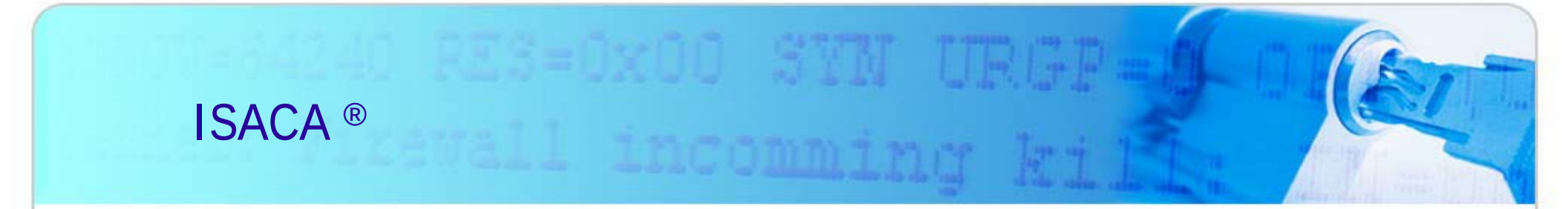
sec4you
Advanced IT-Audit Services Ges.m.b.H.

Cobit®

Initiative Informationssicherheit Austria, 29. März 2007

Ein Vortrag von Manfred Scholz CISA ®, CISM ®

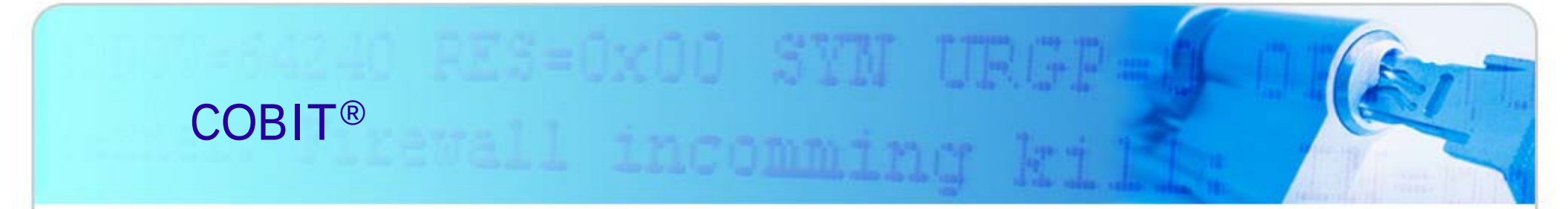
ISACA ®



Information Systems Audit and Control Association

- Ursprünglich ein Berufsverband der Spezialisten für IT- Revision
- 1969 gegründet
- Entwickelte sich in Richtung IT-Governance
- IT-Governance Institute
- weltweit, ca. 50.000 Mitglieder in ca. 140 Ländern
- definiert Standards
- Zertifizierungen, CISA seit 1978 (50000) und CISM seit 2002 (6000)
- www.isaca.org
- www.itgi.com

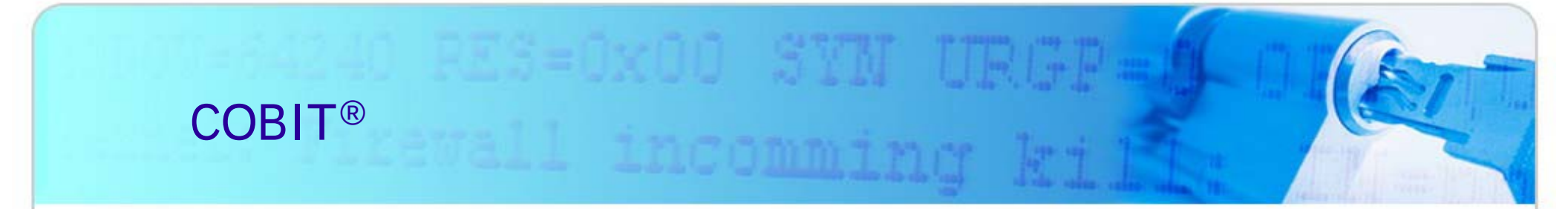
COBIT®



Control Objectives for Information and Related Technology

- International anerkannter Standard zur Prüfung von IT-Systemen
- Synthese von 36 nationalen und internationalen Standards
- Definierte Kontrollziele für IT Prozesse
- Steuerung, Messung oder Prüfung von IT-Prozessen
- Daimler/Chrysler, Philips, Magna Steyr, VA TECH
- Ausgangsbasis für IT-Prüfungen des Bundesrechnungshofes

