fachhochschule stralsund
university of applied sciences

ISO/IEC 38500 – die neue IT-Governance-Norm

Prof. Dr. Michael Klotz

IT-Governance Forum 2009 22. - 23. Juni, Sheraton München Arabellapark

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

Gliederung

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

1. Hintergrund und Entwicklung
2. Zielgruppe
3. Zielsetzung
4. Aufbau der Norm
   - 4.1 Definition „Corporate Governance of IT“
   - 4.2 Prinzipien der Corporate Governance of IT
   - 4.3 Modell der Corporate Governance of IT
   - 4.4 Empfehlungs-Matrix aus Prinzipien und Führungsfunktionen
5. Bewertung

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

1. Hintergrund und Entwicklung

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- erste Ausgabe am 1. Juni 2008 (→ Review 2011)
- verantwortlich im technischen Komitee „ISO/IEC JTC1“ ist der Unterausschuss „SC7 Software and Systems Engineering“ unter der Leitung von Prof. Dr. François Coallier (Québec, Kanada)
- „Entwicklung“ durch Übernahme der australischen Norm „AS8015:2005“ im „fast-track“-Verfahren
- ISO/IEC 38500:2008 Corporate governance of information technology
- basiert auf Corporate-Governance-Verständnis des Cadbury Reports und Corporate-Governance-Grundsätzen der OECD

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

2. Zielgruppe

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- oberste Stakeholder eines Unternehmens

  explizit:

  - Unternehmensinhaber
  - Mitglieder der Aufsichtsorgane
  - Mitglieder der Unternehmensleitung
  - Mitglieder des oberen Managements
- alle, die diesem Personenkreis assistieren oder ihm prüfend/ beratend zur Seite stehen (intern/extern)
  z. B. IT-Auditoren, Rechtsberater, Controller, Gremien
- Anbieter von IKT-Produkten und Service Provider

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

3. Zielsetzung

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- Stärkung des Vertrauens der Stakeholder (Zielgruppe + Kunden, Mitarbeiter und Anteilseigner) in die IT
- Information und Orientierung für die Unternehmensleitung bezüglich der Wahrnehmung ihrer Verantwortung für eine effektive, effiziente und den Erwartungen der Stakeholder entsprechende Nutzung der IT
- Maßstab für die Bewertung der IT-Governance eines Unternehmens

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4. Aufbau der Norm

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- Fokus:
  planvoller Einsatz der IT, ausgerichtet an den Unternehmenszielen und daraus abgeleiteter IT-Strategie
- keine Einschränkungen hinsichtlich der Unternehmensgröße, -form, -branche
- Drei Aufgaben der Unternehmensleitung:
  (1) systematische Bewertung des aktuellen und künftigen IT-Einsatzes
  (2) Steuerung der Erstellung und Umsetzung von IT-Plänen und -Richtlinien
  (3) kontinuierliche Überwachung von Planrealisierung und Richtlinienerfüllung

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4. Aufbau der Norm

fachhochschule stralsund
university of applied sciences

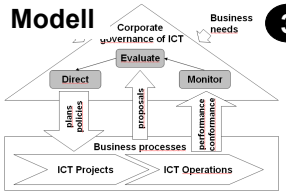
SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

1 **Definitionen**

2 **Prinzipien**

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Modell 3



4 **Empfehlungen**

Prinzip (P)	Führungsfunktionen (F) Bewertung	Leitung	Überwachung
Verantwortlichkeit	<1>	<2>	<3>
Strategie	<4>	<5>	<6>
Beschaffung	<7>	<8>	<9>
Performanz	<10>	<11>	<12>
Konformität	<13>	<14>	<15>
Verhalten	<16>	<17>	<18>

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4.1 Definition „Corporate Governance of IT“

fachhochschule stralsund
university of applied sciences

Cadbury-Report, 01.12.1992

Corporate Governance

2.5 Corporate governance is the system by which companies are directed and controlled. Boards of directors are responsible for the governance of their companies. The

ISO/IEC 38500, 01.06.2008

1.6.3 Corporate governance of IT

The system by which the current and future use of IT is directed and controlled.

4.2 Prinzipen der „Corporate Governance of IT“

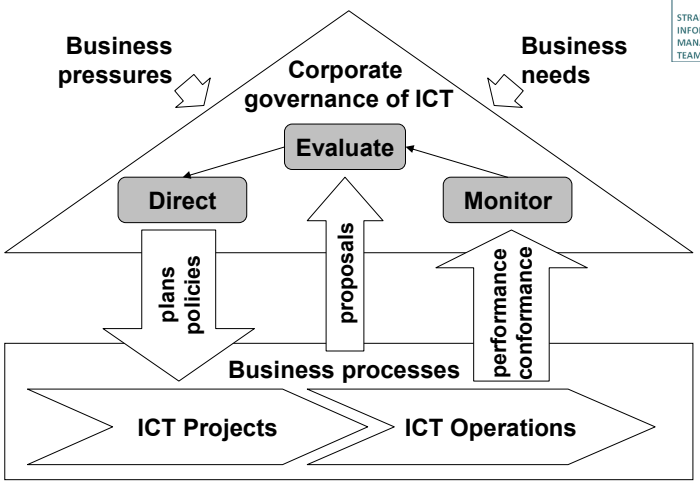
fachhochschule stralsund
university of applied sciences

Nr.	Prinzip	Zielzustand
1	Verantwortlichkeit (responsibility)	• Kenntnis und Akzeptanz der Verantwortlichkeiten für IT-Nachfrage und -Angebot
2	Strategie (strategy)	• Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung der IT-Strategie an der Unternehmensstrategie
3	Beschaffung (acquisition)	• Bedarfsgerechtigkeit von IT-Investitionen • Transparenz und Fundierung des Entscheidungsprozesses
4	Performanz (performance)	• Verfügbarkeit der IT-Services entsprechend den Leistungs- und Qualitätsanforderungen der Geschäftsbereiche
5	Konformität (conformance)	• Konformität der IT mit rechtlichen Vorgaben, Normen, professionellen Standards etc.
6	Verhalten (human behaviour)	• Beachtung der Bedürfnisse von Personen, die in irgendeiner Weise von der im Unternehmen eingesetzten IT betroffen sind (als Nutzer, IT-Spezialisten, Kunden, Lieferanten etc.)

