IT Risk Management and Control Frameworks

Guðjón Viðar Valdimarsson
CIA, CFSA, CISA
Product Manager and Internal Auditor

Stiki

Microsoft Partner
Silver Independent Software Vendor (ISV)

ACP

bsi. ISO 9001 Quality Management ISO/IEC 27001 Information Security Management
Certificate No. FS 67386 ISO 9001
Certificate No. IS 67387 ISO 27001

Summary

- Introduction or the “art” of Risk Management
- The objectives, risks and controls
- Risk Management Methodology
- The control frameworks
- IT Risk Management

Likelihood rating	1	2	3	4	5	6
E	IV	III	II	I	I	I
D	IV	III	III	II	I	I
C	V	IV	III	II	II	I
B	V	IV	III	III	II	I
A	V	V	IV	III	II	II
	Consequence rating					

Introduction or the “art” of Risk Management

“Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities.”

Or how to stop bad things from happening by figuring out what can happen and do something about it !

What do you need ?

To do a risk assessment you need :

Objectives/assets

- What does management and the board want to aim for in terms of risk appetite and risk tolerance.
- What are the critical assets and processess you want to protect

Risks

- What are the relevant risks for the subject/assets at hand

Controls

- What generally accepted control framework is appropriate for the subject matter.

Risk Management Methodology

There are a number areas of risk management areas depending on the industry or subject at hand.

Financial risk management (VaR and CVaR)	Enterprise risk management	Risk management activities as applied to project management	Risk management regarding natural disasters	Risk management of information technology

IT Risk Management

The Certified Information Systems Auditor Review Manual provides the following definition of risk management:

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

Risk Management Methodology

There are a number methods of risk management in use but for the most part, these methods consist of the following elements, performed, more or less, in the following order:

1. Identify, characterize assets/critical processes
2. Identify, characterize threats
3. Assess the vulnerability of critical assets to specific threats
4. Determine the risk
5. Identify ways to reduce those risks
6. Prioritize risk reduction measures based on a strategy

The control frameworks

The control frameworks are relevant for the risk area.

- Financial risk management (VaR and CVaR) use a specialized control framework such as described in Basel II.
- Enterprise Risk Management systems are using a general ERM control framework such a COSO.
- Risk management of information technology generally adopts either ISO 27001 or COBIT 5 depends on the region and size of company.

The control frameworks

The status of controls is crucial. The question is whether they actually exist and if they are effective.

- IT auditors seek to verify the existance of controls and their effectiveness
- Only implemented controls are relevant for risk mitigation (risk treatment)
- The generally accepted control frameworks are the standard, user defined control frameworks lack the reference to best practice.

IT Risk Management

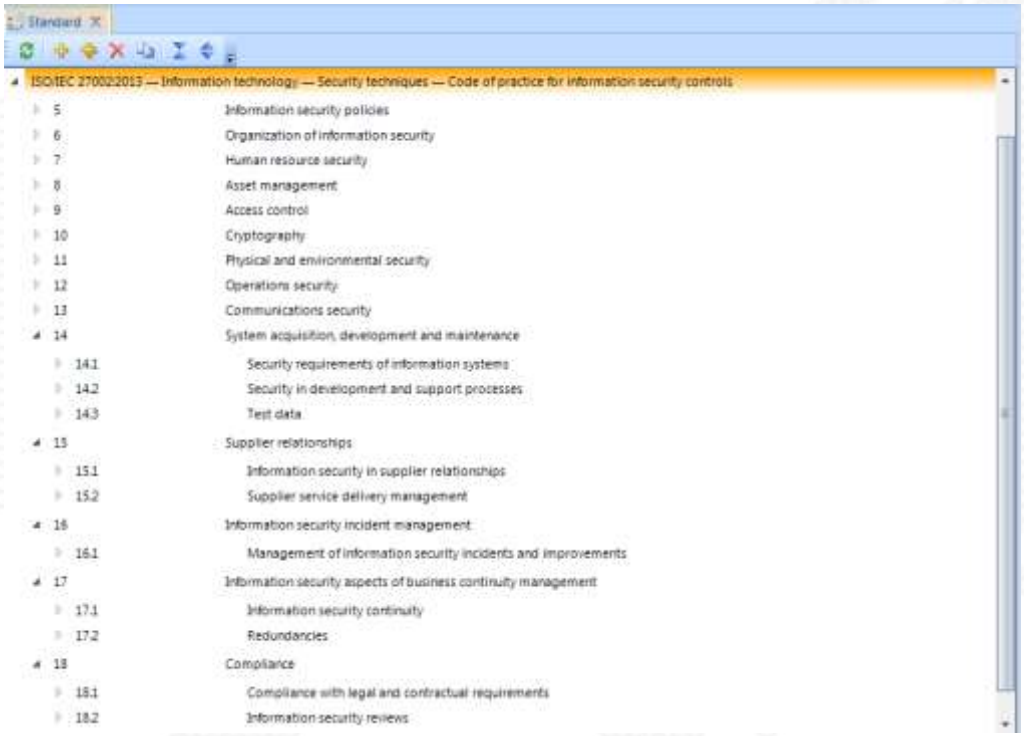
The ISO/IEC 27002:2013 Code of practice for information security management recommends the following be examined during a risk assessment:

- Security policy and organization of information security
- Asset management
- Human resources , physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance, (see Systems Development Life Cycle)
- Information security incident management,
- Business continuity management and regulatory compliance.

IT Risk Management

The quick way:

- Select framework
  - ISO 27001 is the most common in Europe and Asia
  - Certifiable standard



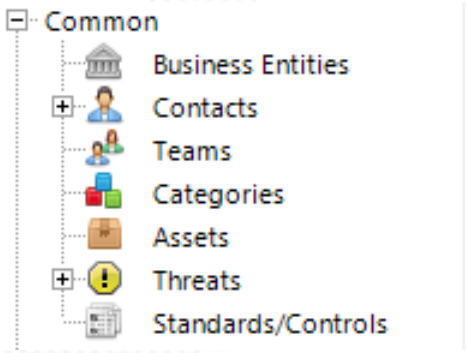
Microsoft Partner
Silver Independent Software Vendor (ISV)

Stiki

IT Risk Management

The quick way :

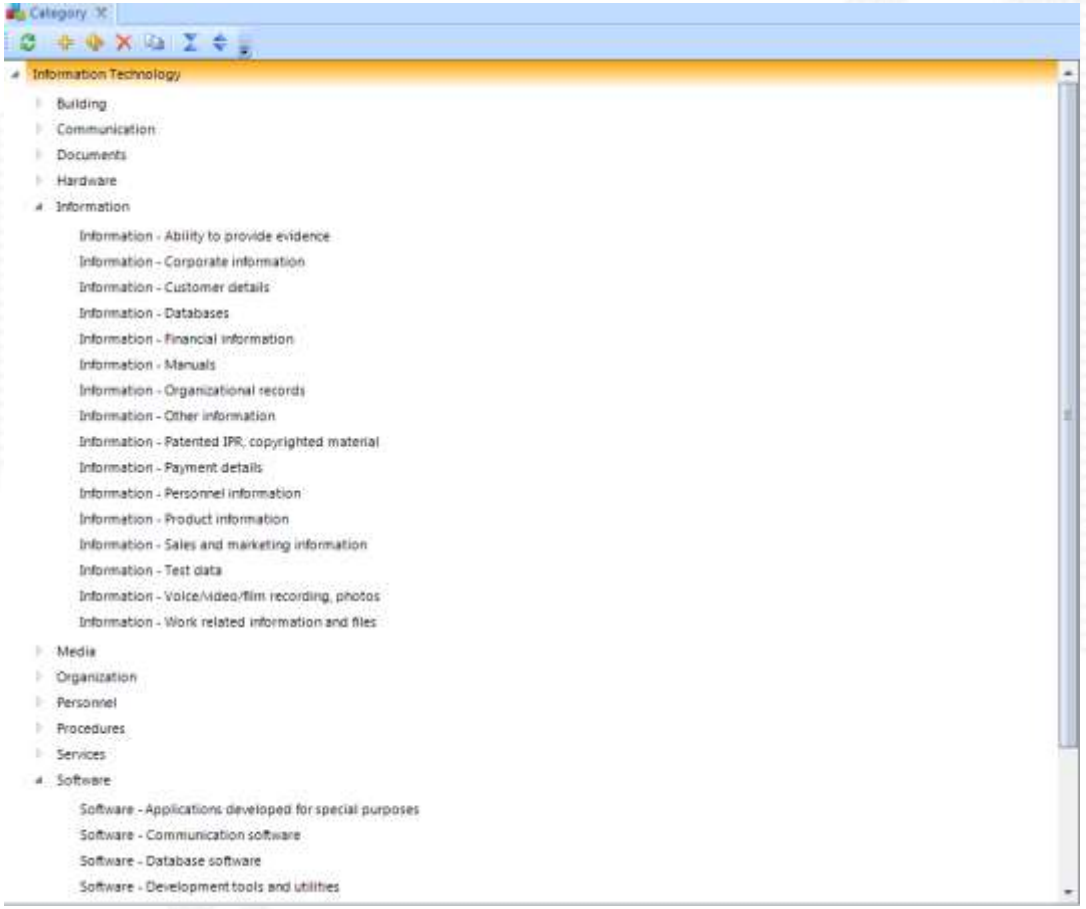
- Determine scope
- Contacts
- Metrics
- Risk appetite