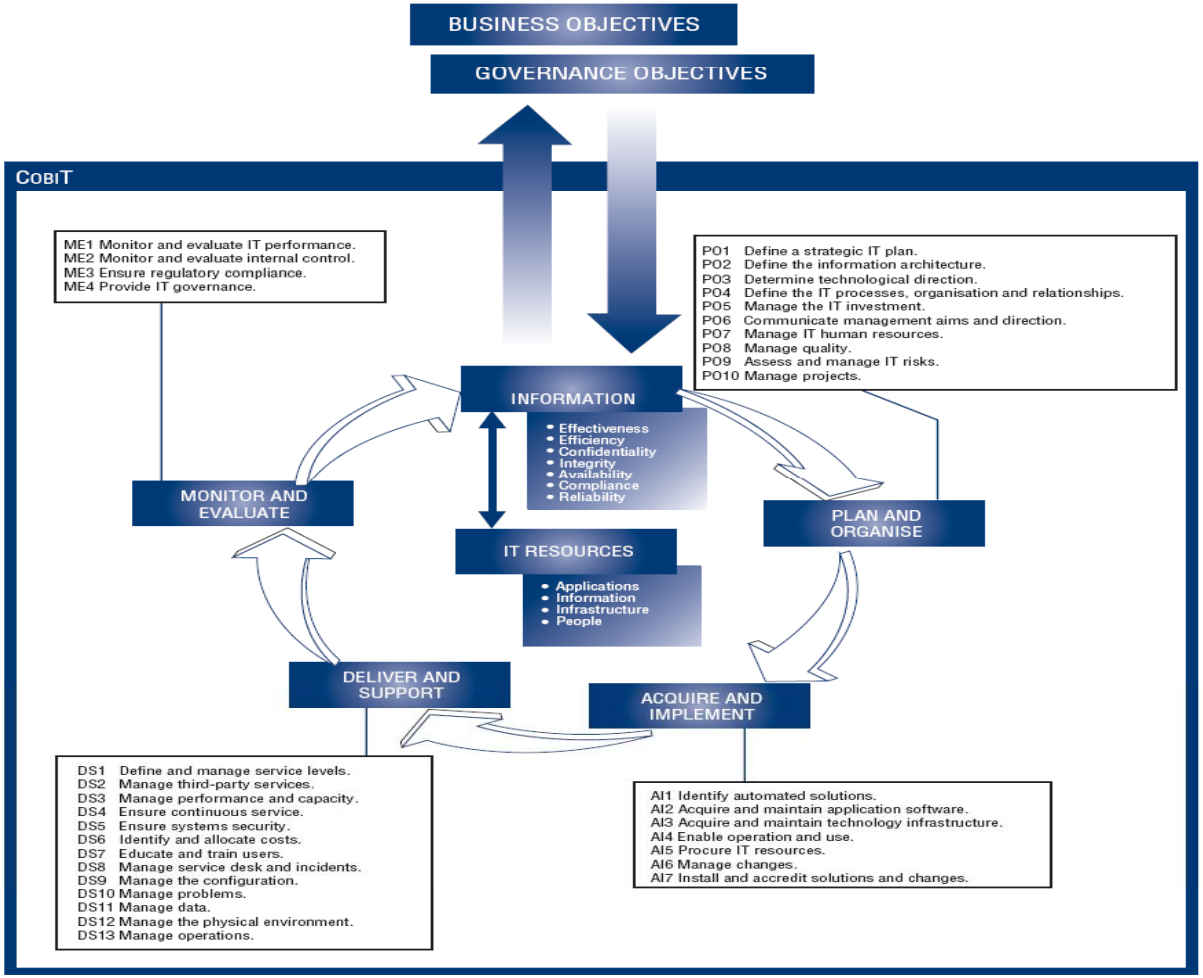
COBIT®



Eingeflossene Standards:

