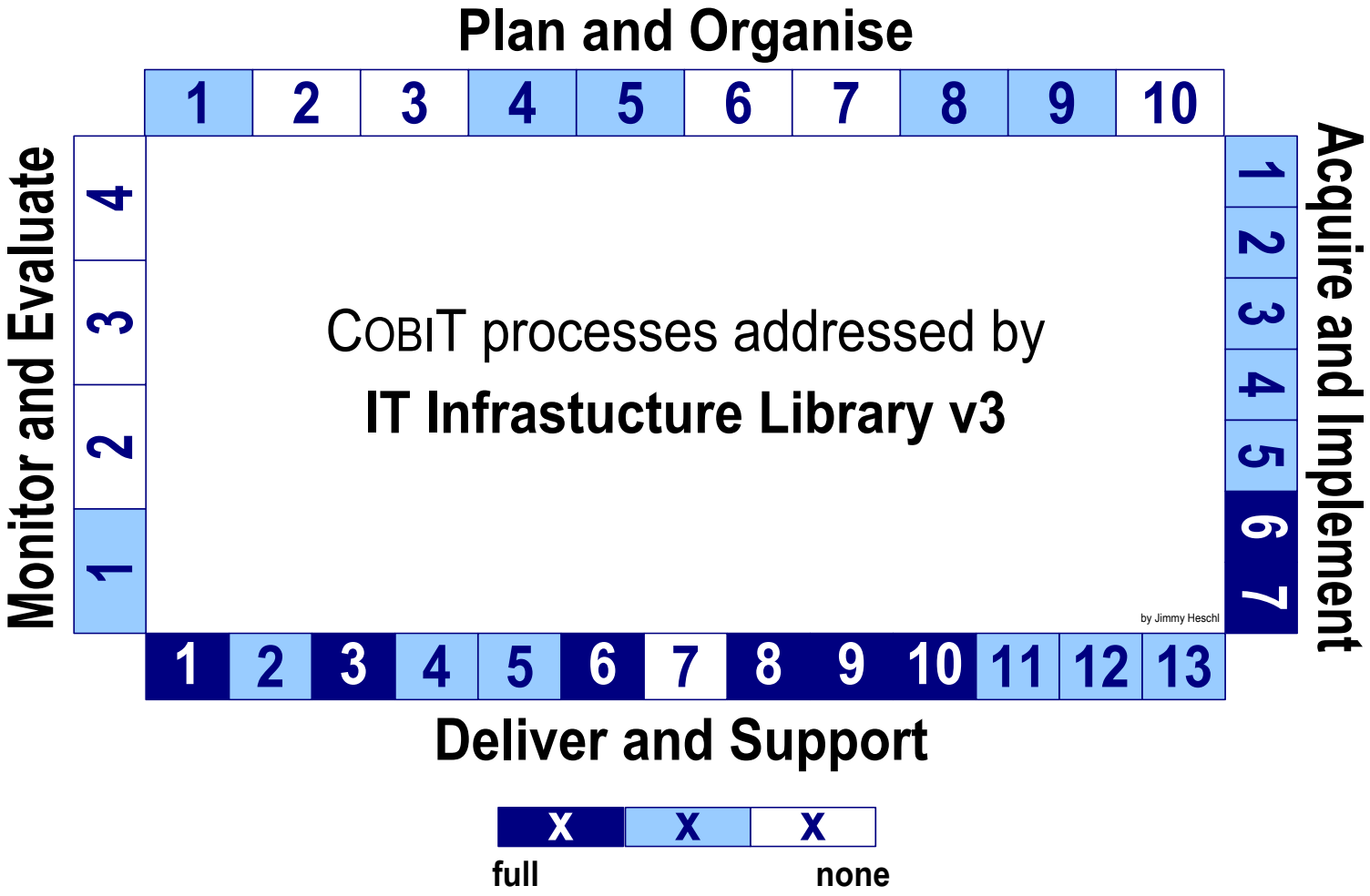
both

ITIL

ITIL v3 Highest-Level Mapping