IT Risk Management

The quick way :

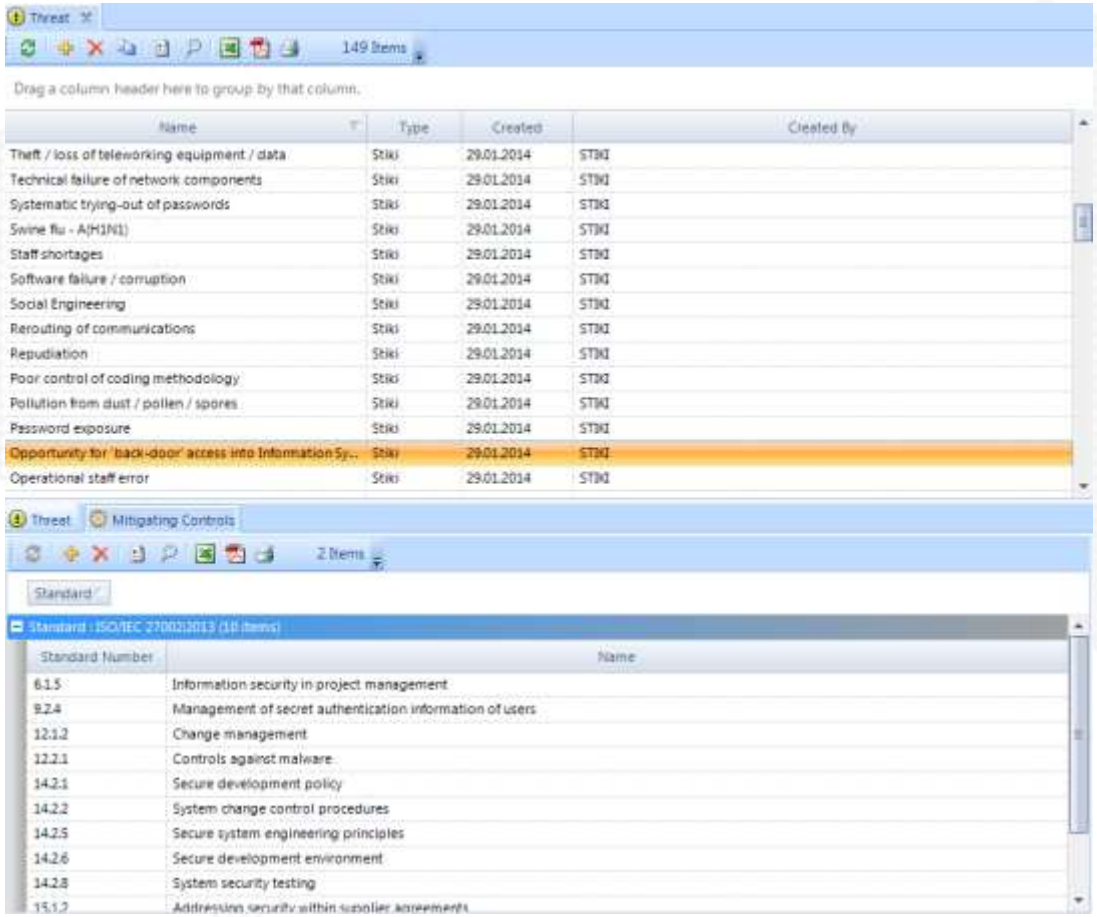
- Assets based on asset classification
- Threats from a threat database



