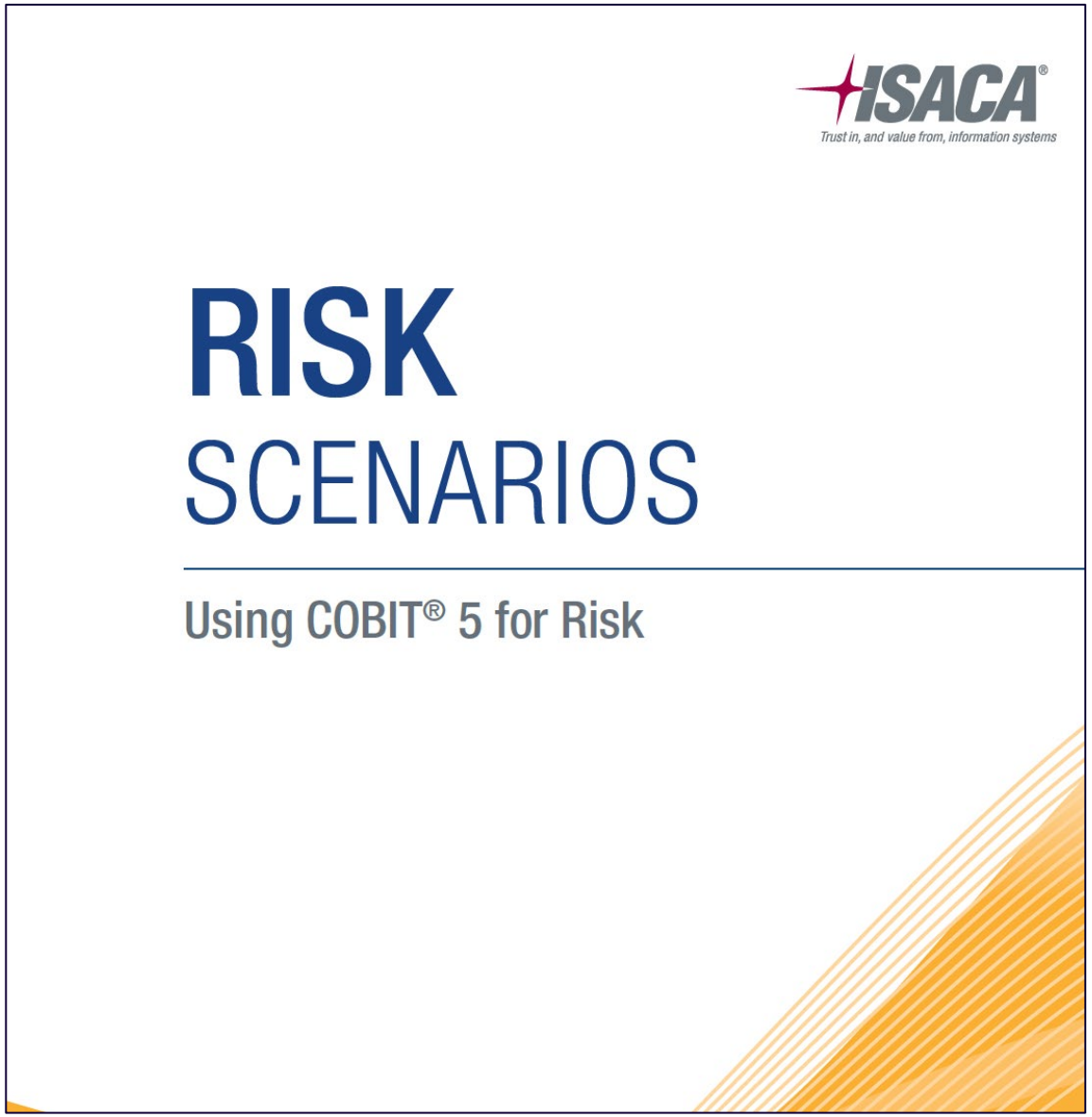
Sikt

Risk scenarios

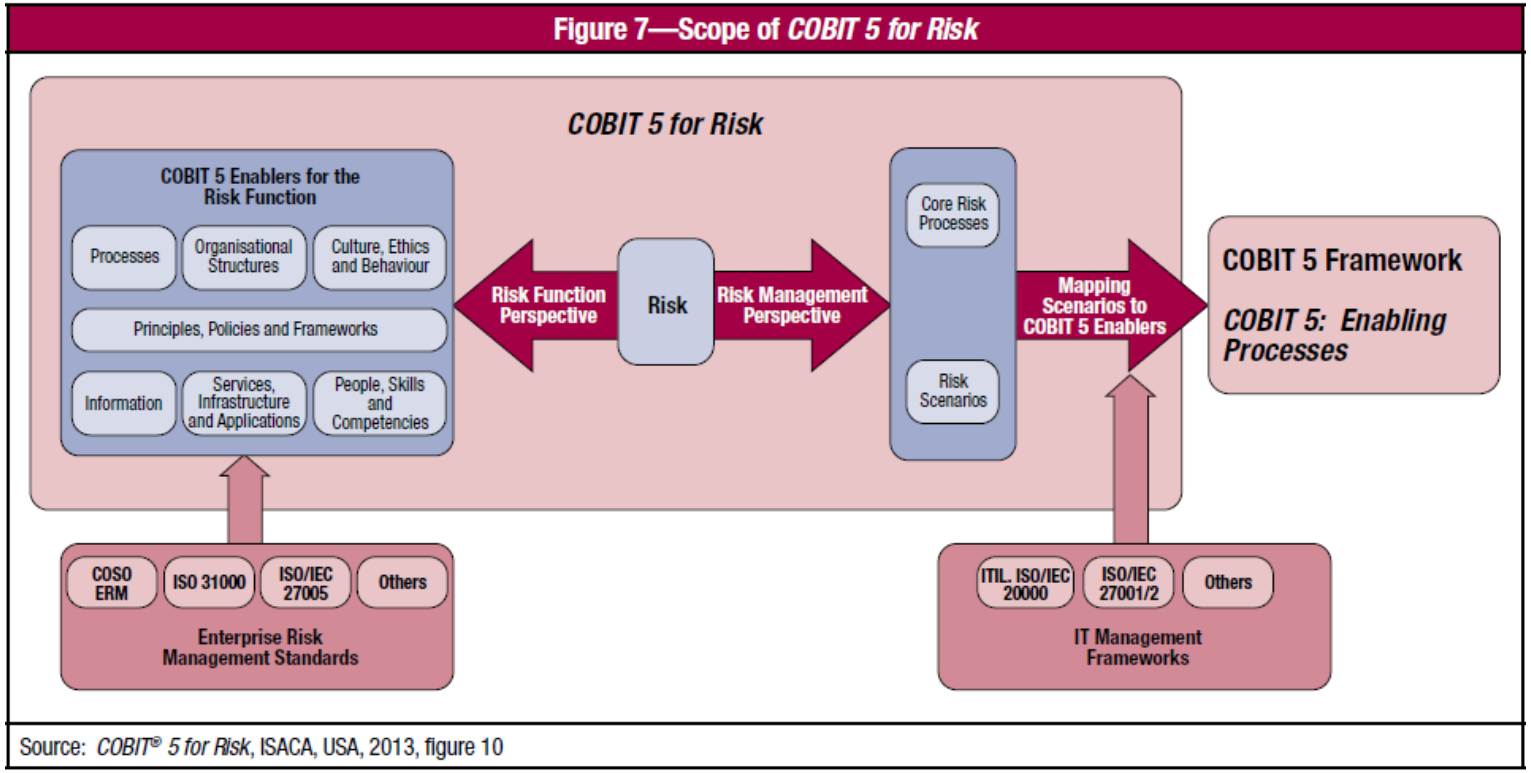
Rolf Sture Normann
Sikt - Norwegian Agency for Shared Services in Education and Research

Sikt


ISACA
Trust in, and value from, information systems
RISK
SCENARIOS
Using COBIT® 5 for Risk

