Wert und Kosten der IT-Security

Der Weg zur wertorientierten IT-Security Governance

26. Decus Symposium, Königswinter, 10. April 2003

Dr. Stephan Teiwes

Special Assurance and Advisory Services, Zürich

ERNST & YOUNG
Quality In Everything We Do

Agenda

1. Aktuelle Situation
2. Wertorientiertes IT-/IT-Security Management
3. Evolution von Budgeting- nach Beyond-Budgeting-Modell
4. IT-/IT-Security Governance
5. Integrierte, wertorientierte Führungsmethodik
6. IT-Risk-Management
7. IT-/IT-Security Balanced Scorecard
8. COBIT als Kontrollmodell
9. Leistungsvereinbarung
10. Wertorientiertes IT-Security Assessment
11. Tools zur wertorientierten Steuerung der IT-Security
12. Zusammenfassung

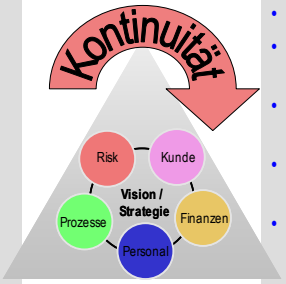
ERNST & YOUNG
Quality In Everything We Do

Aktuelle Situation

Kritische Diskrepanz zwischen den Anforderungen an die Geschäftskontinuität und den praktischen Sicherheitsvorkehrungen

Anforderungen

- Erhaltung der auf Geschäftskontinuität
- Identifikation der IT-Assets im Unternehmen
- IT ist einer der wesentlichen Geschäfts-treiber und Unterstützungsprozesse
- Erhaltung der IT-Geschäftskontinuität
- Verständnis über die Zusammenhänge zwischen Geschäftsstrategie, Risiko-Management und (IT-)Sicherheits-Management
- Verständnis der Zusammenhänge von Wert- und Kostentreibern, Wert- und Kostenerfassung, Werterhaltung



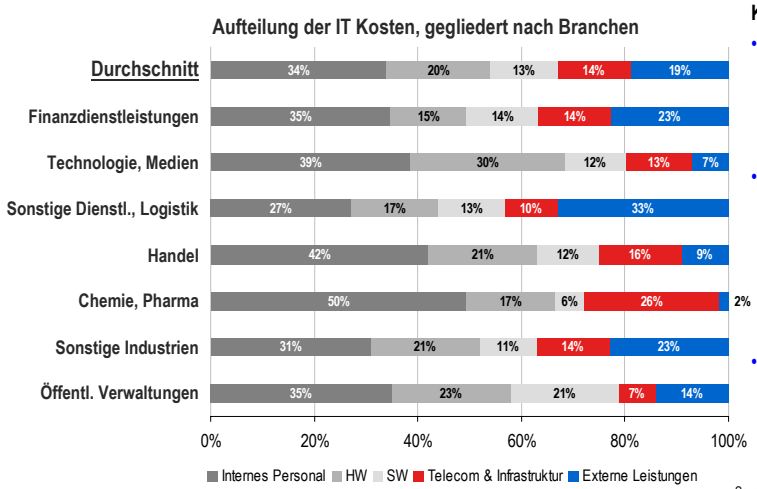
Geschäftsstrategie

Defizite

- (IT-) Risiko-Management ist noch nicht oder nur stellenweise umgesetzt
- Schutzobjekte sind nicht identifiziert
- Es besteht keine unternehmensweite Geschäftskontinuitätsplanung.
- Krisenmanagement ist unzureichend (Mängel: Personal, Know-how, Training)
- Kein unternehmensweite einheitliche Risikokultur; unzureichende Koordination
- IT und IT-Security sind nicht messbar, nicht nachvollziehbar, kein Kontrollsystem – keine IT- und IT-Security-Governance
- Kosten sind oft nicht transparent, nicht zuordenbar
- IT-Sicherheit ist heterogen

Aktuelle Situation

Studie bei Schweizer Unternehmen zeigt starke Unterschiede bei Kostenstruktur und Controlling in der IT



Kernaussagen:

- In den Unternehmen sind die Praktiken in der Organisation der IT und bei der Erhebung der IT Kosten sehr unterschiedlich
- De Facto existiert heute kein einheitl. Standard im IT Controlling und in der Beur-teilung von Kosten bzw. Leistung. Das erschwert den Vergleich, die Transparenz und die Steuerung
- Oft verfügt das IT-Controlling nicht über den in der Befragung geforderten Detaillierungsgrad der Zahlen

