

Appendix 1: Abstracts



Trust in, and value from, information systems

SCANDINAVIAN CONFERENCE

2010

ISACA Sweden Chapter are hosting the conference in
Gothenburg Sweden
20 – 21 of April 2010



Abstracts Key note speakers

“Global Security Overview”

Speaker: Bengt Lundberg
Vice President and Chief Security Officer (CSO),
Volvo Group

TBD

Bank Corporate Governance – challenges within IT Governance, Operational risk and Organisational Complexity.

Speaker: Einar J. Lyford
Senior Advisor
The Financial Supervisory Authority of Norway(FSA/Finanstilsynet)

Bank Corporate Governance is of great relevance both to individual banking organisations as well as national and global financial communities when servicing their markets. The operations behind the services offered, have over a relative short period of time emerged from manual operations to semi- or fully IT based operations establishing more complex organisational structures through interdependency with other financial institutions and extended outsourcing of IT processes and application development.

IT systems supporting this development including internal reporting and complex services, has gradually been developed over time based on multi technologies both in core systems and multiple relevant applications. The IT infrastructure has been stretched in different directions substantially increasing operational complexity.

IT competence within the organisations is varying. IT systems, applications and subsequent IT investments have often been perceived so complex that it has been met with ignorance both from the senior management and the business responsible units.

The major challenge within Bank Corporate Governance is consequently to focus on IT Governance and how to implement an efficient governance structure. This challenge can only be met by acknowledging that IT is a core asset within strategic management and bank corporate governance where an IT based market platform is set to perform secure and reliable transactions between clients in a two-sided market, both in national and global terms. This will require substantial organisational learning both at the senior management level and at the board member level.

The future direction of Information Security good practice

Speaker: Steve Durbin
Vice President Sales and Marketing,
ISF

In this presentation I will introduce the audience briefly to the Information Security Forum and what it stands for.

I will then take them through a short description of the ISF approach to good practice in information security and how this forms the basis of everything that we do at the ISF.

I will then move on to look to the future and I will be describing how the ISF approaches the future of risks and threats to the confidentiality integrity and availability of information in the future. I will touch on the role of information security within an organization, highlighting the fact that this should be to support and enable the business, for without a successful business, there is no need for information security!

However a key task for information security is to defend the business against threats that could cause business impact, and to permit the business to operate. This is encapsulated in the ISF's Threat Horizon methodology. I will explain the concept, provide examples of how this has been used in the past and will also detail predictions for 2010/2011.

Having established what the future might look like I will then look more practically at how good practice should evolve over time to address the needs, demands and requirements that the future may potentially bring.

I will close with some tips and guidance for meeting the challenges of the future in a business effective fashion.

Abstracts Governance

Paving the way for a new corporate policy using the “no surprises” rule

*Speaker: Erik Dagfinn Wisløff, CISA, CISM
Senior Risk Management Advisor
Telenor Group*

Successfully rolling out and implementing a corporate policy and procedure in a multi-national company relies on people across jurisdictions, cultures and subject domains accepting the principles and tasks that are outlined. It is not enough that the policy and procedure has business value; it must be accepted and understood.

The presentation will review the approach Telenor Group Risk chose in 2006 when developing a new policy and procedure for Enterprise Risk Management and their chosen strategy for the subsequent updates. Key topics include

- Outlining the chosen approach to gain buy-in from key stakeholders
- Reviewing the process for developing the policy and procedure content
- Highlighting key learning points

Usable Privacy and Identity Management

*Speaker: Prof. Dr. Simone Fischer-Hübner
Karlstad University*

In our networked society, users have lost effective control over their personal spheres and privacy is increasingly at risk. When communicating over the Internet, individuals leave long lasting trails of personal data. Social network sites, where users tend to disclose very intimate personal details about their personal life as well as social and professional contacts, have in recent years caused serious privacy concerns.

