ITIL and Business Continuity (Service Perspective)

Hepix 2012 Conference

Prague, 23-27 April 2012

Patricia Méndez Lorenzo, Mats Moller

On behalf of the (IT&GS) Service Management team

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Outlook

- ITIL Principles
- Risk Management in ITIL
- Elements of Risk Management
- Quantification of Risks: Risk Assessment Method
- Examples applied to CERN functions
- Summary and plans

ITIL Principles

Business and **Service** Continuity Management require a formal analysis of the **risks** affecting the services or the business

- **ITIL processes** involved : Service Continuity Management and Availability Management
  - Establishment of a **Continuity & Availability Plan** through:
    - ✧ Risk Assessment
    - ✧ Critical Services identification

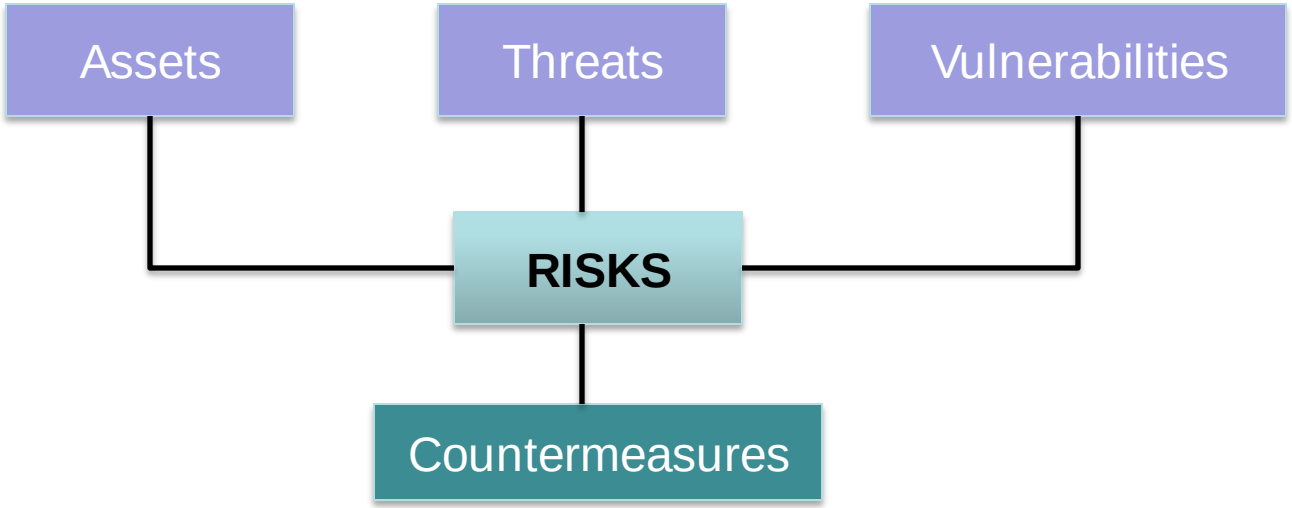
ITIL and Business Continuity

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Risk Management in ITIL

- Purpose of the process
  - Identification and quantification of risks
    - ✧ To ensure the provision of CERN services
    - ✧ To protect CERN business interests & assets
    - ✧ To support and maintain CERN's reputation
    - ✧ This means: Protect the organization's ability to perform its business
  - Application of (cost-) justifiable **countermeasures** ensuring the availability of the services

Essential management function, not just a technical process



CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Elements of Risk Management

Risk equation:

R = f (A, V, T), where:

- A = Asset (in some cases considered '*cost*')
  - Anything that can contribute to the delivery of a service; anything with a certain value
  - Example: People, data, applications
- V = Vulnerability
  - Weakness that can be accidentally triggered or intentionally exploited
  - Example: single points of failures (SPOF)
- T = Threat
  - Anything that might exploit a vulnerability
  - Example: Terminated employees, airport close to CERN

✓ *There is not too much to do against threats. However we can have influence on the vulnerability*