Source: IT-Kosten und IT-Performance 2002, EY Schweiz

Aktuelle Situation

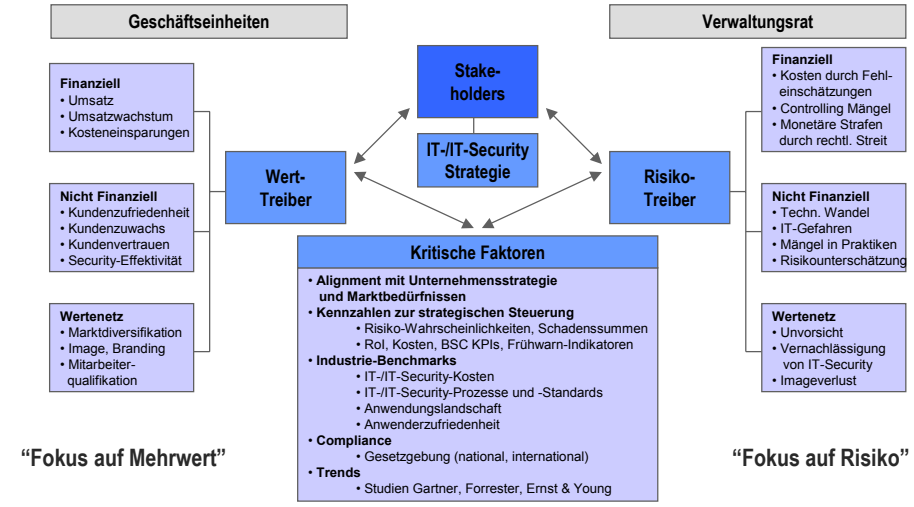
Handlungsbedarf angesichts der Defizite im Risiko-, Business-Continuity- und Krisenmanagement

- Die meisten Unternehmen sind auf Krisensituationen schlecht oder gar nicht vorbereitet
- Die Bereitschaft zur Investition in die Verbesserung der Sicherheit ist prinzipiell vorhanden. Doch der Einsatz von Geldern soll nachweislich eine Wertschöpfung für das Unternehmen sein
- Das Verständnis der Wertschöpfung durch IT-Risiko-Management und IT-Security muss verbessert werden
- Handeln ist notwendig
  - – Hastiges Vorgehen durch Angst vor wachsenden Bedrohungen (Terror) birgt wiederum die Gefahr, falsche Massnahmen aus einem Unverständnis heraus zu beschliessen. So können hohe Investitionen leicht ihr Ziel verfehlen und der Krisenfall darum zur Katastrophe werden.
  - \+ Gezieltes Handeln und koordiniertes Vorgehen sind erforderlich: erster Schritt ist eine Diagnose, um die eigene Situation zu verstehen, zu beurteilen und darauf aufbauend Massnahmen zu planen, einzuleiten und deren Umsetzung zu kontrollieren.
- Wertorientierte Planung und Umsetzung schaffen Kosten- und Nutzentransparenz und Wertschätzung
- Kontroll- und Steuermechanismen erhalten Sicherheit und deren Wert

  Sicherheit, die durch Investitionen geschaffen worden ist, soll dem Unternehmen auch erhalten bleiben.

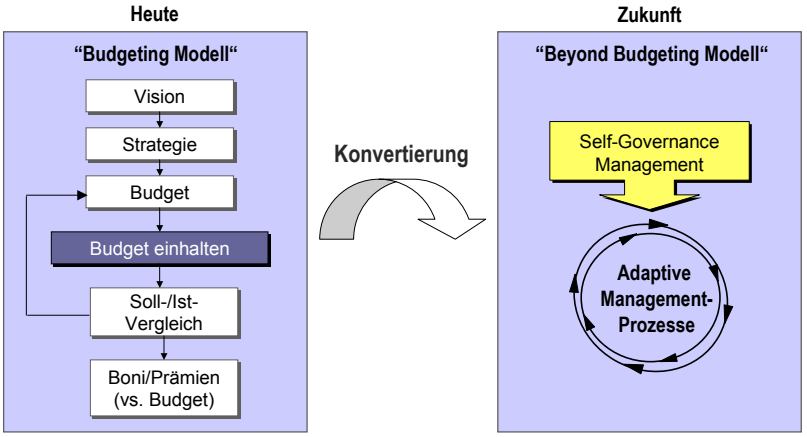
Wertorientiertes IT-/IT-Security Management

Werttreiber und Risikotreiber werden miteinander in Beziehung gestellt



Blick auf die Evolution: vom Budgeting-Modell zum Beyond-Budgeting-Modell

Der Wechsel des Modells trägt dem dynamischen Verhalten von Markt und Kunden Rechnung.