Privacy-enhancing identity management systems, such as those developed within the PRIME and PrimeLife EU projects, allow users to act securely in the information society while keeping sovereignty over their personal spheres. This presentation will first discuss emerging privacy risks and will present basic concepts of the PRIME/PrimeLife architecture. Finally, it will discuss HCI challenges for usable privacy-enhancing identity management

IT Governance: hvilken innfallsvinkel har du?

*Speaker: Nils Due-Gundersen,
Manager
Accenture*

IT Governance – det dreier seg om styring, lederskap og beslutninger som skal generere forretningsverdi. Flott, men hvordan?

Presentasjonen tar for seg ulike innfallsvinkler til IT Governance ved å se nærmere på verktøy og løsninger, eksempelvis rammeverk, modeller, prinsipper, strukturer, fora, prosesser etc. Som publikum skal du få bedre kjennskap til hva som fremmer IT Governance, og hvordan dette kan gjøres/tilnærmes rent praktisk.

Governance and control of CA (Certificate Authority)

*Speaker: Claus Rosenquist, CISA
PBS/DanID*

Safety and technical infrastructure behind NemID is extremely complex and extensive. When NemID is put into operation, it will enable users to access the public self-service systems, a number of private IT services and all banking services.

Operation, administration and management requires that DanID establish a rigorous governance and control structure based on best practices and frameworks.

The Governance structure must handle many different stakeholders as government, finance, IT vendors, auditors and affiliates.

The session will address the methods and principles by which DanID will manage the governance and IT security behind the NemID setup, including reporting to be done to the public and financial sectors.

Abstracts Governance

Ensure and prove the business value of IT

*Speaker: Erik J. Andersen, CGEIT,
Director IT Governance consulting,
Symbic A/S*

Most organisations don't know the real value of the investments in IT. They don't have clear value statements about measurable expectations. And they don't measure what value is actually realized from IT investments.

This leads to an over-focus on cost control and short term financial benefits, which is only a small part of real potential value of IT.

You can't steer a ship on a ocean journey by looking out at the endless water. You need a clear strategy, direction and navigation. Also, you can't keep the ship on course by oiling the machine, though you supply the necessary power for sailing the wrong way.

Why do complex IT-enabled business projects so often run off track, causing scandals?

Operational Risk Management

*Speaker. Ole Hvidkjær, CISM, CISA,
Senior Adviser, Operatinal Risk,
Danmarks Nationalbank*

Danmarks Nationalbank's objectives and tasks shall be fulfilled and performed on the basis of fundamental values such as quality and professional skills, diligence, efficiency, security and control. This requires systematic analysis of and decisions about the performance of tasks, including whether operational risk management is sufficient. This session will describe how operational risk management is organized and how classification of business activities, risk assessments, security, procedures, business continuity and incident handling fits into the OpRisk management framework.

IT Governance in real life – with a little help from COBIT and ITIL

*Speaker: Christian F. Nissen,
CEO,
CFN People*

Everybody talk about IT Governance and business driven IT these days but very few do something about it. During this presentation you will get practical advice on how to approach IT Governance initiatives in your own organization based on a case from Denmark and best practices from COBIT, VAL IT, ITIL and Weill & Ross.

- What do we mean by IT Governance, and why is it interesting?
- How do you set up appropriate organizational governance structures and roles to facilitate business driven decision making?
- How do you prioritize and manage the investments and resources allocated to the portfolio of services, projects and customers?
- How do you set up goals, measurements and controls to manage the performance of the IT enabled services and investments?
- How do you support the IT Governance framework with agreements, models, processes and tools?
- How do you approach the necessary organizational changes

Identity federations and e-ID's – new legal opportunities with the e-delegations proposal

*Speaker: Per Furberg
Advokat/Attorney-at-law
Setterwalls*

E-delegation has had the task is to propose a strategy for the agency's work on e-government. A key component of this work is the proposal put forward to establish a coordinating mechanism for e-identification, electronic signatures and related services - an autonomous governing board (Board of e-coordination) to provide services to affiliated agencies, such as . legitimation, signature and stamp, etc. Support is also given for the corresponding development of the economy. To the proposal, now under consideration at the Cabinet Office, is also introducing " e-service identifications for the public sector and industry. - Per Furberg, who participated in the process of preparing the proposals, will tell us about the solution and the legal possibilities that it can provide.