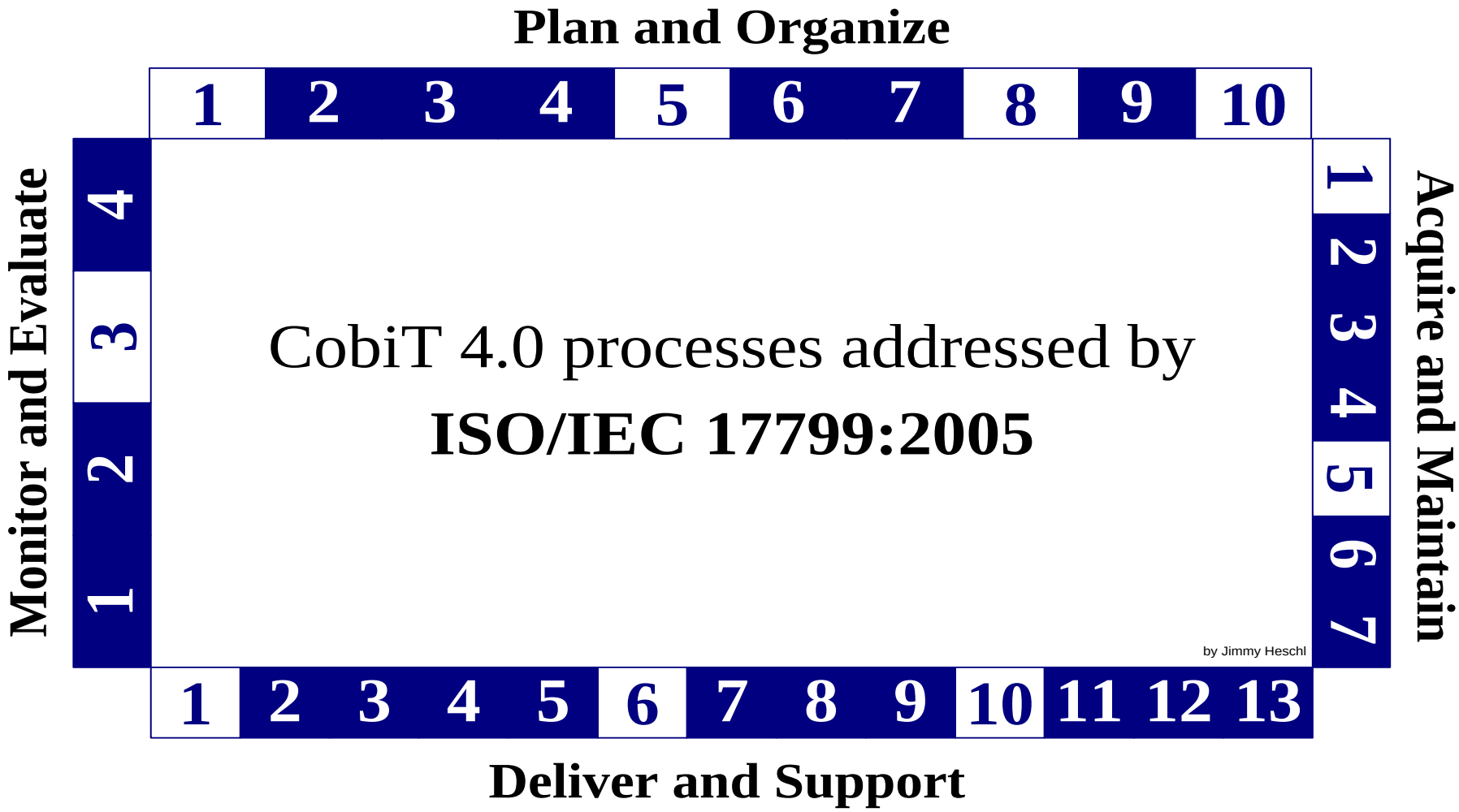
ITIL v3 High-Level Mapping