Scope of Cobit 5 for risk

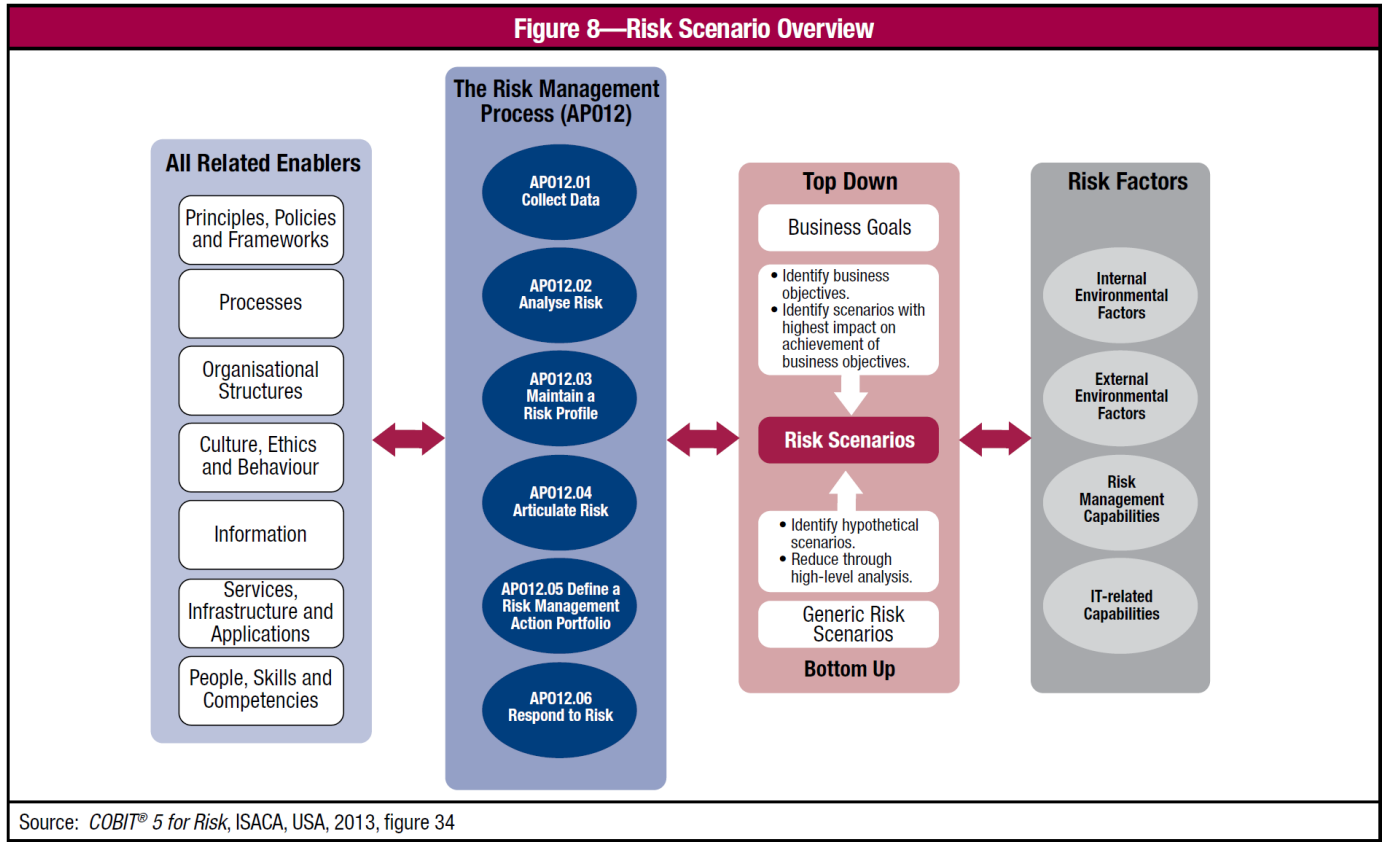
- Risk function
  - What is needed to build and sustain effective core risk governance and management activities
- Risk management
  - How the core risk management process of identifying, analysing, responding to and report on risk can be assisted by the Cobit 5 enablers



Sikt

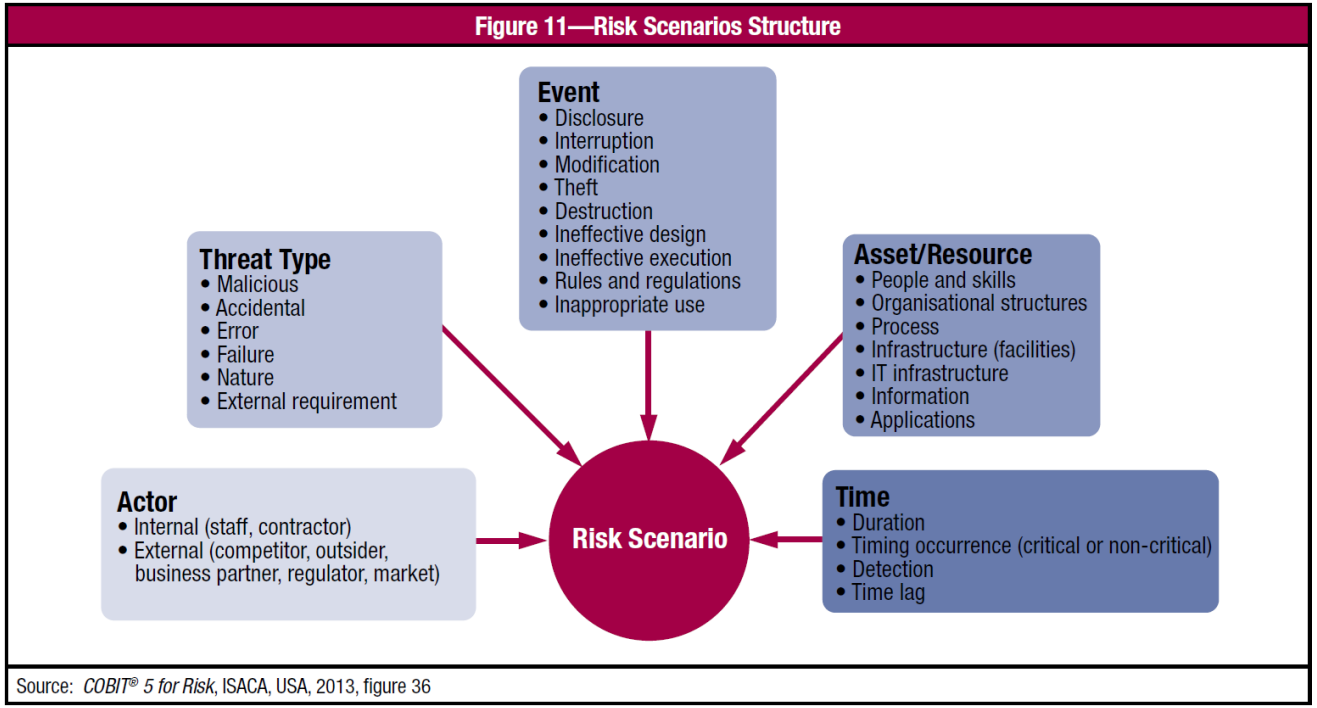
A key information for the Cobit 5 core risk management process (APO12) is risk scenarios