IT Risk Management

The quick way :

- Threats from a threat database linked to the control framework



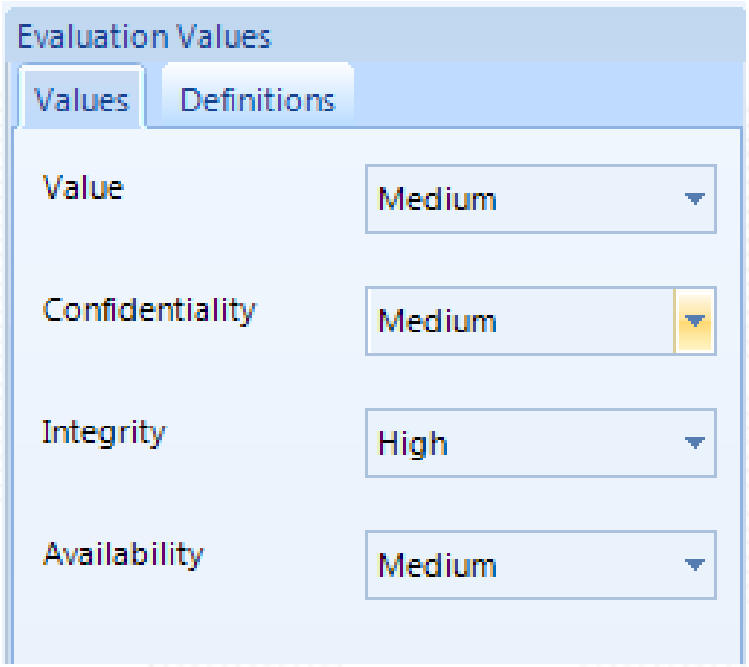
Microsoft Partner
Independent Software Vendor (ISV)

Stiki

IT Risk Management

The quick way :

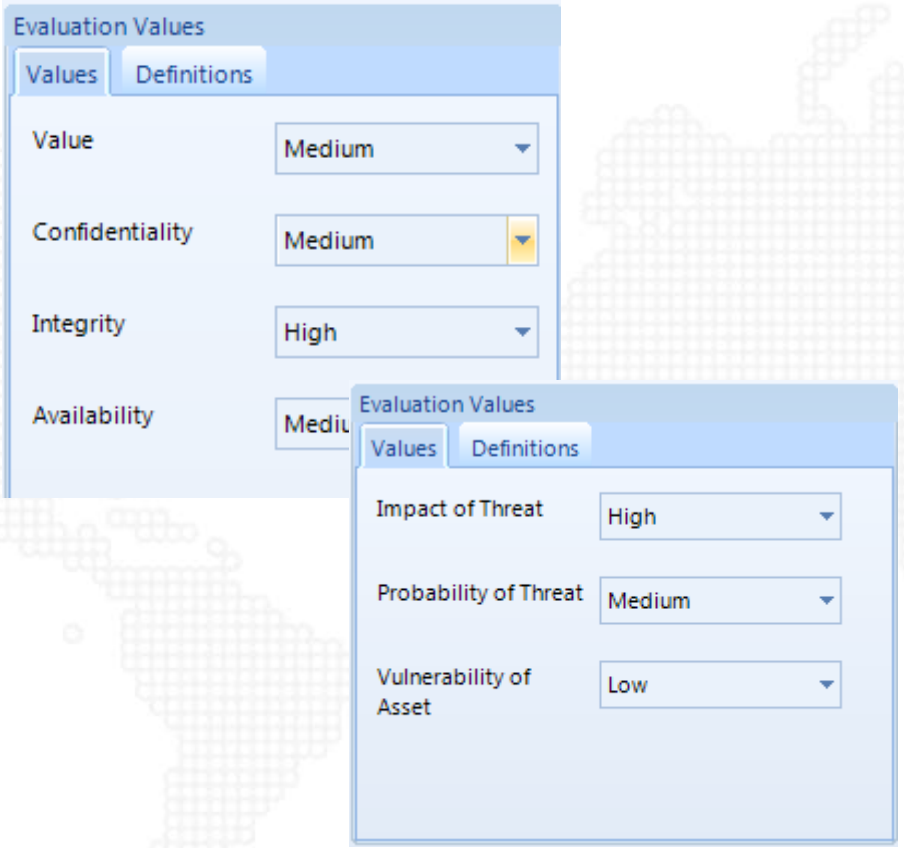
- Risk assessment determines value for asset regardless of threats



