ISACA®
Trust in, and value from, information systems
Switzerland Chapter

Nr. 01 | März 2012 | www.isaca.ch
NEWSLETTER

IT Governance
Effective governance requires among others an integrated process model and framework of accountability **Seite 49**

CGEIT
CGEIT, die berufsbegleitende Zertifikatsausbildung in IT-Governance von ISACA Switzerland Chapter **Seite 52**

ISACA-Training
Aktuelle Aus- und Weiterbildungsmöglichkeiten für Mitglieder und Nicht-Mitglieder **Seite 52**

Implementing IT Governance

Effective governance requires an integrated process model, framework of accountability, management system, clearly assigned roles, process triggers, actionable tasks and real-time tracking.

Von Peter Hill

There have been many attempts to better manage information and technology (IT) with a range of different models over the past three decades. Management by Objectives (MBO), Total Quality Management (TQM), ISO 9001, Six Sigma, LEAN are some of the approaches used by companies seeking to improve effectiveness and drive efficiencies. Now it's the turn for «IT Governance».

What is IT Governance?

IT Governance is about the stewardship of information and technology resources by a company's board of directors on behalf of all stakeholders. As with any other strategic resource, a company's board must ensure that the stakeholders receive the expected benefit from the investment in and use of information technology. While the board is accountable for the corporate governance of information and technology (IT), the board delegates responsibility to executive management to implement an IT governance framework and deliver value.

What is an IT Governance Framework?

An IT governance framework provides the conceptual structure to establish accountability for the management processes and decisions the affect the success of IT supporting the effective and efficient management of IT resources to facilitate the achievement of an organisation's strategic objectives. It creates clarity about who has what decision-making authority regarding the use of IT and it enables the board to hold those with decision-making authority accountable for using IT to achieve the organisation's strategic objectives. An IT governance framework comprises three levels of decision-making authority and accountability for the efficient and effective management of IT resources.

ZWEI AWARDS FÜR DAS ISACA SWITZERLAND CHAPTER

2011 war ein herausragendes Jahr für das Schweizer Chapter. Wir durften den K. Wayne Snipes Award entgegennehmen als Anerkennung für das beste sehr grosse Chapter in Europa/Afrika. Gleichzeitig erhielten wir in der gleichen Kategorie eine Auszeichnung für die höchste «Erneuerungsrate» (87,3%) der Mitgliedschaft. Wir freuen uns sehr darüber und hoffen auf weitere aktive Mitarbeit im Vorstand und unter den Mitgliedern. Mehr Informationen finden Sie auf www.isaca.ch über uns.

At level 1 (strategic), the Board (or a sub-committee of the board - an IT Steering Committee) governs IT by:

- Evaluating - the current and future use of IT by examining strategies, proposals and supply arrangements for IT (internal, external, or both).
- Directing – the responsibility and priority in preparing and implementing a management system of plans, policies and processes so that the use of IT supports business objectives and the achievement of agreed strategic outcomes (via an IT governance charter).
- Monitoring – receives reports about:
  - the current and future use of IT,
  - progress towards delivering the performance expected from IT measured against agreed plans and business objectives, and
  - the use of IT is in conformance with internal policies and external obligations (regulatory, legislation, common law and contractual).

Also at level 1, the Audit committee (another sub-committee of the board) will govern IT by:

- Evaluating, directing and monitoring the management of risks associated with the use of IT as they relate to financial reporting; and

the Risk committee will govern IT by:

- Evaluating, directing and monitoring the management of risks associated with the use of IT as they relate to achieving strategic, operational and compliance objectives, but excluding those related to financial reporting (unless the Audit committee and Risk committee are combined).

At level 2 (management), one or more oversight authorities govern by overseeing the management lifecycle:

- Plan – design efficient and effective processes, implementation plans and governance mechanisms to achieve the desired outcomes,
- Implement – organise and lead the implementation of the organisational structures, processes and working practices; configure, customise and maintain process artefacts,
- Operate – execute the tasks and respond to issues affecting the desired outcomes; analyse the efficiency and effectiveness of the processes and practices deployed,
- Act – to correct deviations in performance that will impact the desired outcomes.

At level 3 (operational), IT management delivers by:

- Tracking – the activities being executed with the aim of achieving stated goals,
- Supervising – organising and re-organising IT activities so that there is increased reliability in achieving the stated objectives,
- Checking – analysing performance and risk management across IT,
- Controlling – detecting and correcting inefficiencies and poor performance and remediating risks found within IT.