Abstracts Governance

BCP and Risk Management from a Volvo IT perspective

Speaker: Stefan Karlsson,

Volvo IT

CIO:n och IT Governance: Klassresans hotande baksmälla

Speaker: Johan Magnusson

Centre for Business Solutions Chalmers University

The lecture will cover various aspects of the current and possible development surrounding the role of the CIO and the relationship between the CIO and IT Governance.

Abstracts Assurance

The Clarity Project for Internal Audit Standards

*Speaker: Anders Bisgaard, CPA
Beierholm*

In developing the clarified ISAs, IAASB acknowledged that a good audit is a “thinking audit” – one in which the auditor gives thoughtful consideration to the circumstances. This lecture will highlight the following

- The purpose and objectives for the clarity project,
- Objectives to help the auditor to understand what the aim of the work is and to use professional judgment in applying that understanding to the work that needs to be done in the specific circumstances of the engagement,
- Help the auditor to understand the purpose of the requirements / outcome to which the requirements are directed, and formulate the procedures necessary in complying with the requirements, and
- The auditor need to step back and evaluate whether the aim of the work has been achieved; if not, to then decide whether more needs to be done to achieve the objectives in the particular circumstances of the audit and whether sufficient appropriate audit evidence has been obtained.
- The ability to achieve an individual objective is equally subject to the inherent limitations of an audit.

IT audit over Financial reporting

*Speaker: Torkil Hindberg, CISA
Senior Manager, IT Advisory
KMPG*

IT audit as part of a financial audit has traditionally been focusing on General IT Controls and often related to infrastructure and security measures. This is of course all important subjects to cover in the audit, but does it always contribute to support the financial auditors goal; the audit statement?

The presentation will look at how the IT auditor can help the financial auditors in confirming the financial statements through the IT way of thinking. IT auditors confirming financial audit objectives through relying on application logics and data analysis. The goal is a more efficient financial audit with better quality.

Key factors to success:

- IT auditor involvement from planning to completion
- Understanding of the scope
- Understanding that there are two clients involved (financial audit team and the audit client)
- Being able to communicate in financial audit language
- Focusing on achieving objectives wider than the IT perspective
- Deliverables that meet the expectations, both internally and externally

ISAE 3402 in Practice

*Speaker: Jess Kjær Mogensen, CGEIT, CPA
PWC*

Entities outsource aspects of their businesses to organizations that provide services ranging from performing a specific task under the direction of the entity to performing one or more of the entity’s business functions. Frequently, such services relate to information used by the service organization’s clients to prepare their financial statements. Clients and their auditor often need a description of the relevant controls at the service organization and assertions about the effective design of those controls and their operating effectiveness. ISAE 3402 deals with assurance engagements to provide a report for use by user entities and their auditors on the controls at a service organization that provides a service to user entities that is likely to be relevant to user entities’ internal control, as it relates to financial reporting.

In this lesson you will hear about the following:

- The differences from RS3411 and SAS70 reports.
- How a typical ISA3402 reporting is expected to be.
- How to deal with operational controls that have no material financial impact.

Business improvement initiatives in regulatory controlled industries

*Speaker. Staffan Söderberg
Acando*

When a company initiates efficiency programs, lower cost is usually the driving factor. The primary objective is to reduce cost, lead times and improve product quality. In industries where strict regulations are governing how activities are carried out it tends to be focused on compliance instead. Traditional methods of Business Process Management, Lean Sigma, address not the compliance part, which can result in the company loosing compliance with regulatory requirements. What is needed are methods to gain better control on exactly what are the requirements and where they are met in the business.

