Risk Management
for SME's

SANS Information Security Webcast

17 Jan 2012
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

SANS Webcast archive:
https://www.sans.org/webcasts/risk-management-smes-94934

Slide handout (English):
http://nouvelstrategies.com/InfoSec-for-SMEs

Slide handout (French):
http://www.hesge.ch/heg/ccsie/CCSIE_ressources.html

Agenda

- Introduction to information risk management
- ISO 27005: the "new" risk management standard
- Risk assessment/management methodologies for SME's
- Risk metrics
- Final words

What is information risk?

- Risk is the potential harm that may be caused by a future event.
- Information risk focuses on reducing harm to information- and IT-related resources.
  - Loss of confidentiality, integrity, or availability.
- Information risk is the responsibility of many parts of the organization in addition to IT:
  - management
  - human resources
  - legal
  - purchasing
  - finance
  - facilities

What are information resources?

- Information resources can be defined in categories:
  - information
  - IT infrastructure
  - computer hardware
  - people
  - computer software
- Information exist in different formats:
  - digital: disk, tape, USB/solid-state devices
  - paper: printouts, books
  - oral: live/recorded conversations

The relationship between risk management and information security?

- An information risk management program identifies, assesses, and prioritizes risks—and then determines the best way to control these risks.
- An information security program implements controls to achieve risk management objectives.
- Organizations implement information security as part of the process of risk management.

Simple risk management strategy for SME's

1. Risk assessment drives the process, determining what risks need to be addressed.
2. An information security program is implemented to achieve the risk management objectives identified during the risk assessment.
3. An IT audit/assessment verifies that risk objectives have been been successfully achieved.

Agenda

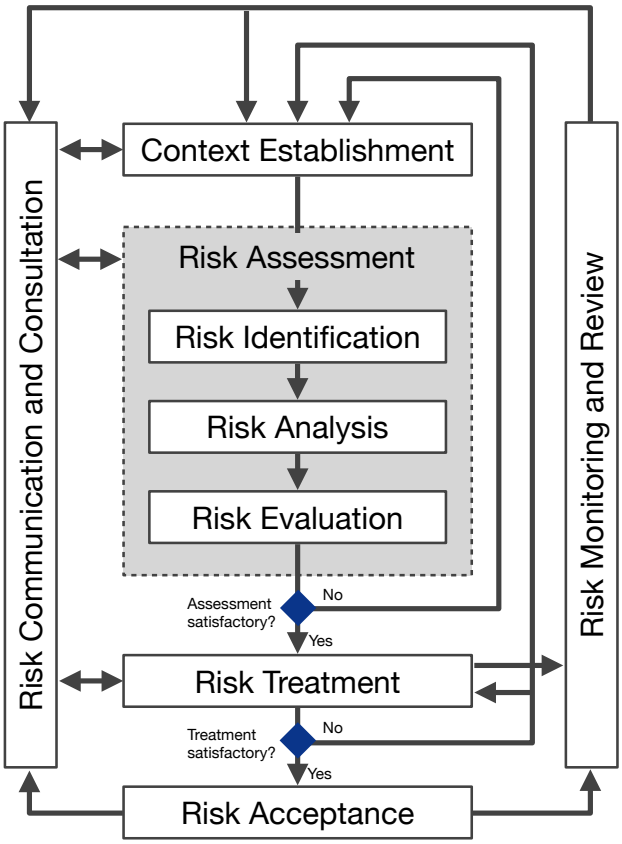
- Introduction to risk management
- ISO 27005: the “new” risk management standard
- Risk assessment/management methodologies for SME’s
- Risk metrics
- Final words

What is ISO 27005?

- The International Organization for Standardization (ISO) standard for “Information Security Risk Management:
  - First released in 2008, updated in 2011.
  - Part of the ISO 27000-series of information security standards.
- Defines a basic, risk management process.
- Redefines some risk management jargon that may cause some short term confusion.

ISO 27005 risk management process

1. Context establishment
2. Risk assessment
3. Risk treatment
4. Risk acceptance
5. Risk monitoring/review



Risk treatment

- A risk treatment plan is a proposal to management that describes how to respond to risks reported in a risk assessment.
- ISO 27005 defines 4 options (and new jargon) for risk treatment:
  - Risk retention (formerly risk acceptance)
  - Risk reduction (formerly risk mitigation/remediation)
  - Risk sharing (formerly risk transfer)
  - Risk avoidance

Agenda

- Introduction to risk management
- ISO 27005: the “new” risk management standard
- Risk assessment/management methodologies for SME’s
- Risk metrics
- Final words

Risk assessment/management methodologies

- There are many methodologies for risk assessment and risk management.
  - CRAMM, DUTCH A&K Analysis, EBIOS, FAIR, ISAMM, ISF Methods, Mehari, OCTAVE / OCTAVE Allegro, SP800-30, ...
  - The EU ENISA website maintains a list: http://rm-inv.enisa.europa.eu/rm_ra_tools.html
- These methodologies are complex generally take 6-12 months commitment to learn and implement.
  - This often doesn’t scale for SME’s

Developing a strategy for information risk assessment that works for SME's

What's the better strategy for performing risk assessment?