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Quantification of Risks

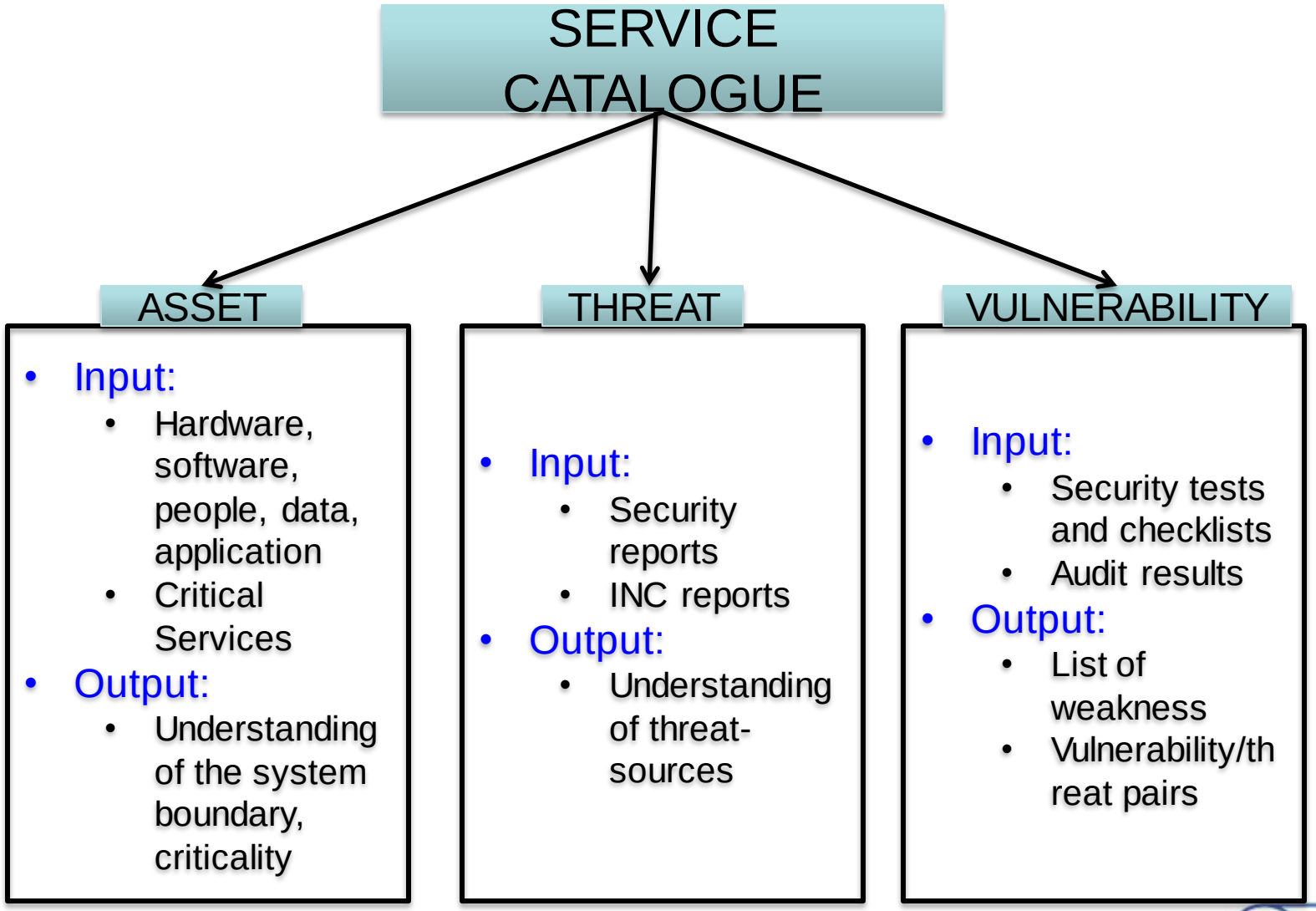
- Aim of a formal approach:
  - Identification of the risks affecting the services
  - Application of countermeasures based on the impact in case of failure
    - ✧ Reduction of the risk likelihood, severity and unpredictability
- Procedure:
  - Qualitative and quantitative evaluation of the risk function variables
  - Business Impact Analysis (BIA) procedures which identifies critical services
  - Definition of countermeasures based on:
    - ✧ Cost-justifications
    - ✧ Impact
    - ✧ Acceptance threshold