Abstracts Assurance

The PCI challenges now and in the future

Speaker. Lars Syberg

FortConsult

The PCI standard has now been around for 5 years and for many people it is still a relatively new thing. Despite the short history, for a standard that is, the PCI standard has had significant influence on many companies due to the fact that their security mechanisms and processes are now being dictated directly from an American organisation.

Lars Syberg, PCI Product Manager at FortConsult, will share the experiences he has gained by working with PCI projects in banks and chains of shops during the past 5 years. As one of the only PCI auditors in Scandinavia represented in the VISA and PCI Council's closed meetings, Lars has obtained a great deal of insight into the development and future plans of the standard. In his presentation he will give the participants a glimpse into this world and at the same time provide insight to what can be expected from the next generation of the PCI standard

Governance of projects and the role of the audit

Speaker. William Dennett

Senior Manager

Metier

Governance of individual projects and a portfolio of projects is an important theme for companies who derive much of their production from an organisation that uses projects as the primary mechanism for delivery.

The presentation will cover:

1. Governance of projects – the role in achieving operational excellence
2. Objectives of project governance
3. Scope of project governance – Stage gate process and reviews
4. Audits
5. Case study 1: oil and gas
6. Case study 2: major public project
7. Case Study 3: IT project
8. Best practice

TBD

Speaker: Stefan Simonson, CISA, CISM, CGEIT, CCSA, CGRCP-IT

Partner

Amentor

As the importance of IT is increasing and more and more companies state that their IT solutions are heavily business critical, the risks associated with the use of IT are likewise increasing. In this session, Stefan presents the most common IT risks that the companies are facing. In his presentation he also goes through typical audit findings associated with the risks and what companies need to do to avoid them. To highlight the importance of good IT risk management, Stefan uses examples taken from the media during the last years.

Jeg er sikkerhetsansvarlig – hvorfor vil ingen spise lunsj sammen med meg?

Speaker: Rune Ask

Risk & Compliance Manager

Det Norske Veritas

Mange sikkerhetsansvarlige føler i dag at de blir sett på som en kjepp i virksomhetens hjul – en som alltid sier «Nei» til alle de aktivitetene som brukerne ønsker å gjøre. De blir ansett som «mørkemenn» som bare fokuserer på trusler og farer, og blir derfor sjeldent eller aldri involvert i nye prosjekter før disse går mot slutten eller er ferdige og får derfor liten påvirkning på den endelige løsningen.

Foredraget vil ta for seg hva en sikkerhetsansvarlig bør ha av kvaliteter og hvordan man skal få informasjonssikkerhet på agendaen i virksomheten, i stedet for å bli sett på som en bremsekloss.

Multiple Compliance Management

*Speaker. Bo Thygesen,
Aggrit*

How to ensure that you comply with multiple frameworks.
How to gain benefits/synergy from implementing one
framework for other frameworks.

The challenge is the several compliance demands Basel II,
ISO2700X, ITIL, Cobit etc.

The shortest way for compliance. A practical presentation
about compliance in entities, that need to comply with
several framework.

Multiple framework compliance especially hits
organizations within the public, financial and
pharmaceutical sectors. To design a compliance program
that enables synergies between the various initiatives will
increase efficiency, reduce risk and cost. The talk will go
through the various elements of multiframework
compliance and give practical guidelines on how to reach
shortest way to compliance in these environments.

Compliance Trends 2010

*Speaker: Thomas Baltzer Joensen
PBS*

A practical integration of ISO 27001 and ISO 27005 for superior security management.