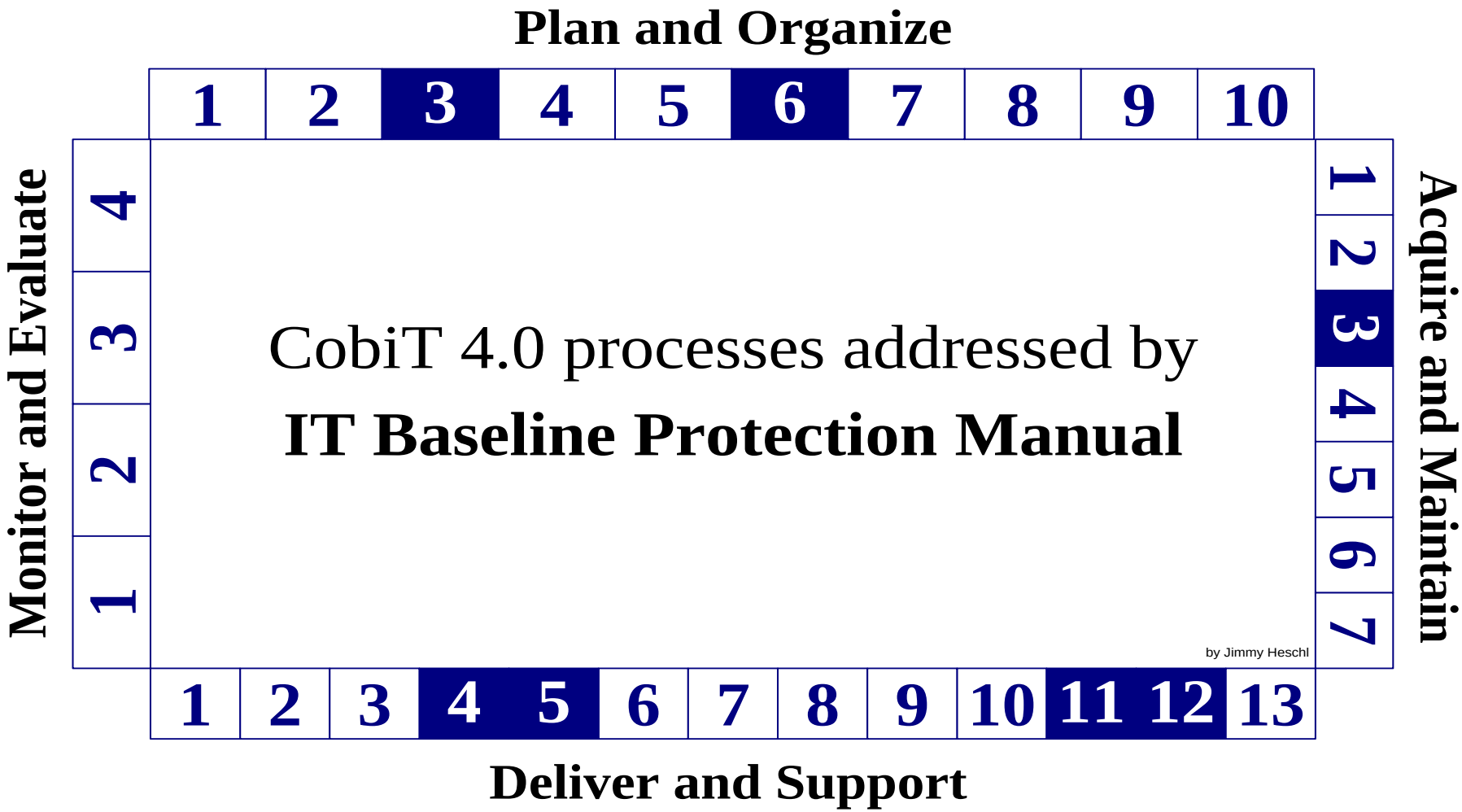
ITIL v3 Detailled Mapping (excerpt)