- Top-down approach
- Bottom-up approach
- Enablers
- Risk management process
- Risk factors



Sikt

- **Actor** —Who generates the threat that exploits a vulnerability?
- **Threat type** (the nature of the event)—Is it malicious? If not, is it accidental or is it a failure of a well-defined process? Is it a natural event?
- **Event**—Is it disclosure of confidential information, interruption of a system or of a project, theft or destruction?
- **Asset/resource** —On which the scenario acts. An asset is any item of value to the enterprise that can be affected by the event and lead to business impact.
- **Time**—Dimension, where the following could be described, if relevant to the scenario: – The duration of the event, e.g., extended outage of a service or data centre



Sikt

Characeristics of good scenarios

Figure 13—Characteristics of Good Risk Scenarios	
Characteristic	**Explanation**
Relevance for decision	Scenarios should deliver meaningful information to support decisions. Generic (market or industry) scenarios are usually not adequate enough and need to be augmented.
Consistency	Each scenario has to be compelling by itself. If it is not, the credibility of a scenario can be negatively affected.
Plausibility	Scenarios need to be realistic. They must meet principal requirements of basic feasibility.
Likelihood	Each scenario should, to a certain extent, be likely to occur.
Timely	Scenarios must reflect current events and circumstances.

Sikt

Generic risk scenarios

Figure 14—Example Risk Scenarios

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0101	Portfolio establishment and maintenance	P	P	S	Wrong programmes are selected for implementation and are misaligned with corporate strategy and priorities.	Programmes lead to successful new business initiatives selected for execution.
0102		P	P	S	There is duplication between initiatives.	Aligned initiatives have streamlined interfaces.
0103		P	P	S	A new important programme creates long-term incompatibility with the enterprise architecture.	New programmes are assessed for compatibility with existing architecture.
0104		P	P	S	Competing resources are allocated and managed inefficiently and are misaligned to business priorities.	

Sikt

Risk scenario categories

- Portfolio establishment and maintenance
- Programme/projects life cycle management
- IT investment decision making
- IT expertise and skills
- Staff operations
- Information
- Architecture
- Infrastructure
- Software
- Business ownership of IT
- Supplier
- Regulatory compliance
- Geopolitical
- Infrastructure theft or destruction
- Malware
- Logical attacks
- Industrial action
- Environmental
- Acts of nature
- Innovation

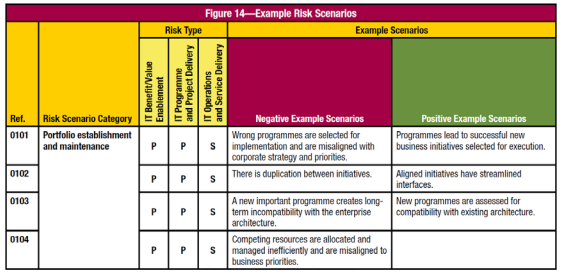


Figure 14—Example Risk Scenarios

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0101	Portfolio establishment and maintenance	P	P	S	Wrong programmes are selected for implementation and are misaligned with corporate strategy and priorities.	Programmes lead to successful new business initiatives selected for execution.
0102		P	P	S	There is duplication between initiatives.	Aligned initiatives have streamlined interfaces.
0103		P	P	S	A new important programme creates long-term incompatibility with the enterprise architecture.	New programmes are assessed for compatibility with existing architecture.
0104		P	P	S	Competing resources are allocated and managed inefficiently and are misaligned to business priorities.	