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Risk Assessment Method

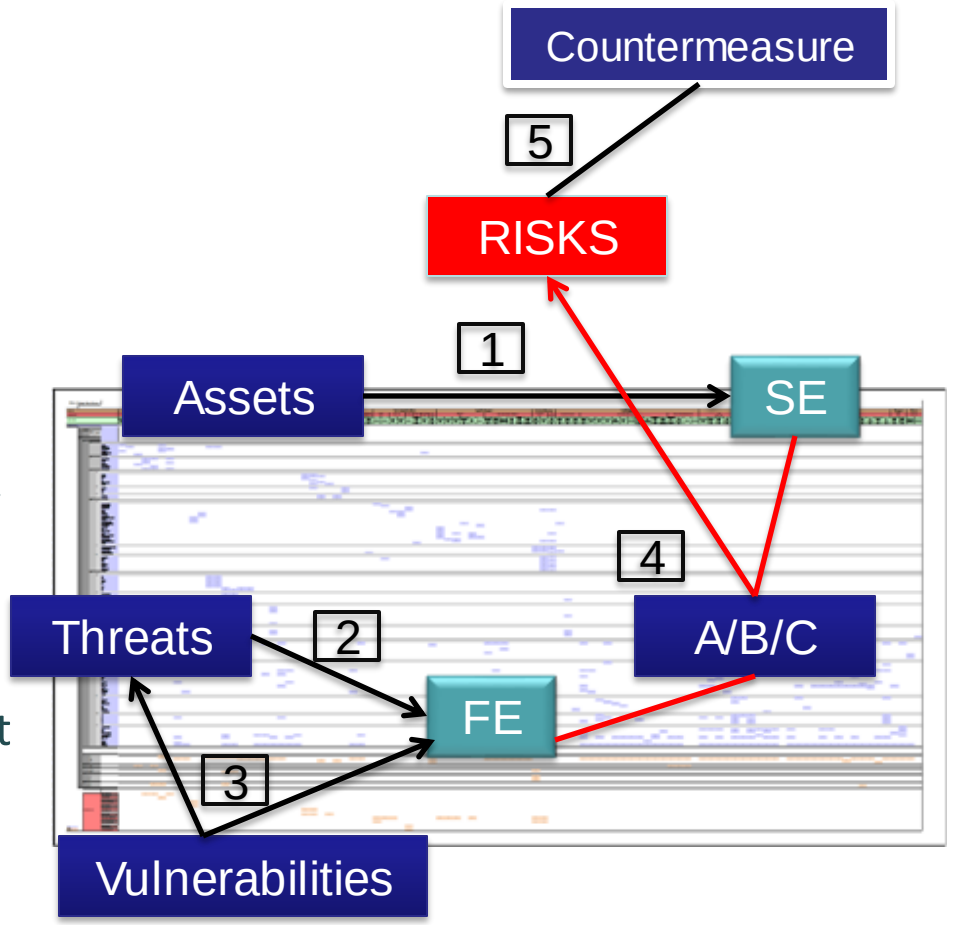
1. IDENTIFICATION → Risk equation variables and available control analysis
2. CALCULATION→ Likelihood determination and Impact analysis
3. RISK DETERMINATION→ Risk-level matrix OR risk evaluations
4. COUNTERMEASURES → Necessary actions and control recommendations
5. Results DOCUMENTATION

STEP1: Identification of variables



Our Source of information: Service Catalogue

- To define Assets
  - Specific value of each Service Element for the organization
    - Identification of critical services
    - Evaluation of the cost in case of a service lose
- To define Threats
  - Individual threats affecting the Functional Elements (hence the organization)
- To define Vulnerabilities
  - Known weak points against the defined threats
- Define Threats/Vulnerabilities pairs (relations)
  - In association to the assets



STEP1: Vulnerability/Threat

- Identification of Vulnerability/Threat pairs
  - This identification is necessary to quantify the risk

Vulnerability	Threat-Source	Description
Terminated employee ID's are not removed from the system	Terminated employees	Dialing into the company's network and accessing the systems
Guest ID is enabled on the servers	Unauthorized users (hackers)	Unauthorized users can access data
Single points of failures: not redundant expertise	Sickness	Experiment cannot apply a specific patch…