CobiT		ITIL	Coverage
Control Objective	**Name**		
PO1	Define a Strategic IT Plan	SS 1 Introduction SS 2 Service management as a practice SS 3 Service Strategy principles SS 3.5 Service Strategy fundamentals SS 4 Service strategy …	A+
PO1.1	IT Value Management	SS 2.2 What are services? SS 3.1 Value creation SS 3.4 Service structures SS 4.4 Prepare for execution SS 5.1 Financial Management SS 5.2 Return on Investment SS 5.3 Service Portfolio Management	C
PO1.2	Business-IT Alignment	SS 2.1 What is service management SS 2.3 The business process SS 2.4 Principles of service management	C
PO1.3	Assessment of Current Capability and Performance	SS 4.4 Prepare for execution CSI 5.2 Assessments	C
PO1.4	IT Strategic Plan	SS 3.3 Service provider types SS 3.5 Service Strategy fundamentals SS 4.1 Define the market SS 4.2 Develop the offerings SS 4.3 Develop strategic assets …	C
PO1.5	IT Tactical Plans	SS 4.4 Prepare for execution SS 7.1 Implementation through the lifecycle SS 7.2 Strategy and Design …	C

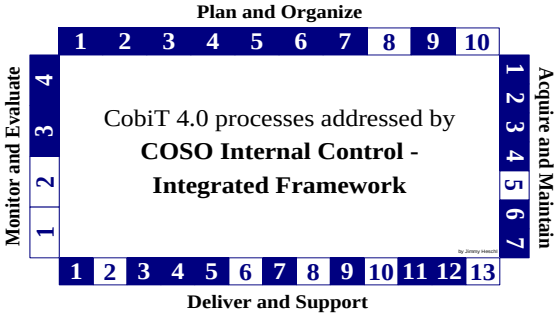
COBIT & ISO/IEC 27002

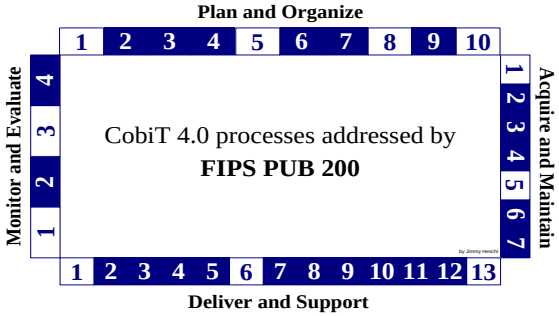


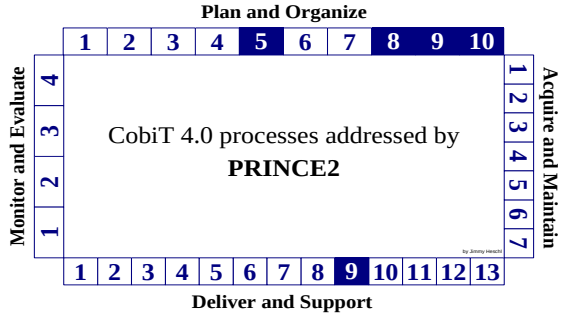
COBIT & BSI Grundschutzhandbuch

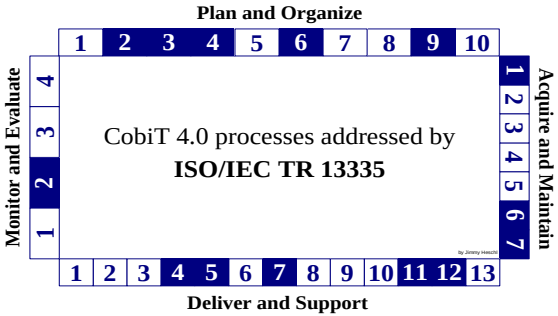


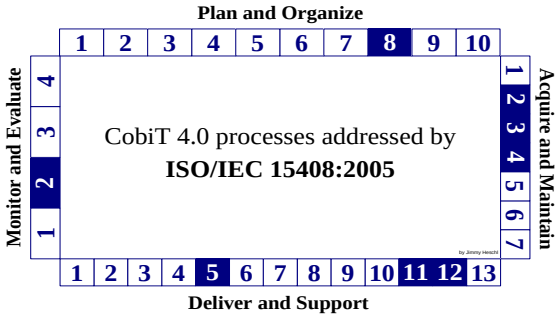
COBIT & viele andere …

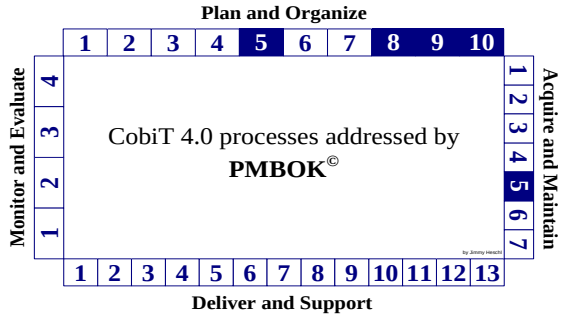


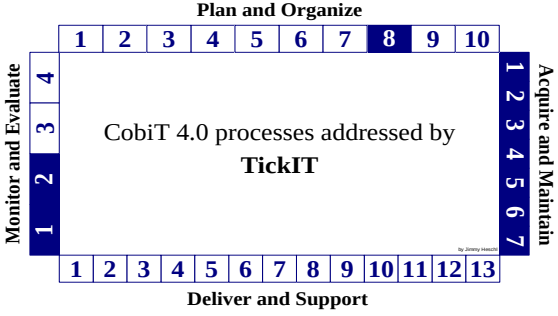


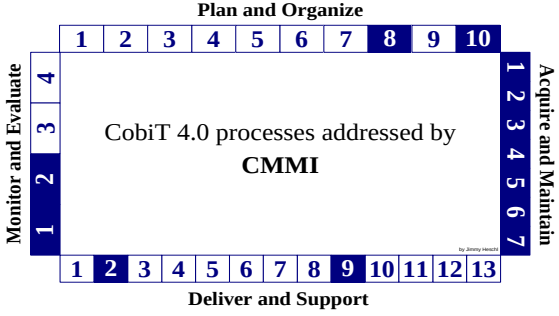


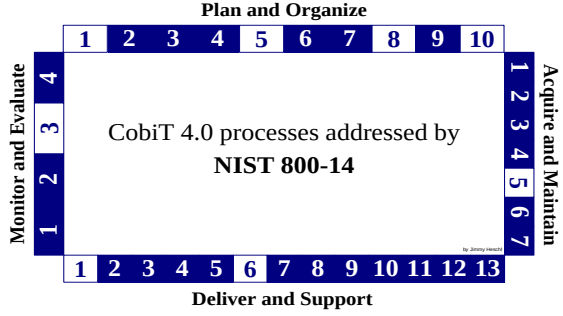




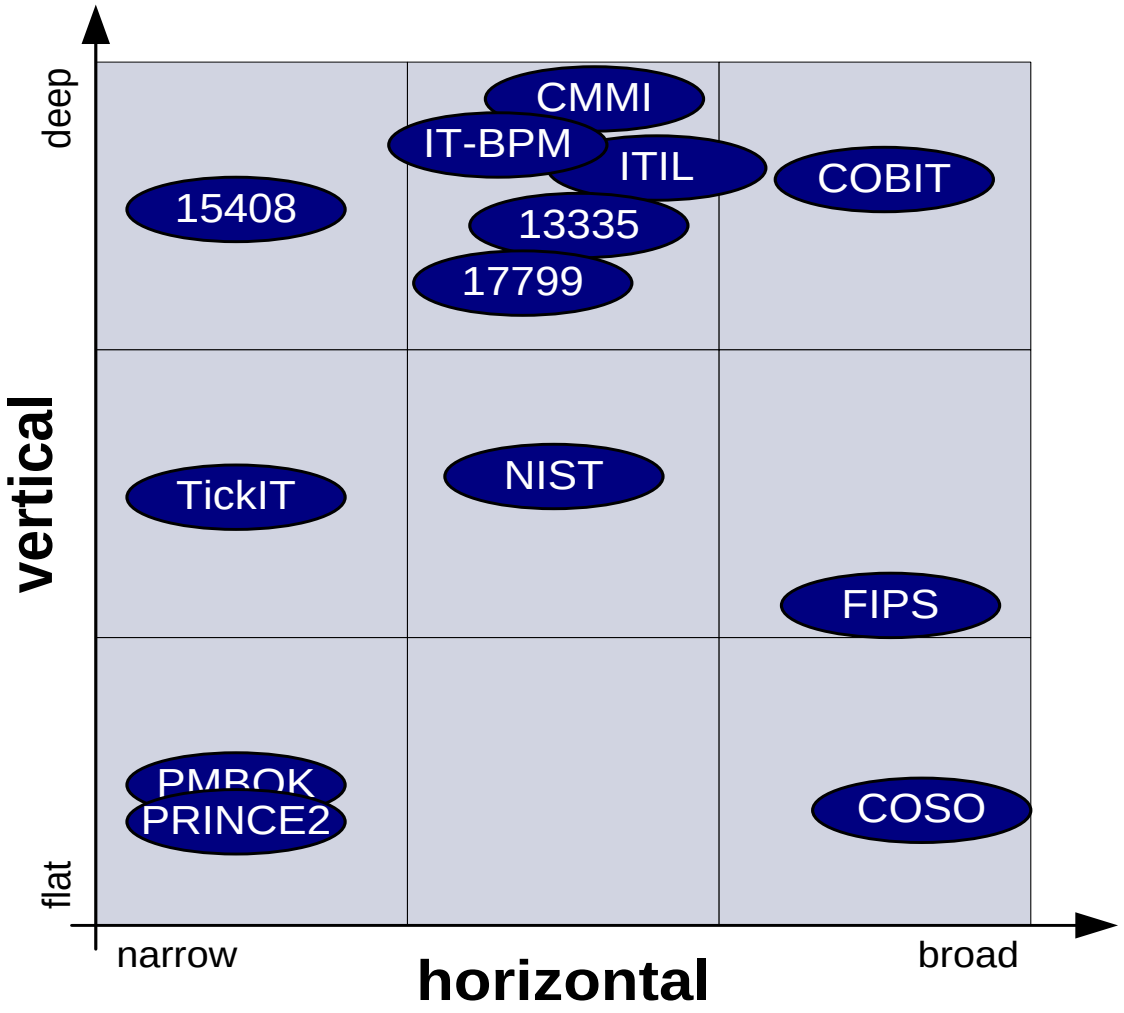








Vergleich von Standards



Umsetzung & Ausblick

Aufgaben und Rollen

- **Berater ist verantwortlich für**
  - Vorbereitung und Moderation der Workshops
  - Mediator bei Problemen
  - Coaching der Process Owner
  - Beibringung von Best Practices und Empfehlungen
  - Beibringung von Modellprozessen, Vorlagen, Beispielen, etc
- **Process Owner ist verantwortlich für**
  - Vorbereitung, Teilnahme und Nachbereitung der Workshops
  - Beibringung von speziellen Prozessinformationen
  - Koordination mit weiteren Ansprechpersonen
  - zukünftige Umsetzung und laufende Verbesserung des Prozesses (auch ohne Berater)
  - Umsetzung von Änderungen
  - Aufzeigen von möglichen Problemen und Mitarbeit an der Lösung
- **Beide sind verantwortlich für**
  - Teamarbeit
  - Die Qualität des Prozesses
  - Den Erfolg des Projektes

Nutzen durch IT Governance

- Aufbau eines angemessenen Internen Kontrollsystems (§ 82 AktG), auch nach den neuen strengeren US-Regelungen (Sarbanes-Oxley)
- Unterstützung bei der Erhöhung des Shareholder Value
- Absicherung des Vorstandes
- Ausrichtung der IT an den Unternehmensstrategien
- Umsetzung sämtlicher international relevanter Standards (ITIL, CMM, ISO 2700x,…) unter dem COBIT-Rahmenwerk
- Qualitätssteigerung in der IT
- Geplante Steuerung der Prozess-Reifegrade (Maturity Model)
- Optimierte Steuerung und Messung der IT
- Effizienzsteigerung in der IT
- Nachweisbarer Nutzen der IT