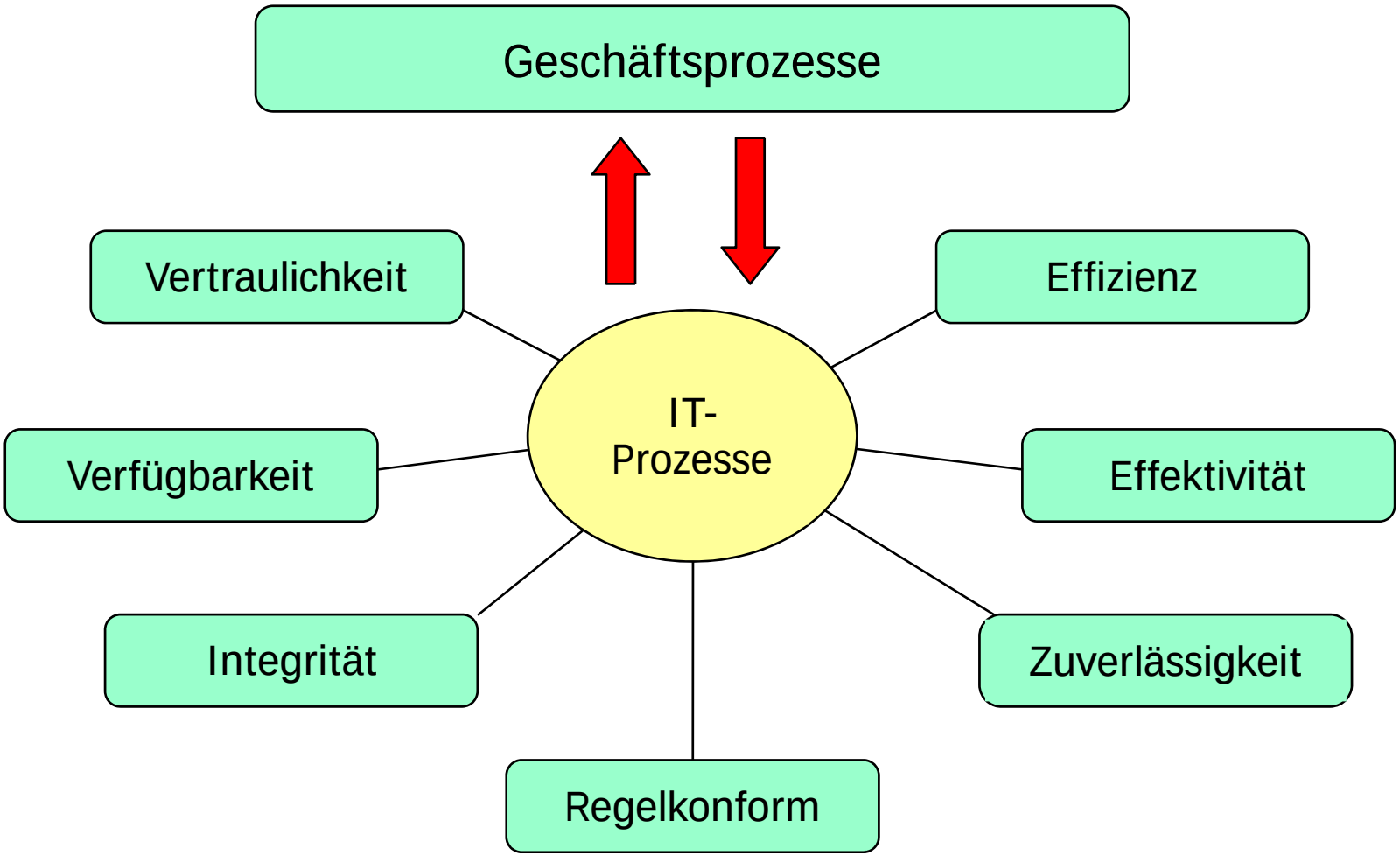
- Technisch: ISO, EDIFACT, uva.
- Geschäftspraktiken: EU, OECD, ISACA, uva.
- Qualifikationskriterien: ITSEC, TCSEC, ISO 9000, CC, SPICE, uva.
- Berufsstandards: COSO, IFAC, AICPA, IIA, GAO, uva.
- Industriepraktiken: ESF 14, IBAG, NIST, DTI, uva.
- Neue industriespez. Anforderungen