Ziel: effiziente Nutzung von Finanzkapital und anderen Ressourcen

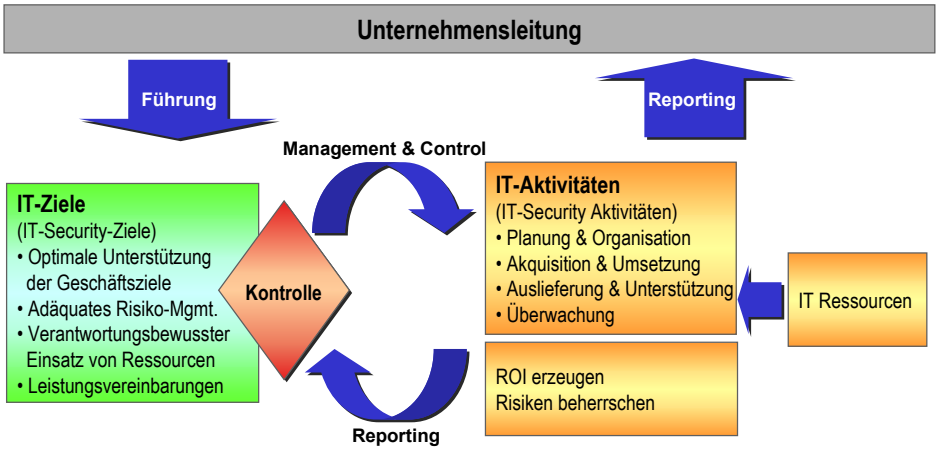
Ziel: hohe Anpassungs- und Innovationsfähigkeit

Budgeting vs. Beyond-Budgeting: was ändert sich?

Kriterium	Budgeting Modell	Beyond Budgeting Modell
1. Ziele	1. Fixes Jahresziel	1. Wettbewerbsorientierte Ziele
2. Bonus-system	2. Zumeist auf der Basis individueller Ziele	2. Auf Basis von Team-bezogenen Zielen
3. Planung	3. Unternehmensbezogen	3. Kundenbezogen "Customer first"
4. Ressourcen	4. Zentral gesteuerter Einsatz verhindert Reaktionsfähigkeit	4. Bedarfsorientierte Entscheidung und Ressourcenplanung
5. Koordination	5. Unternehmensorientiert und somit statisch	5. Marktorientiert und somit dynamisch
6. Strategisches Controlling	6. Vergleich der Ist-Zahlen mit Budget; Fehlen von strategisch relevanten Informationen	6. Strategisch relevante, entscheidungsorientierte und vielseitige Informationen

IT- / IT-Security Governance

Prinzip der Steuerung von IT und integrierter IT-Security in einem formalen Prozess nach CobiT

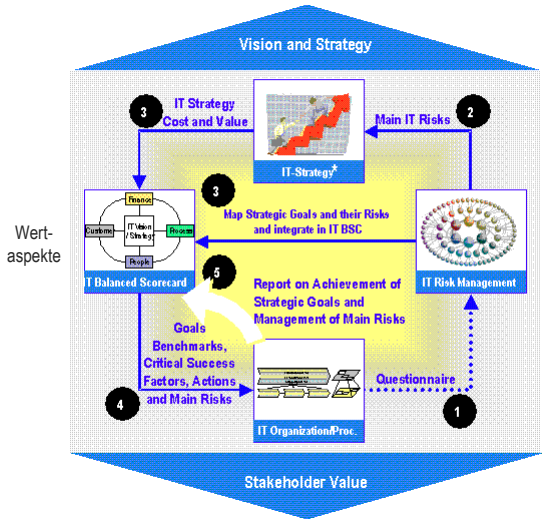


Einsatz einer integrierten, wertorientierten Führungsmethodik

Risikoorientierter Prozess zur Wertsteuerung

Vorteile

- Risikoorientiertes Führungs- und Controlling-Instrument, basierend auf den strategischen Zielen
- Transparenz schafft Vertrauen beim Stakeholder (Stakeholder-Orientierung)
- Integration von Risiko-Management in die Balanced Scorecard (BSC) Ansatz
- Reduktion von Redundanzen bei Führung und Reporting
- Strategiekonforme IT- und IT-Security Projekte und Budgetierung