Ausblick

- **Die Zeit ist reif**
  - Für nachvollziehbare und messbare IT Prozesse
  - Einhaltung internationaler Standards
  - Interne Kontrollsysteme auch in der IT
- **Die Umsetzung erfordert (hohen) Aufwand**
- **Nutzen ist auch kurzfristig zu erzielen (ROI hoch)**
- **Professionelle Unterstützung empfehlenswert – besonders auch mit Prüfungs- und Kontroll – Know How**

Wenn der Wind stark weht,
bauen die einen Mauern,
die anderen Windmühlen!

(chin. Weisheit)

Thank You!

Contact Information:

Jimmy Heschl

eMail: jimmy@heschl.at

Facebook: jimmyheschl

Skype: jimmyheschl

Abkürzungsverzeichnis

AC	Application Control
AD	Application Development
AI	Acquire and Implement
AICPA	American Institute of CPAs
AktG	Aktiengesetz
BAO	Bundesabgabenordnung
BCP	Business Continuity/Contingency Planning
BS	British Standard
BSC	Balanced Scorecard
BWG	Bankwesengesetz
CAB	Change Advisory Board
CAB/EC	Change Advisory Board for Emergency Changes
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CI	Configuration Item
CIO	Chief Information Officer
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CMDB	Configuration Management Database
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integrated
CMO	Chief Marketing Officer
COBIT	COBIT
COSO	Committee of Sponsoring Organisations
DB	Database
DS	Deliver and Support
DSG	Datenschutzgesetz
ECV	Emittenten-Compliance-Verordnung
FAIT	Fachgutachten zur Prüfung der IT
FIPS	Federal Information Processing Standard
FS DV	Fachsenat für Datenverarbeitung
FS HR	Fachsenat für Handelsrecht
FSC	Forward Schedule of Changes
GEIT	Governance of Enterprise IT
GoB	Grundsätze ordnungsgemäßer Buchführung
GSHB	Grundschutzhandbuch
HIPAA	Health Insurance Portability and Accountability Act
HW	Hardware
ICOFR	Internal Control Over Financial Reporting
ICT	Information and Communication Technology
IDW	Institut der Wirtschaftsprüfer
IEC	International Electro technical Commission
IFAC	International Federation of Accountants
IKS	Internes Kontrollsystem
IRM	Information Risk Management
ISA	International Standards on Auditing
ISACA	Information Systems Audit and Control Association
ISO	International Standardisation Organisation
ISP	Internet Service Provider
IT	Informationstechnologie, Information and related Technology
IT-BPM	IT Baseline Protection Manual
ITGC	IT General Controls
ITGI	IT Governance Institute
ITIL	IT Infrastructure Library
ITIM	IT Infrastructure Management
ITSM	IT Service Management
KFS	Kammer Fachsenat für Datenverarbeitung
KFS/DV1	Fachgutachten 1 des KFS
KFS/DV2	Fachgutachten 2 des KFS
KGI	Key Goal Indicator
KonTraG	Kontroll- und Transparenzgesetz
KPI	Key Performance Indicator
ME	Monitor and Evaluate
MEIT	Managementof Enterprise IT
NIST	National Information Security and Technology
OP	Operation
PC	Process Control
PCAOB	Public Company Accounting Oversight Board
PMBOK	Project Management Body of Knowledge
PO	Plan and Organise
PRINCE	Projects in Controlled Environments
PS	Prüfungsstandard
PSA	Projected Service Availability
RFC	Request for Change
ROI	Return-On-Investment
RZ	Rechenzentrum
SAS	Statement on Auditing Standard
SD	Service Desk
SLA	Service Level Agreement
SLM	Service Level Management
SLR	Service Level Requirements
SOX	Sarbanes Oxley Act
SQP	Service Quality Plan
SW	Software
UC	Underpinning Contract