IT Risk Management

The quick way :

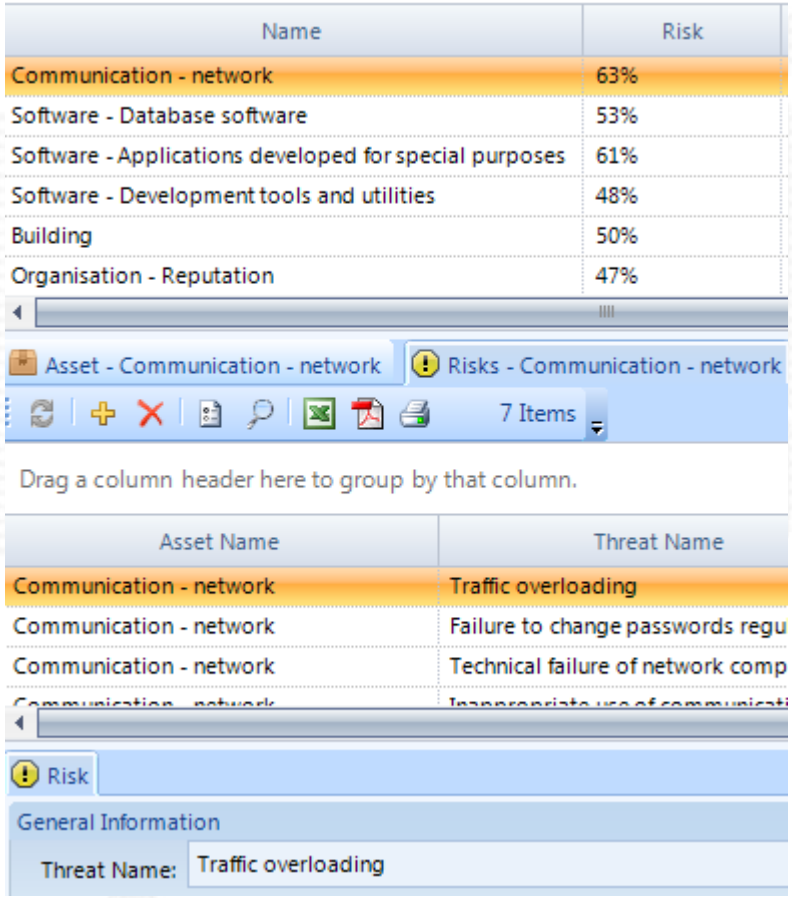
- Risk assessment determines value for asset regardless of threats
- Threats linked to specific assets and rated consistently



IT Risk Management

The quick way :