Wert-aspekte

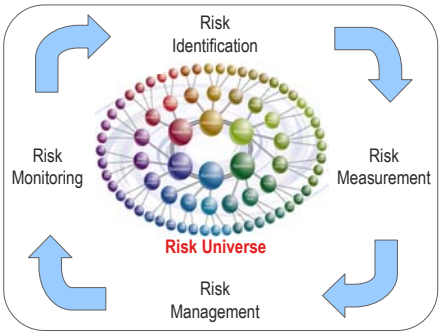
Risiko-aspekte

IT-Risk-Management

Mittels IT-Risk-Management werden die Risikotreiber festgestellt und überwacht

Kritische Aspekte

- Einheitliche Sprache und Verständnis bei Risikoverständnis und -beurteilung
- Einbezug aller Bereiche bei einheitlichem (ggf. globalen) Ansatz
- Festlegung von Verantwortlichkeiten
- Schaffung einer Risikokultur durch Integration eines risikobewussten Denkens im Tagesgeschäft
- Klare Vorgaben, wie Risiken identifiziert, gemessen, gehandhabt und reduziert werden sollen
- Automation der Risk-Prozesse
- Trennung der Kontrollfunktion von der Managementfunktion

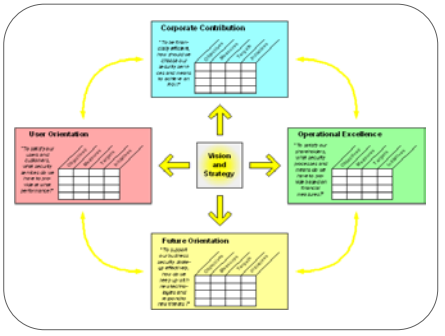


IT- / IT-Security Balanced Scorecard

Mittels Balanced Scorecard können auch die Wert- und Kosten-Treiber der IT-Security festgestellt und überwacht werden.

Vorteile

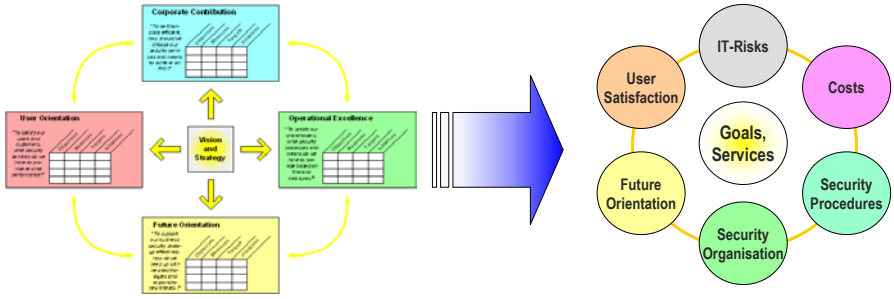
- Monitoring der Leistung operativer Prozesse und der langfristig für den Erfolg relevanten Faktoren durch eine balancierte Menge von Messkriterien
- Es gibt finanzielle und nicht-finanzielle Messkategorien und -kriterien
- Die Messkriterien müssen mit der IT-(Security-) Strategie verbunden sein
- Die IT- (Security-) Strategie muss in eine Menge „greifbarer" Objekte und Messwerte verschiedener Messkategorien abgebildet werden
- Die Kategorien der IT-Security Balanced Scorecard können nach Bedarf spezifiziert werden