COBIT®

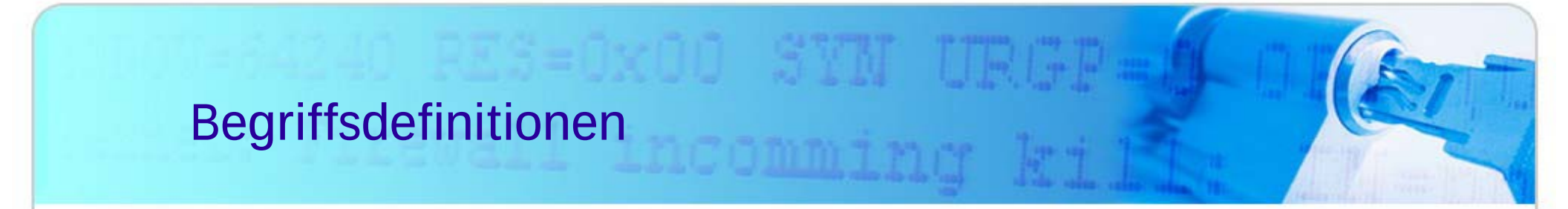


Quelle: COBIT 4.0

COBIT®


Geschäftsprozesse
Vertraulichkeit
Effizienz
IT-
Prozesse
Verfügbarkeit
Effektivität
Integrität
Zuverlässigkeit
Regelkonform

Begriffsdefinitionen

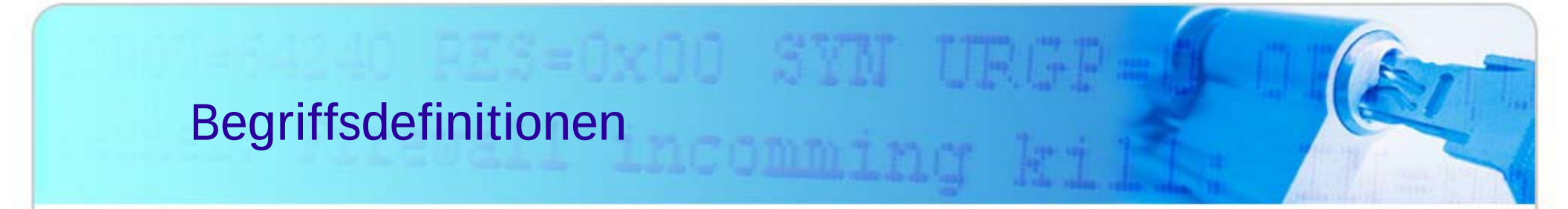


IT-Governance

ist die Verantwortung von Führungskräften und Aufsichtsräten
und besteht aus Führung, Organisationsstrukturen und Prozessen,
die sicherstellen, dass die Unternehmens-IT dazu beiträgt,
Die Organisationsstrategie und -ziele zu erreichen und zu erweitern.

Quelle: COBIT 4.0

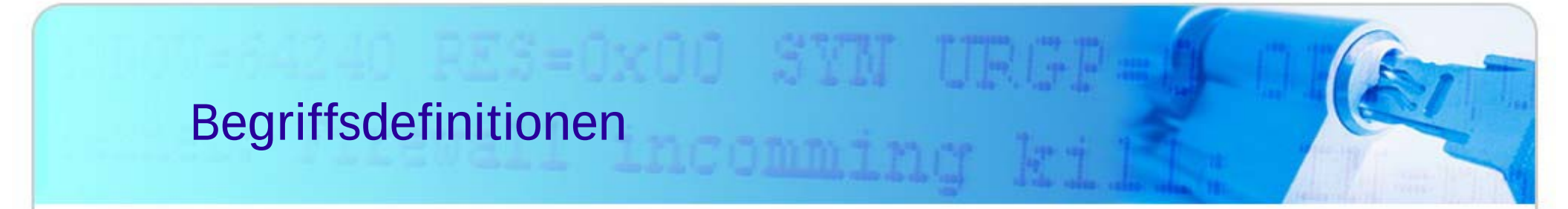
Begriffsdefinitionen



IT-Governance

- Einführung eines internen Kontroll-/ Steuerungssystems (IKS)
- IT ist an das Kerngeschäft ausgerichtet
- IT unterstützt das Geschäft und maximiert den Gewinn
- IT-Ressourcen werden verantwortungsvoll eingesetzt
- IT-Risiken werden angemessen verwaltet (Risikomanagement)
- Messung der Performance