The Accountability Framework

Governance occurs at the strategic, management and operational levels through the assignment of decision-making responsibilities and authority to encourage desirable behaviour in the use and provisioning of IT. While the CIO has overall responsibility to account for the use and provisioning of IT, individual IT managers have responsibility to render reports about their specific areas of responsibility.

The primary purpose of the Accountability Framework is to communicate to IT and business managers who have which responsibilities to render reports about what has been achieved from the work performed. Because there is overlap within and between IT and business processes, there is always the risk that two managers may have the same accountability, no manager is allocated accountability to render reports, or a manager is assigned accountability for areas and actions over which he/she has no responsibility. Typically, a process reference model (e.g. CobiT or ITIL) is used to identify and clarify responsibilities for information and related technologies.

As processes describe a structured set of activities organised to achieve specific purposes, process descriptions provide a useful reference to determine which managers are responsible for which outcomes and which activities within these processes are important to delivering these outcomes. Consequently the Accountability Framework summarises the key roles within the organisation and the respective responsibilities of the managers responsible for these roles.

Role and Job Descriptions for IT Personnel

Role and job descriptions are a cornerstone to governance. They usually provide the detailed descriptions of individual responsibilities, working relationships and performance measures. Mapping role descriptions to a process reference model provides the CIO with assurance that responsibilities for key process-level activities are assigned, gaps are identified and duplications are removed. This ensures that individual performance measures are related to specific process responsibilities and outcomes necessary for the process to achieve its purpose. Senior managers are typically responsible for a number of processes, whilst

ACCOUNTABILITY FRAMEWORK

PROCESS OWNERS (o)		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2	AI3	AI4	AI5	AI6	AI7	DS1
1.1 Head: Governance, Strategy & Performance	4	o					o												
1.2 Head: Planning, Architecture & Investment	8		o	o	o	o		o				o				o			
1.3 Head: Risk, Continuity, Security, Compliance	6								o	o									
1.4 Head: Solution Delivery	7										o		o		o		o	o	
1.5 Head: Service Management	6																		o
1.6 Head: Technical Services	3													o					
ROLES with at least one process area - A or R		**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**AI1**	**AI2**	**AI3**	**AI4**	**AI5**	**AI6**	**AI7**	**DS1**
2.1 Technology Officer				R															
2.2 Manager: Information Security			R	R	R														
2.3 Enterprise Integration Architect				R															
2.4 IT Process Architect					R														
2.5 Application Portfolio Architect																			
2.6 Information Security Officer										R									
3.1 Manager Business and Process Analysis									R			R	R				R		
3.2 Manager Applications Portfolio & Sol. Design													R						
3.3 Manager Project Office											R								
3.4 Manager Development and Integration									R				R		R				
3.5 Manager Maintenance													R		R				
3.6 Manager Testing																		R	
3.7 SOA Capability Manager													R						
3.8 Application Portfolio Manager													R				R		
3.9 Development Framework Manager									R	R			R						
3.10 Enterprise Business Analyst												R							
3.11 Project Manager											R								
4.1 Manager Service Support																	R	R	
4.2 Manager Service Delivery*																R			R
4.3 Manager: End-User Support																			
4.4 Manager: Mainframe and Hosting																			R

PROCESS OWNERS (o)		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	AI1	AI2
1.1 Head: Governance, Strategy & Performance	4	o					o						
1.2 Head: Planning, Architecture & Investment	8		o	o	o	o		o				o	
1.3 Head: Risk, Continuty, Security, Compliance	6								o	o			
1.4 Head: Solution Delivery	7										o		o
1.5 Head: Service Management	6												
1.6 Head: Technical Services	3												
ROLES with at least one process area - A or R		**PO1**	**PO2**	**PO3**	**PO4**	**PO5**	**PO6**	**PO7**	**PO8**	**PO9**	**PO10**	**AI1**	**AI2**
1.1 Head: Governance, Strategy & Performance		R	R	R	R				R		R		
1.2 Head: Planning, Architecture & Investment		R	R	R		R				R	R	R	R
1.3 Head: Risk, Continuity, Security, Compliance		R	R	R	R	R	R			R			
1.4 Head: Solutions Delivery											A	A	R
1.5 Head: Service Management						R							
1.6 Head: Technical Services						R							
2.1 Technology Officer				R									
2.2 Manager: Information Security			R	R	R								
2.3 Enterprise Integration Architect				R									
2.4 IT Process Architect					R								
2.5 Application Portfolio Architect													
2.6 Information Security Officer										R			
3.1 Manager Business and Process Analysis									R			R	R
3.2 Manager Applications Portfolio & Sol. Design													R
3.3 Manager Project Office											R		
3.4 Manager Development and Integration									R				R
3.5 Manager Maintenance													R

managers have specific responsibilities within individual processes. Senior managers are primarily responsible for the process outcomes achieved, whilst managers have responsibility for specific process and sub-process areas. Senior managers are accountable for their processes (i.e. they are required to render reports regarding their successes) whilst managers are responsible for the execution of the process and key activities within the process.