Klassische IT-Balanced Scorecard

Erweiterte IT-Security Balanced Scorecard

Modifikation der klassischen Balanced Scorecard um zusätzliche Dimensionen

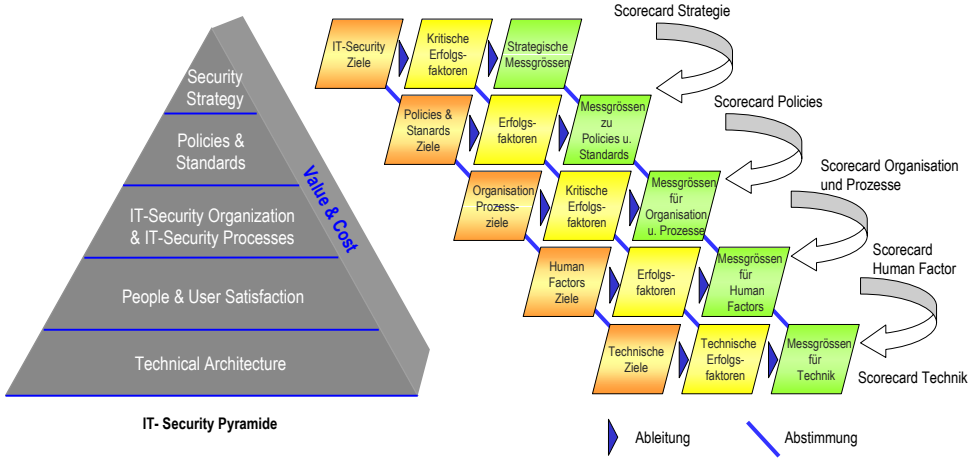


Klassische IT-Balanced Scorecard

Modifizierte IT-Balanced Scorecard

Anwendung der Balanced Scorecard in der IT-Security

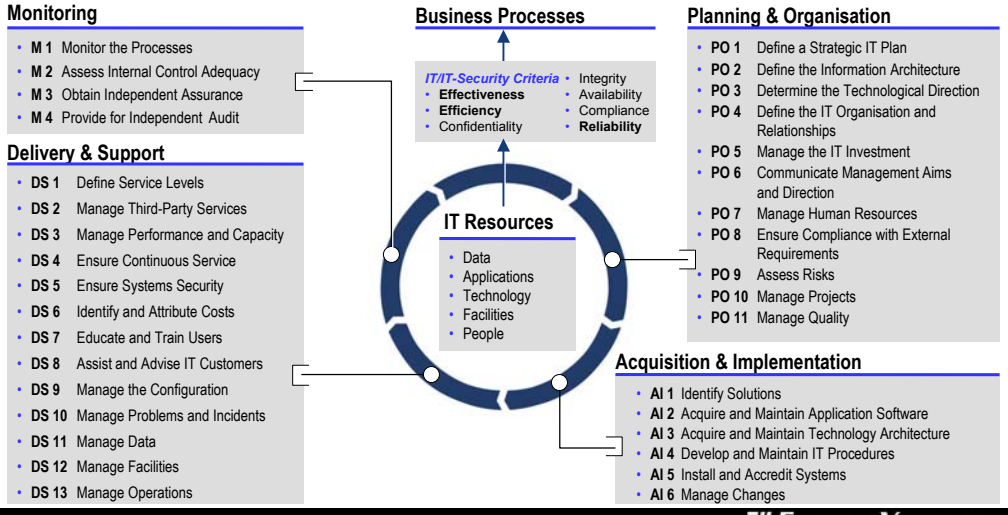
In dem hierarchischen Modell müssen die horizontale Ableitungen und vertikale Abstimmungen berücksichtigt Kategorien .



IT- Security Pyramide

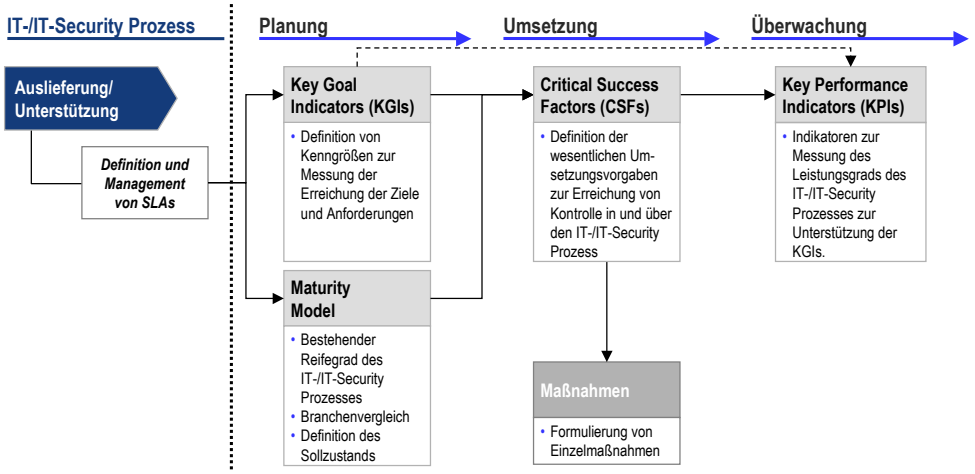
CobiT als Kontrollmodell der Prozesse in IT / IT-Security

CobiT ist ein internationaler Standard und beschreibt IT-Prozesse nach 4 Bereichen (Megaprozesse) sortiert.