Begriffsdefinitionen



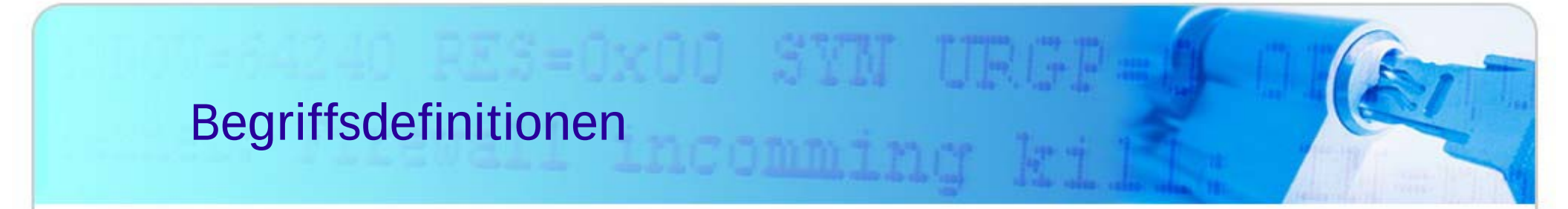
Control (Kontrolle)

- Maßnahme (z.B. Richtlinie, Passwort, ua)
- Das Risiko unvorhergesehener Ereignisse soll vermindert bzw beherrscht werden
- Verhinderung, Erkennung oder Korrektur
- Geschäftsziel wird mit höherer Wahrscheinlichkeit erreicht

> Control is defined as
> the policies, procedures, practices and organisational
> Structures designed to provide reasonable assurance
> that business objectives will be achieved and that
> Undesired events will be prevented or detected
> and corrected.

Quelle: COBIT 3rd Edt. – Executive Summary

Begriffsdefinitionen



Control Objective (Kontrollziel)

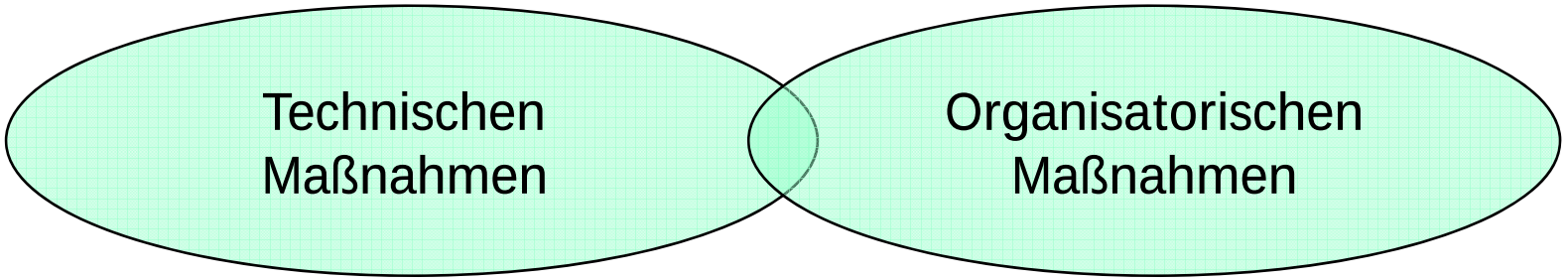
- Definiertes Ziel eines IT-Prozesses
- Wird durch wirksame „controls“ erreicht

> IT Control Objective is defined as
> a statement of the desired result or
> purpose to be achieved by implementing
> control procedures in a
> particular IT activity.