4.3 Modell der „Corporate Governance of IT“

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM



praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4.4 Empfehlungs-Matrix aus Prinzipien und Führungsfunktionen

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

	Führungsfunktionen (F)		
Prinzip (P)	Bewertung	Leitung	Überwachung
Verantwortlichkeit	<1>	<2>	<3>
Strategie	<4>	<5>	<6>
Beschaffung	<7>	<8>	<9>
Performanz	<10>	<11>	<12>
Konformität	<13>	<14>	<15>
Verhalten	<16>	<17>	<18>

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4.4 Empfehlungs-Matrix aus Prinzipien und Führungsfunktionen

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Nr.	Prinzip	Ziele
2	Strategie (strategy)	• Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung der IT-Strategie an der Unternehmensstrategie

Führungsfunktion **Bewertung**

- Die Unternehmensleitung sollte die Entwicklungen sowohl auf der IT- als auch der Geschäftsprozessseite bewerten um sicherzustellen, dass die IT auch die künftigen Geschäftsanforderungen unterstützt.

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4.4 Empfehlungs-Matrix aus Prinzipien und Führungsfunktionen

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Nr.	Prinzip	Ziele
2	Strategie (strategy)	• Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung der IT-Strategie an der Unternehmensstrategie

Führungsfunktion **Leitung**

- Die Unternehmensleitung sollte innovative IT-Projektvorschläge anregen und fördern, so dass das Unternehmen technische Potenziale nutzen, neue Herausforderungen meistern, neue Geschäftsmöglichkeiten wahrnehmen oder Unternehmens-prozesse verbessern kann.

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

4.4 Empfehlungs-Matrix aus Prinzipien und Führungsfunktionen

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

Nr.	Prinzip	Ziele
2	Strategie (strategy)	• Berücksichtigung der aktuellen und künftigen Potenziale der IT im Rahmen der strategischen Planung • Ausrichtung der IT-Strategie an der Unternehmensstrategie

Führungsfunktion **Überwachung**

- Die Unternehmensleitung sollte den Fortschritt bewilligter IT-Projekte überwachen um sicherzustellen, dass die Projekt-zielsetzungen im geplanten Zeitrahmen und mit den geplanten Ressourcen erreicht werden.

praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

5. Bewertung

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- 46 normative Aussagen zum Führungshandeln der IT-Governance thematisieren wesentliche Rahmenbedingungen und Komponenten von IT-Governance
- Schwerpunkte in den Bereichen „Wertbeitrag der IT“ und „Business/IT-Alignment“ (Prinzipien der Beschaffung und Performanz) sowie IT-Compliance (Prinzip Konformanz)
- IT-Risikomanagement kein explizites Prinzip, risikobezogene Aktivitäten jedoch in mehreren Feldern der Matrix enthalten
- Prozessorientierung der IT dagegen kaum angesprochen
- neuer Fokus: Personenkreis, der von der IT in unterschiedlichen Rollen betroffen ist (Prinzip Verhalten)

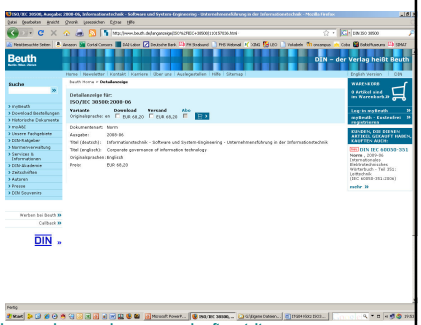
praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

5. Bewertung

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

- Norm ist für ein Unternehmen hilfreich bei der Klärung von Begriff und Bedeutung von IT-Governance
- Empfehlungen beziehen sich auf das „Was?“, aber nicht auf das „Wie?“
- Norm (46 Empfehlungen) kann als **Ausgangspunkt** einer Bewertung der eigenen IT-Governance dienen („Was tun wir bereits, was nicht?“)
- keine Handlungsdruck i. S. eines zu erwerbenden Zertifikats



praxis verstehen — chancen erkennen — zukunft gestalten
understand reality — face challenges — create future

Kontakt

Prof. Dr. Michael Klotz

FH Stralsund, FB Wirtschaft/SIMAT
Zur Schwedenschanze 15, 18435 Stralsund
Fon +49 (0)3831 45-6946
Fax +49 (0)3831 45-6604
eMail michael.klotz@fh-stralsund.de

fachhochschule stralsund
university of applied sciences

SIMAT
STRALSUND INFORMATION MANAGEMENT TEAM

CC IT-Governance, -Riskmanagement, and -Compliance

Aktuelle Projekte/Kurse:

- IT-Process and Control Framework
- Complianceorientierte Prozessorganisation
- Compliance Online-Kurs (ab Oktober 2009)

ISACA
erkennen — zukunft gestalten
ace challenges — create future