CobiT als Kontrollmodell der Prozesse in IT / IT-Security

Für jeden IT-Prozess gibt es Managementrichtlinien in Form von Maturity Models, Critical Success Factors, Key Goal Factors und Key Performance Indicators, um eine bestmögliche Planung, Umsetzung und Überwachung zu unterstützen.



Leistungsvereinbarung (Service Level Agreements) und Standardisierung

Vorteile einer Einführung

- Unterstützung von guter und detaillierter Umsetzung des Service Managements
- Definition von Funktionen, Rollen und Verantwortlichkeiten im Service-Bereich
- IT und IT-Security-Dienstleistungen, die den Anforderungen durch Geschäftsziele oder Kunden entsprechen; dadurch höhere Kundenakzeptanz
- Messbare Leistungen und Kosten der IT- und IT-Security-Services; dadurch besseres Wertverständnis und bessere Möglichkeiten der Verrechenbarkeit von Leistungen nach dem Verbraucherprinzip
- Höhere Produktivität und Effizienz durch den gezielte Einsatz von Wissen und Erfahrung
- Basis für eine Quality-Management-Systematik im IT Servicemanagement
- Möglichkeit des (internationalen) Erfahrungsaustausches und Vergleichs bei Einsatz standardisierter Methoden

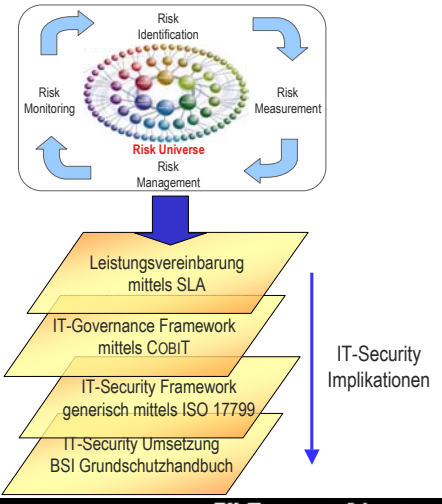
Leistungsvereinbarung und IT-Security

IT-Security ist ein wesentlicher Bestandteil der Leistungsvereinbarungen

Elemente eines SLA

1. Performanz
2. Kosten
3. **IT-Security**
4. **Verfügbarkeit**
5. **Business Continuity**
6. **Disaster Recovery**
7. Regelung von Schadensansprüchen bei Nichteinhaltung

Security

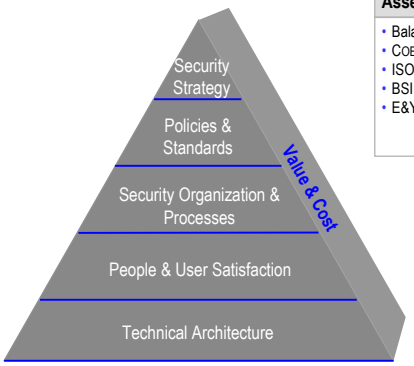


Prinzip eines wertorientierten IT-Security Assessments

Die Prüfbereiche sind entlang der IT-Security Pyramide gegliedert

Grobe Beurteilungskategorien

- Security Strategy: Eignung der IT-Risk- und IT-Security Massnahmen bzgl. der Geschäftsziele und -initiativen
- Policies & Standards: Eignung der Policies und Standards bzgl. der Geschäftsanforderungen
- Security Organisation & Processes: Reifegrad der Organisation und Prozesse sowie Anpassungsfähigkeit an neue Anforderungen und Technologien
- People & User Satisfaction: Grad der Berücksichtigung des „Human Factor“
- Technical Architecture: Reife und Adäquatheit technischer Massnahmen
- Value & Cost: Wertbeitrag und Kostenperspektive



Information Security Pyramid

Ernst & Young Assessment

- Balanced Scorecard
- COBIT
- ISO17799
- BSI Grundschutz
- E&Y Methodik

Wertorientiertes IT-Security Assessment von Ernst & Young

Prüfbereiche können modular nach individuellen Anforderungen ausgewählt und priorisiert werden.