Quelle: COBIT 3rd Edt. – Executive Summary

Controls (Maßnahmen)

Kombination bestehend aus

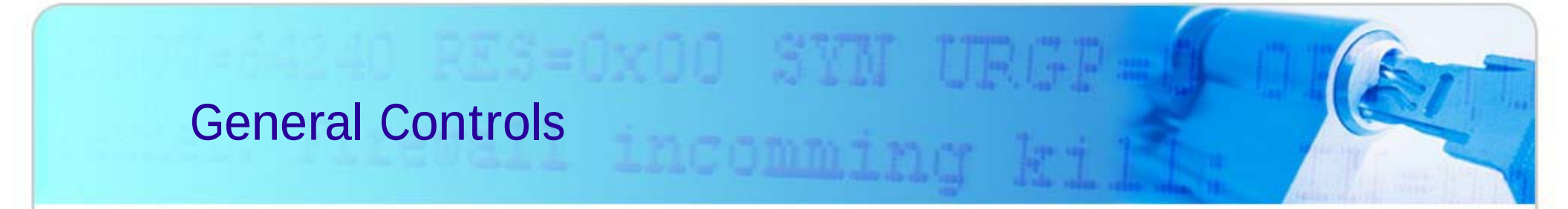


Mit erhöhter Wahrscheinlichkeit werden unvorhergesehene Ereignisse **verhindert**, **erkannt** oder **korrigiert** und so das Geschäftsziel erreicht.

Controls (Maßnahmen)

Preventive	Detective	Corrective
Funktionentrennung	Prüfsummen	Notfallpläne
Zutrittskontrolle	Reports	Backup-Prozeduren
Eingabeüberprüfung	Interne Revision	Neustart von Diensten
Schulung	Fehlermeldungen	