An Accountability Framework assists identify any gaps, duplication and work overload in the assignment of responsibilities. Issues are resolved by adjusting the individual role descriptions and assignment of individuals to roles. New role descriptions are determined from an analysis of each process and the level of responsibility (i.e. «senior manager» = process owner, «manager» = process manager and «supervisor» = team leader) is clarified.

Performance measures are derived directly from either the process outcomes or the responsibilities assigned to the specific role (i.e. owner, manager, team leader). Consequently managing individual performance drives the achievement of process, IT, business and strategic objectives.

The Management System

The objective of a management system is to continually improve the operational processes whilst operating and executing the daily activities of each process. ISO 9001 and ISO 27001 are examples of management systems for quality and information security. Each comprises the lifecycle approach of Deming (i.e. Plan, Do, Check and Act).

On a regular basis issues arise in each process that need management attention. Some relate to the work being performed, some to the configuration of the process being used, and others from problems that arise. A management plan is used to record the acceptance/rejection of the issues that arise and maintain an order of priority. This management plan feeds an implementation plan which is monitored in the medium-term and has scheduled review points. The implementation plan for each issue addresses the resources, tasks and responsibilities for introducing, developing and executing the work required to resolve the issue. When designing and executing the implementation plan, managers:

- determine the sequence of implementation,
- document roles and responsibilities,
- determine the target dates for implementation and
- decide on the frequency and format of reporting against milestones.

The challenge for managers is to coordinate work that needs to be planned and executed across a number of processes and functional units. Within the manager's own area of authority a manager is able to redesign processes and practices and re-assign work priorities. However, with an established accountability framework, each manager is empowered with specific responsibilities and entrusted with defined decision-making authority. To succeed, managers need to collaborate and coordinate their actions.

Actionable Tasks for better Governance

Frameworks like CobiT and ITIL provide important guidance about the required tasks that make up generally accepted best practice for IT processes and the actual process of implementing or modifying the recommended practices. Companies often struggle to define and implement the processes, triggers, controls and governance mechanisms recommended and frequently there is considerable upfront investment in simply understanding the requirements of the selected frameworks with little real value actually being created or governance established.

What companies require is a management system and streamlined processes with clearly defined accountability for actionable tasks that if followed, manage the risks, deliver the results expected and support regulatory compliance obligations.

A management system should facilitate cross-divisional co-operation and teamwork, promote compliance and continuous improvement. A management system will include:

- Assess, plan and execute the processes and their continuous improvement
- Tracking that processes are capable of delivering against enterprise, governance, management and control objectives
- Make use of the available implementation guidance:
  - sources of good practice
  - emerging standards
  - compliance requirements
  - automation opportunities
  - productivity improvements.

Implementing the levels of a governance framework will establish effective governance of information and technology resources. The board is able to direct, managers continuously improve and staff deliver the performance expected.

DER AUTOR

Peter Hill (CISA, CISM, CGEIT) is an IT Governance specialist with over fifteen years related experience. He is currently a director of the IT Governance Network, a company specialising in IT Governance, CobiT, ISO 38500, ISO 27001, management systems and training. The IT Governance Network also provides integrated CobiT and ITIL process, risk management and compliance solutions and management systems on the mobile platform.

Information des Verbandes

IT-Governance – weckt die Prinzessin aus dem Schlaf!

Fast täglich wird in der Presse über Misserfolge im Informatikumfeld berichtet. Die gescheiterten Millionenprojekte, welche es bis in die Öffentlichkeit schaffen, sind jedoch nur die Spitze des Eisberges: ausufernde Kosten, instabile Anwendungen, abgestürzte Systeme bis zu verlorenen Daten stellen leider in vielen Unternehmungen die traurige Realität dar.