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

STEP 2: Risk calculation

- Previous elements needs to be evaluated in terms of **likelihood** and **impact**
  - Likelihood depends on the threat-source and the vulnerability level (e.g., High, Medium, Low)
    - ✧ L = f (T, V)
  - Impact depends on the criticality and the asset (e.g., High, Medium, Low)
    - ✧ I = f (C, A)
- Existing mitigating security controls should be considered

Risk = Likelihood x Impact

Example of basic Risk matrix

Impact ⟹ / Likelihood ⇓	Low (10)	Medium (50)	High (100)
High (1.0)	Low =10	Medium = 50	High = 100
Medium (0.5)	Low = 5	Medium = 25	Medium = 50
Low (0.1)	Low = 1	Low = 5	Low = 10

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

STEP 3: Risk Determination

A complete risk determination will include both qualitative inputs and risk assessment based on the risk-matrix

Vulnerability	Threat Source	Description	Controls	Likelihood	Impact	Risk Level
Terminated employee ID's are not removed from the system	Terminated employees	Dialing into the company's network and accessing the systems	Account locked after 90 days	L (0.1)	H (100)	L (10)
Guest ID is enabled on the servers	Unauthorized users - hackers	Unauthorized users can access data	None	H (1)	H (100)	H (100)
Single points of failures: not redundant expertise	Sickness	Experiment cannot apply a specific patch…	None	M (0.5)	M (50)	M (25)

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

STEP 4: Countermeasures

- Formal establishment of actions based on the risk assessment towards risk mitigation
  - Effectiveness and costs

Risk Level	Countermeasures
High	Strong need for measures to put in place ASAP
Medium	Plan developed within reasonable period of time
Low	Can we accept the risk and do nothing?

Examples applied to CERN functions

- Assets: CERN facilities
  - Examples applied to: EDH, CERN Service Desk
- Criticalities: (defined as impact of application lost)

Criticality	Description	Factor	Levels
Minor	nil	1	Very few people affected; < 1KCHF
	Hardly visible	2	Several people affected; < 5KCHF
	Very limited	3	Small group affected; < 10KCHF
Average	Limited	4	People affected > 20; cost < 20KCHF
	Visible	5	People affected > 50; cost < 50 KCHF
	Significant	6	People affected > 100; cost < 100 KCHF
Major	Very important	7	People affected > 150; cost < 400 KCHF
	Important	8	People affected > 500; cost < 1MCHF
Critical	Disastrous	9	People affected > 1000; cost < 10MCHF
	Catastrophic	10	People affected > 1000, > 10MCHF, life danger

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Examples applied to CERN functions

- Threats/Vulnerabilities
- Likelihood Calculations and mitigation plans

Common Threat-Sources
Natural Threats – Floods, electrical storms, etc
Human Threats – network attacks, errors, malicious sw upload, etc
Environment Threats – pollution, long-term power failure, etc

Likelihood	Factor
No (once > 10 years)	Impossible → 1
	Almost impossible → 2
	Very unlikely → 3
Maybe (once in 5-10 years)	Unlikely → 4
	Little plausible → 5
	Plausible → 6
	Likely → 7
Yes (once < year)	Very likely → 8
	Almost certain → 9
	Certain → 10

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Examples applied to CERN functions

- Final calculation of risk and recommendations:

Threat x Vulnerability = Probability

Probability x Impact = RISK

Threats	Loss of data: 5		Viruses: 5		Hacking: 8		Strike: 7	
Assets	V	Risk	V	Risk	V	Risk	V	Risk
EDH	4	180	3	135	4	288	4	252
Service Desk	4	180	2	90	4	288	4	252

Mitigation plans over Risk > 200

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it

Summary and Plans

- Risk Management is a crucial process to ensure the continuity of the services and the business
  - Formal approach in needed for consistency, scalability and predictability
- In the Service Management project, we have established some of the fundamental processes that will supply necessary inputs:
  - **Service Catalogue**, INC Mgt, Change Mgt and SLM (ongoing)
- Establishment of the process foreseen in 2012 following a formal ITIL approach that will require the involvement of both Service Owners and Users

Your feedback and knowledge will be crucial to ensure a continuity plan for all our services

CERN IT Department
CH-1211 Genève 23
Switzerland
www.cern.ch/it