General Controls

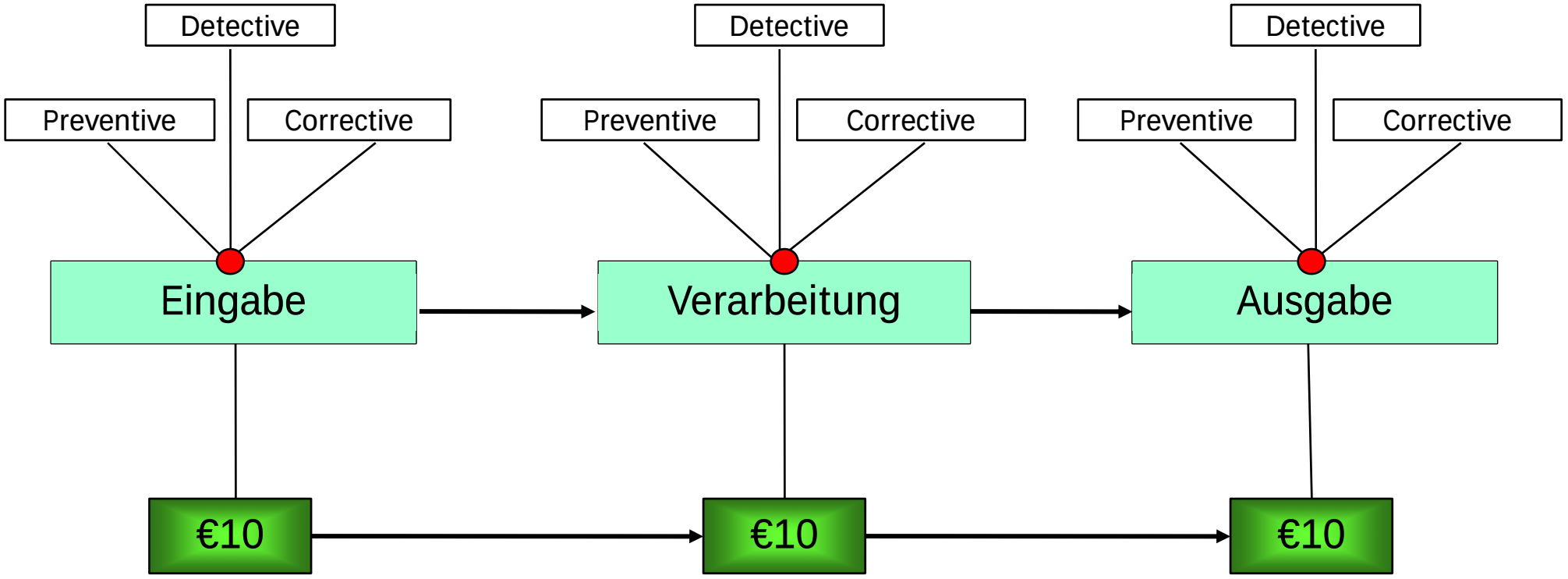


Eigenschaften	Beispiele
▪ High Level Controls ▪ Erstrecken sich über das gesamte Unternehmen ▪ Nicht an eine Applikation gebunden	▪ IT-Strategie ▪ Organisation und Management ▪ Risikomanagement ▪ Zugriff auf Daten und Programme ▪ Systementwicklung ▪ Changemanagement ▪ Notfallplanung ▪ Benutzerverhalten ▪ Physischer Zugriffschutz ▪ Schulung/Ausbildung

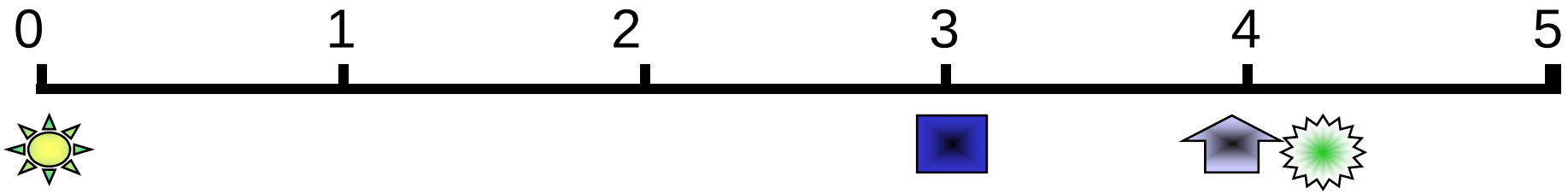
Application Controls

Eigenschaften	Beispiele
▪ Stellen sicher das nur vollständige, genaue und gültige Daten verarbeitet werden ▪ Ergebnisse entsprechen den Erwartungen ▪ Daten werden angemessen gewartet ▪ Doppelte Transaktionen werden erkannt	▪ Passwörter ▪ Prüfsummen ▪ Einfache Eingabemasken ▪ Signaturen ▪ Fehlerkorrektur Prozeduren ▪ Transaktionsprotokoll ▪ Versionsverwaltung ▪ Fortlaufende Nummerierung

Application Controls



Reifegrad Modell



Reifegrad

0 – Nicht existent
1 – Ad hoc
2 – Wiederholbar aber intuitiv
3 – Definierter Prozess
4 – Kontrolliert und messbar
5 – Optimiert

Symbole

Aktueller Status

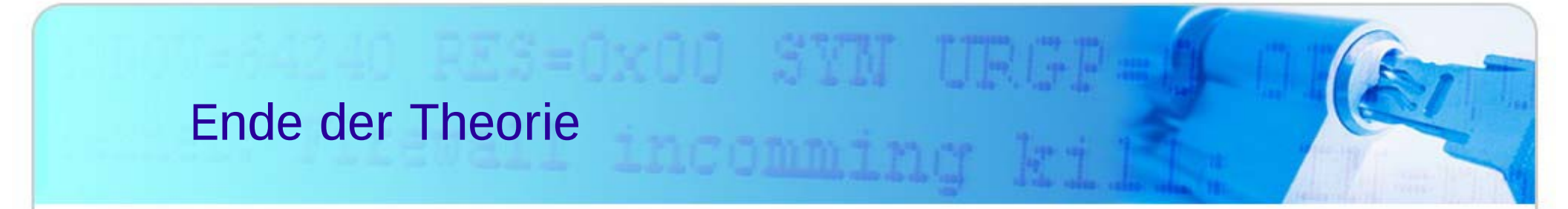
Internationaler Standard

Best Practice

Strategisches Ziel

Quelle: COBIT 3rd

Ende der Theorie



Viel Erfolg!

Tel.: +43 2262 728 57
Manfred.Scholz@sec4you.com