Auch heute noch schiebt man die Schuld in aller Regel der Informatik – insbesondere dem Informatik-Management – zu. Vergessen geht dabei, dass auch die Fachbereiche sowie die Geschäftsleitung eine «Mitschuld» an solchen unerwünschten Ereignissen tragen. Es reicht nicht, wenn sich ein Unternehmen nur um das klassische Management der Informatik kümmert: Governance muss – wie im obigen Artikel aufgezeigt – auf einer höheren Ebene erfolgen und sich um die zentralen Themen wie z.B. Definition von Leitplanken, Ausrichtung der IT-Strategie auf die Geschäftsstrategie, Integration von IT-Risikomanagement in das unternehmensweite Risikomanagement wie auch die Überwachung der IT kümmern.

Dies sind einige der zentralen Themen, welche im CGEIT-Berufsbild von ISACA abgedeckt sind und am zwei Mal jährlich stattfindenden ISACA-Examen auch geprüft werden. Das ISACA Switzerland Chapter betreibt bereits seit mehreren Jahren die berufsbegleitenden Zertifikatsausbildungen in IT-Governance – in den aktuell laufenden Kursen sind rund 20 Personen dabei, was auf das bestehende Interesse an solchen Ausbildungen aufzeigt.

CGEIT Certified in the Governance of Enterprise IT® An ISACA® Certification

WEITERE INFORMATIONEN

Interessieren Sie sich für die fünf Fokus-Bereiche von IT-Governance: Strategic Alignment, Risk Management, Resource Management, Value Management und Performance Measurement? Informieren Sie sich auf unserer Website www.isaca.ch
ISACA Switzerland Chapter Aus- und Weiterbildung

ISACA-TRAINING

Datum	Code	Hauptthema – Kurstitel
12.3.12	RIM-KK	**Risikoprüfungen und kontinuierliche Risikoüberwachungen:** Wirksame Überwachung von Risiken
13.3.12	IKS-KK	**IKS: Design, Betrieb, Überwachung und Unterhalt:** Effizientes Design & wirksame Überprüfung von anwendungsabhängigen Kontrollen
15.-16.3.12	LAB-IPS	**iPhone & iPad Security**
19.3.12	ACC-IPG	**Wirksamer Zugriffsschutz (Access Control):** Zugriffsschutz richtig konzipieren und prüfen
19.-21.3.12	COB-FB	**ISACA COBIT 4.1 Foundation Zertifikat**
2.4.12-8.5.12	CISA-PV	**CISA-Prüfungsvorbereitungskurs 2012|1:** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer
10.4.12-9.5.12	CISM-PV	**CISM-Prüfungsvorbereitungskurs 2012|1:** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer
12.4.12-11.5.12	CRISC-PV	**CRISC-Prüfungsvorbereitungskurs 2012|1:** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer
16.4.12-10.5.12	CGEIT-PV	**CGEIT-Prüfungsvorbereitungskurs 2012|1:** Kompakter Prüfungsvorbereitungskurs für erfahrene Kursteilnehmer
17.4.12	LAB-WS	**Wireless & Mobile Security**
18.-19.4.12	PR-BJ	**Risiken im (IT-) Projektumfeld erkennen und managen:** Identifikation, Bewertung und Management typischer Projektrisiken
18.-19.4.12	LAB-NP	**Networking & Penetration Testing**
23.4.12	ISMS-EXP	**ISO 27000/2 Self Assessment - effiziente ISMS Standortbestimmung:** ISMS-Ausbaugrad effizient und korret messen
2.-3.5.12	LEA-RW	**Meistern kritischer Situationen (für Revisoren und Sicherheitsbeauftragte):** Verbesserung des persönlichen Kommunikationsverhaltens in kritischen Situationen
7.5.12	AWA-KK	**Wirksame Awareness-Kampagnen gestalten und umsetzen:** Systematische Planung/Durchführung von Aktivitäten und Kampagnen für anhaltende Awareness (mit zahlreichen Beispielen/Erkenntnissen aus der Praxis)
7.-8.5.12	LAB-NA	**Network Analysis - Sniffing**

Das gesamte Trainingsangebot mit näheren Informationen finden Sie online unter www.isaca.ch

IMPRESSUM ISACA NEWS

Herausgeber, Redaktion: ISACA Switzerland Chapter
Adresse: Kurssekretariat, c/o ITACS Training AG, Stampfenbachstr. 40, 8006 Zürich
Erscheinungsweise: 4x jährlich in Swiss IT Magazine
Mitgliedschaft: Wir begrüssen alle, die Interesse an Audit, Governance und Sicherheit von Informationssystemen haben. Es ist nicht notwendig, dass Sie Sicherheitsspezialist oder Revisor sind, um bei uns Mitglied zu werden. Weitere Informationen finden Sie unter www.isaca.ch

Copyright: © Switzerland Chapter der ISACA