*Speaker: Jan A Svensson
Director Information Security
Göteborgs stad*

New IT Security Model

Speaker: Jens Roed Andersen

In a very hostile environment, where the threat scenario changes almost daily and where funding has become scarce, the focus for information security needs to be put on Risk Management as well as the integration of the design and architecture in multiple risk scenarios. As new business models for IT service delivery arise, new security challenges is showing up, creating a growing need for a new way of thinking, designing and controlling information security. SaaS and Cloud Computing solutions might ave reached a higher maturity level, where the business case is valid, but the old perimeter based information security paradigme needs a brushup, utilising "out-of-the-box" creative thinking. This is paramount, in order for companies to utilise the full potential of these new technologies without compromising company security and general value. Since the potential benefits for the business of utilising new technologies and delivery models are huge, the information security community needs to be ready for this.

Can security be measured?

*Speaker: Professor Erland Jonsson,
Computer Security Chalmers University*

Non Stop Security –

Building security awareness the sweet way

*Speaker: Hilde Grunt, Draw Manager
Norsk Tipping AS*

Since 1999 “Non Stop Security” has been an internal brand name in Norsk Tipping. It started as a campaign but has become a way of thinking and a way to communicate. “Non Stop Security” gave Norsk Tipping an IT Security award in 2002, awarded by IT Sikkerhetsforum.

The presentation is an overview of 10 years of work with security culture and communication. It’s a story about security focused on business objectives using chocolate as a symbol and communication tool. Non Stop Security is also a story about staying power in building high level security and security awareness throughout the business.

The presentation will focus on how to develop a strong security culture to achieve a high level of security. Key topics are:

- You need more than campaigns; it is about daily activities and stamina.
- The use of logo and symbols in communication.
- You measure what you treasure. (And the other way around.)
- The Non Stop Security Game: the human factor, cardboard and chocolate

Risk management 2.0 – the key to cloud security

Speaker: Ulf Berglund, CISM

Senior Consultant

I Secure You2 AB

Movements towards the cloud delivery model is a very appealing proposition for most. A thorough information security strategy is the basis for a secure movement. Multidimensional risk management adds extra solidity and helps clarify the landscape with clear indicators for effective evaluation and incident handling.

Information- and IT-security at Ringhals, the targets Nuclear Power Plant in Sweden - how, what and why?

Speaker. Gert-Olof Nilsson

Controler Information- and IT-Security

Ringhals

Ringhals is the largest energy producer in Sweden and the availability of the production is of national interest. As a nuclear power plant there is also a large responsibility to ensure the security and safety of the process.

This in combination with the fact that it has become more and more obvious over recent years that the electricity sector is a very likely target for a cyber attack puts large demands on Ringhals to ensure the Information- and IT-security.

The speech will talk about the current external requirements, the threat to the energy sector and what Ringhals has done to respond to the situation from an Information- and IT-security perspective.

Continuous authentication: the user is the strongest link

Speaker. Patrick Bours

Associate Professor

Gjøvik University College

Normally the user is considered to be the weakest link in the "security chain". In this presentation we will show that we can improve the security of a computer system by actually looking at the behavior of the user behind the keyboard. We will show that an illegitimate user will be detected already within a few minutes of activity.

Data Protection and Privacy - Results from a global data privacy study

*Speaker: Gaute Lien, CISA, CISM, CISSP
Senior Manager,
Accenture*

The survey was a joint effort between Accenture and Ponemon Institute and harvested responses from 5512 cross-industry business and 15,732 individual respondents from 19 countries. The outcome is a better understanding on how data privacy perceptions and practices around the globe inform and influence data-protection strategies and provide concrete recommendations to improve the integrity, confidentiality and availability of data as part of a high-performance security agenda

Top level security

*Speaker: Per Thorsheim
Security coordinator
EDB Business Partner*

For any publicly listed companies there are corporate governance rules for the handling of inside information, and any trading based on such information is forbidden. Laws and regulations usually refer to handling such information with "due care", but the interpretation of this is left to each company and sometimes single entities within the company. How do you control access to such information?

This presentation will talk about common mistakes in this area, how misunderstandings occur between executive, legal, audit and technical staff, and how auditors themselves are commonly part of the problem. Real-life examples as well as recommendations will be provided.