Assessment Areas

Group Level

- ❑ *Corporate Information & IT Security Strategy*
- ❑ *Corporate Information & IT Security Policies*
- ❑ ...

Business Level

- ❑ *IT Security Risk Control*
- ❑ *IT Security Policies and Standards*
- ❑ *Access Control and Data Ownership*
- ❑ *Compliance*
- ❑ *IT-Security Lifecycle*
- ❑ *IT-Security in IT Projects and IT Systems Development*
- ❑ *IT Security Threats & Vulnerabilities*
- ❑ *Business Continuity and Disaster Recovery*
- ❑ *IT-Security Awareness*
- ❑ ...

Office Level

- ❑ *IT-Security Architecture*
- ❑ *Network Security*
- ❑ *Systems Security*
- ❑ ...

Issues

- ❑ *Goals*
- ❑ *IT-Risks*
- ❑ *Security Procedures*
- ❑ *Security Organization*
- ❑ *Future Orientation*
- ❑ *User Satisfaction*
- ❑ *Costs*

BSC Ansatz

Organization: Is the IT risk control initiative organized?

3.1	Is there a committee with the final responsibility for the IT risk control initiative?
3.2	Is there is a management group with final authority and responsibility for specifying and approving information security risk control standards?
3.3	Are roles and responsibilities defined?
3.4	Are there enough ressources for the initiative? (How many people are engaged in the initiative?)
3.5	Is the staff qualified for performing the IT risk control initiative (procedures and services)?
3.6	Are the interfaces to all other relevant instances (IT risk management, IT security, Business Continuity Services, IT audit, Chief Risk Officer, etc.) well defined?
3.7	Are the IT risk control standards universally deployed, controlled, and administered across the entire organization?
3.8	Are special tools for risk control automation used?
3.9	Is a centralized evaluation and of IT risk management situation enabled by this tool?
3.10	Are IT risk control services specified?
3.11	Is there an independent instance with the responsibility of controlling the IT risk control initiative (e.g. risk management or IT audit)?
3.12	Is there an entity with final responsibility for risk control reporting?
3.13	Are there regular meetings for sharing information and for decision making within the group?

Ausschnitt eines vordefinierten Questionnaires

Modell zur Ermittlung von Value und Costs

Der Wert eines Prüfbereichs ist im wesentlichen die Summe gewichteter KPIs. Die Kosten eines Prüfbereichs werden aus der Summe der Detailkosten ermittelt.

Value and Cost Evaluation Model

Assessment Areas	Area Weight	Issue	Issue Value	Issue Weight
Area 1	f_1	Issue 1,1	$V_{1,1}$	$W_{1,1}$
		...	...	
		Issue 1,k	$V_{1,k}$	$W_{1,k}$
Area 2	f_2	Issue 2,1	$V_{2,1}$	$W_{2,1}$
		...	...	
		Issue 2,m	$V_{2,k}$	$W_{2,k}$
...	...	...	...	...
Area h	f_h	Issue h,1	$V_{h,1}$	$W_{h,1}$
		...	...	
		Issue h,m	$V_{h,m}$	$W_{h,m}$

Area Values	Area Costs
V_1	C_1
V_2	C_2
...	...
V_h	C_h
Σ	Σ
Total Value	Total Costs

Area Value V_h: Sum of Weighted Issue Values

ERNST & YOUNG
Quality In Everything We Do

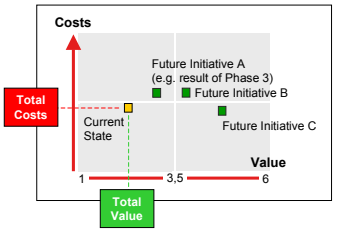
Visualisierung und Reporting

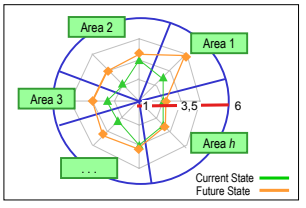
Die Visualisierung der quantitativen Beurteilung der IT-Security unterstützt bei der Management-Entscheidungsfindung.