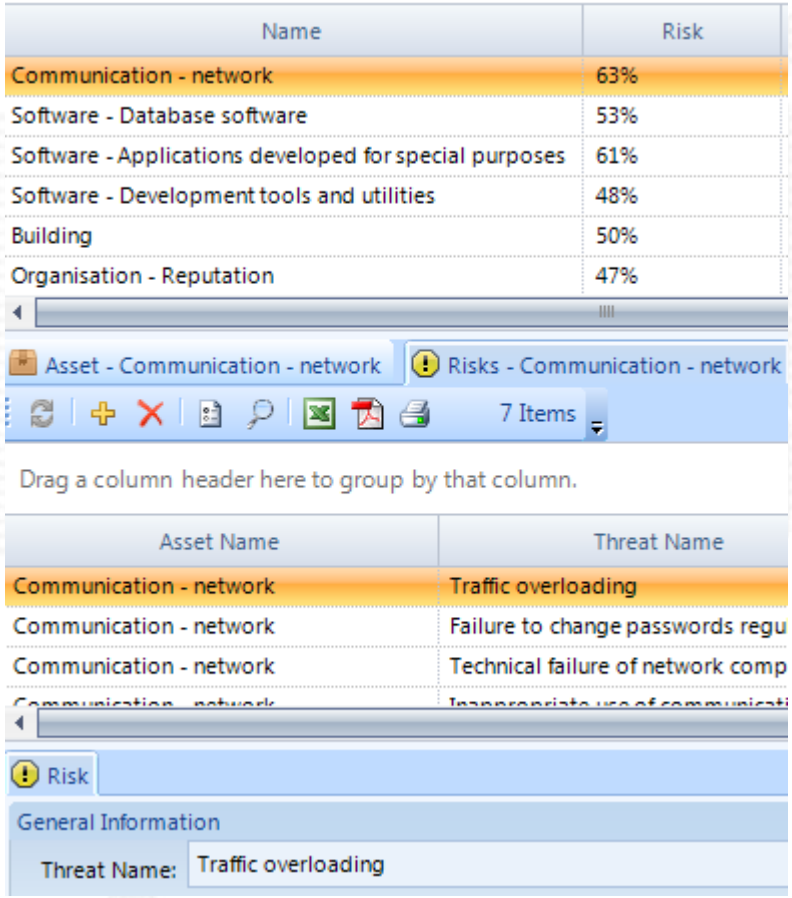
- Calculate inherent risk



IT Risk Management

The quick way :

- Calculate inherent risk



IT Risk Management

The quick way :

- Calculate residual risk
- Decide on risk treatment based on the risk appetite
- Accept risk, transfer, avoid or reduce

119 Items

Dragðu dálk hingað til að hópa eftir þeim dálki

Asset Name	Threat Name	Risk	Current Risk	Future Risk	Treatment
Information - Customer details	Corruption of data	71%	Min	Min	Accept Risk
Information - Customer details	Malicious attack - intention of theft	59%	Min	Min	Accept Risk
Information - Customer details	Malicious software (e.g. viruses)	65%	Min	Min	Accept Risk
Information - Customer details	Back-ups unavailable	65%	Min	Min	Accept Risk
Information - Customer details	Negligent deletion of data	47%	Min	Min	Accept Risk
Information - Organisational records	Corruption of data	53%	Min	Min	Accept Risk
Information - Organisational records	Software failure / corruption	53%	Min	Min	Accept Risk

General Information

Threat Name: Theft of mobile equipment

Asset Name: Hardware - Computing resources

Base Risk: 59% Current Risk: Min Future Risk: Min

Manage Risk: Accept Risk

How/Resources needed:

The current security risk is at minimum so the company has decided to accept that risk.

Controls

37 Items

Drag a column header here to group by that column.

Asset Name	Name	Control Number	Impleme
Hardware - Co...	Unattended user equip...	11.3.2	28.09.2011
Hardware - Co...	Confidentiality agreeme...	6.1.5	28.09.2011
Hardware - Co...	Information labeling an...	7.2.2	28.09.2011
Hardware - Co...	Supporting utilities	9.2.2	28.09.2011
Hardware - Co...	Mobile computing and...	11.7.1	28.09.2011
Hardware - Co...	Responsibilities and pro...	13.2.1	28.09.2011

Microsoft Partner Independent Software Vendor (ISV)

Stiki

Thank you!

Any questions ?

Guðjón Viðar Valdimarsson
CIA, CFSA, CISA
Consultant / Product Manager RM Studio
gudjon@stiki.eu