Jan	12-month risk assessment (no information security program implemented; no risks reduced)
Feb	
Mar	
Apr	
May	
Jun	
Jul	
Aug	
Sep	
Oct	
Nov	
Dec	

vs.

Jan	1-month risk assessment
Feb	Implement information security program to reduce risk
Mar	
Apr	
May	
Jun	
Jul	
Aug	
Sep	
Oct	
Nov	
Dec	

Primary purpose of risk assessment

- Identifying the "top risks" to be corrected or "mitigated".
  - Most organizations are only capable of targeting 5-10 information risks per year.

- Is it possible to identify the top 5-10 risks in less than 6-12 months?

“Knowledge-based” risk assessment

- Knowledge-based risk assessments are based on a “gap analysis” that compares:
  - A well-known industry standard for information security.
  - Your organizations current information security implementation.
- Can be performed rapidly, but:
  - What standard to use? Aren’t information security standards complex too?
  - How to “adapt” for your organization?

CPI-RISC risk assessment

- CPI-RISC
  - Continuous Process Improvement–Risk, Information Security, and Compliance.
  - Developed in cooperation with the Business Information Security Competency Center at the Geneva School of Business Administration. (http://www.hesge.ch/heg/CCSIE/).
- CPI-RISC risk assessment is well adapted for SME’s
- Uses “knowledge-based” risk assessment that references ISO 27001, ISO 27002, ISO 27005, and SANS 20 Critical Security Controls

CPI-RISC risk assessment process

- Task 1.1: Analyze environment
- Task 1.2: Prioritize risks
- Task 1.3: Assess risks
- Task 1.4: Report results

Analyze the business environment

Challenge: how to rapidly determine the critical information risks in a business environment?

- Perform a mini-BIA (Business Impact Analysis).
  - Determine how long the organization can be without an information resource before it negatively impacts the organization.

Prioritize information- and IT-related risks

Challenge: how to rapidly adapt a risk assessment methodology to an SME?

- Use a predefined, simplified information risk framework:
  - organize according to business functions.
  - assign priorities based on analysis of business environment.

CPI-RISC Information Risk Framework

- Originally released in 2010.
- Defines 33 risk areas:
  - organized into 7 business functions:
    - Management
    - Legal
    - Finance
    - Purchasing
    - Personnel
    - Facilities
    - IT
  - based on ISO 27001 and SANS 20 Critical Security Controls.
  - http://cpi-risc.org/en/CPI-RISC.html

Assess information- and IT-related risks

Challenge: how to rapidly adapt a risk assessment methodology to an SME?

- Use a predefined, simplified risk survey template based on the information risk framework.
  - CPI-RISC includes a risk survey template.

Report results as a risk treatment plan

Challenge: how to effectively communicate information risks to management?

- Develop effective risk metrics.
  - CPI-RISC includes the Simple Risk Maturity Model (SRMM) metrics.
- Focus on reporting the top risks.

CPI-RISC risk assessment process

More information published in Jan 2012 (this month)

- In English:
  http://cpi-risc.org/
- In French:
  http://www.hesge.ch/heg/ccsie/CCSIE_ressources.html

Agenda

- Introduction to risk management
- ISO 27005: the “new” risk management standard
- Risk assessment/management methodologies for SME’s
- Risk metrics
- Final words

The role of risk metrics

- Risk metrics have two important roles:
  - Quantifying the current level of risk.
  - Demonstrating the success of your information security program over time.

Risk metrics

- A measurement is the result of counting; a quantitative value indicating the size, length, or amount of something.
- A metric is a the result of analysis; a qualitative or subjective interpretation of a measurement.

Risk Level	Color	Face	Level of risk and potential impact on operational performance, compliance, and financial reporting
H	Red		High
M	Yellow		Medium
L	Green		Low

Simple risk maturity model

- CPI-RISC Simple Risk Maturity Model (SRMM) is a capability maturity model, adapted for risk approximation.
  - Metric for specific risks in an organization, based on whether risks are being managed.
  - Approximates risk.
  - Assumes unmanaged risk correlates with high risk.
    - Distinction limited to information- and IT-related risk.

SRMM matrix

- Defines simple risk maturity score for specific risks:

Score	Definition	Description
1	Ad hoc	Risk is managed inconsistently or unmanaged.
2	Informal	Risk is managed consistently, but without documented processes.
3	Formal	Risk is managed using documented processes.

Agenda

- Introduction to risk management
- ISO 27005: the “new” risk management standard
- Risk assessment/management methodologies for SME’s
- Risk metrics
- Final words

Upcoming Webcasts for SME’s

Feb, 2012 Writing Information Security Policy for SME’s

Mar, 2012 Managing Network-related Risk for SME’s

Apr, 2012 Managing Legal, Regulatory, and Compliance Risk for SME's

Risk Management
for SME's

SANS Information Security Webcast

17 Jan 2012
Geneva, Switzerland

Jim Herbeck
Managing Partner, Nouvel Strategies
JHerbeck@NouvelStrategies.com

Member of Faculty, SANS Institute
JHerbeck@sans.org

SANS Webcast archive:
https://www.sans.org/webcasts/risk-management-smes-94934

Slide handout (English):
http://nouvelstrategies.com/E/InfoSec-for-SMEs

Slide handout (French):
http://www.hesge.ch/heg/ccsie/CCSIE_ressources.html