Nutzen

1. Methode zur quantitativen Beurteilung des Wertes der IT-Security für die Geschäftsprozesse und –ziele
2. Methode zum Self-Assessment für Current State / Future State Benchmarking
3. Im Gegensatz zu herkömmlichen BS7799-orientierten Assessments wird hier im Sinne der BSC auch bzgl. des Geschäftsnutzen geprüft
4. Qualitativ hochwertige Information zur Management-Entscheidungsfindung bei zukünftigen IT-Security-Initiativen
5. Bessere Visualisierung von Wert und Kosten der IT-Security

Information & IT Security Value / Cost Ratio





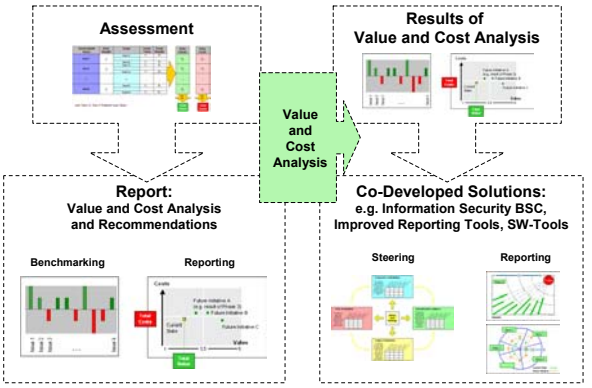
Information & IT Security Value in Selected Areas

ERNST & YOUNG
Quality In Everything We Do

Entwicklung einer integrierten, wertorientierten Führungsmethodik für IT-Security

Wesentliche Schritte

1. Value & Costs Assessment zur Erfassung des Ist-Zustands und Einstellung der wertorientierten Vorgehensweise:
   - Definition der Prüfbereiche
   - Durchführung des Assessments
   - Resultate: Wertbeurteilung, Empfehlungen für Optimierungen
2. Entwicklung von Steuer-Tools zum Erhalt der Wertorientierung
   - Self-Assessment
   - wertorientierte Steuerung gemäss Balanced Scorecard Ansatz
   - Reporting Tools



Zusammenfassung

- Der Kostendruck in den Unternehmen zwingt zur Begründung von Ausgaben
- Es gibt keine einheitliche Vorgehensweise in Unternehmen zur Erfassung von Ausgaben oder Ermittlung von Werten in der IT bzw. IT-Security; entsprechend entsteht ein Erklärungsnotstand gegenüber der Geschäftsführung bzgl. Kosten und Nutzen von Initiativen in der IT- bzw. IT-Security
- Kosten sind Hard-Factors und leicht ermittelt, Werte sind Soft-Factors und schwieriger zu ermitteln
- Eine Assessment-Methodik zur wertorientierten, integrierten IT-Security Governance wurde vorgestellt
- Der Ansatz basiert auf einer Kombination von Risk-Management, IT-Balanced Scorecard und Standards zur Prozessbeurteilung (COBIT, ISO 17799)
- Vorteile der Methodik:
  - eine wertorientierte Beurteilung von Initiativen in der IT-Security zeigt auf, wo Investitionen sinnvoll eingesetzt werden und wo nicht
  - Aktionspläne können auf der Basis der Wertorientierung definiert werden
  - Tools zur Überwachung und zum Erhalt der Wertorientierung können entwickelt werden

Ihr Kontakt

Dr. Stephan Teiwes
ist Berater für IT- und Informationssicherheit bei Ernst & Young, Special Assurance and Advisory Services (SAAS), Zürich. Er hat in seiner langjährigen Tätigkeit diverse Beratungsmandate für Unternehmen in Finanzen, Industrie und Gesundheitswesen wahrgenommen. Zu seinen Spezialgebieten gehören IT-Sicherheits-architek-turen und -infrastrukturen sowie die Sicherheit elektronischer Geschäftsprozesse. Dr. Teiwes ist regelmässig Referent an Kongressen zur IT-Sicherheit im deutschsprachigen Raum und hat zahlreiche Fachartikel publiziert.

Ernst & Young AG
Binzmühlestr. 14
Postfach
8022 Zürich
Schweiz

Tel. +41 79 752 6373
E-Mail: stephan.teiwes@eycom.ch