Sikt

Figure 14—Example Risk Scenarios

Ref.	Risk Scenario Category	Risk Type: IT Benefit/Value Enablement	Risk Type: IT Programme and Project Delivery	Risk Type: IT Operations and Service Delivery	Example Scenarios: Negative Example Scenarios	Example Scenarios: Positive Example Scenarios
0101	**Portfolio establishment and maintenance**	P	P	S	Wrong programmes are selected for implementation and are misaligned with corporate strategy and priorities.	Programmes lead to successful new business initiatives selected for execution.
0102		P	P	S	There is duplication between initiatives.	Aligned initiatives have streamlined interfaces.
0103		P	P	S	A new important programme creates long-term incompatibility with the enterprise architecture.	New programmes are assessed for compatibility with existing architecture.
0104		P	P	S	Competing resources are allocated and managed inefficiently and are misaligned to business priorities.	

Risk type

- IT benefit/value enablement risk
  - Associated with (missed) opportunities to use technology to improve the efficiency or effectiveness of business processes or as an enabler for new business initiatives
- IT programme and project delivery risk
  - Associated with the contribution of IT to new or improved business solutions, usually in the form of projects and programs
- IT operations and service delivery risk
  - Associated with the operational stability, availability, protection and recoverability of IT services, which can bring destruction or reduction of value to the enterprise

Sikt

Figure 14—Example Risk Scenarios

Ref.	Risk Scenario Category	Risk Type: IT Benefit/Value Enablement	Risk Type: IT Programme and Project Delivery	Risk Type: IT Operations and Service Delivery	Example Scenarios: Negative Example Scenarios	Example Scenarios: Positive Example Scenarios
0101	**Portfolio establishment and maintenance**	P	P	S	Wrong programmes are selected for implementation and are misaligned with corporate strategy and priorities.	Programmes lead to successful new business initiatives selected for execution.
0102		P	P	S	There is duplication between initiatives.	Aligned initiatives have streamlined interfaces.
0103		P	P	S	A new important programme creates long-term incompatibility with the enterprise architecture.	New programmes are assessed for compatibility with existing architecture.
0104		P	P	S	Competing resources are allocated and managed inefficiently and are misaligned to business priorities.	

Risk scenario outcome

- Positive outcomes are scenarios that can result in value creation or preservation.

- Negative outcomes are scenarios that can result in value destruction or failure to gain.

Sikt

Generic risk scenarios – example 2

Figure 14—Example Risk Scenarios *(cont.)*

Ref.	Risk Scenario Category	Risk Type			Example Scenarios	
		IT Benefit/Value Enablement	IT Programme and Project Delivery	IT Operations and Service Delivery	Negative Example Scenarios	Positive Example Scenarios
0801	Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)	P	S	P	New (innovative) infrastructure is installed and as a result systems become unstable leading to operational incidents, e.g., Bring your own device (BYOD) programme.	Appropriate testing is conducted before setting infrastructure into the production environment to ensure the availability and proper functioning of the entire system.
0802		P	S	P	The systems cannot handle transaction volumes when user volumes increase.	
0803		P	S	P	The systems cannot handle system load when new applications or initiatives are deployed.	
0804		P	S	P	Intermittently, there are failures of utilities (telecom, electricity).	Second line utilities are foreseen and stand by 24/7 to support the continuous execution of business critical transactions.
0805		P	S	P	The IT in use is obsolete and cannot satisfy new business requirements (networking, security, database, storage, etc.).	IT is an innovator, ensuring a two-way interaction between business and IT.
0806				P	Hardware fails due to overheating.	

Using Cobit 5 enablers to mitigate risk scenarios

Risk Scenario Category 8: Infrastructure		
Risk Scenario Category	Infrastructure Scope: Hardware, operating system and controlling technology; selection/implementation, operations and decommissioning	
Principles, Policies and Frameworks Enabler		
Reference	**Contribution to Response**	
Architecture principles	Define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise.	
Change management policy	Define the rules and guidelines to change infrastructure components in a controlled and safe way.	
Process Enabler		
Reference	**Title**	**Governance and Management Practices**
APO02.03	Define the target IT capabilities.	Define the target business and IT capabilities and required IT services. This should be based on the understanding of the enterprise environment and requirements; the assessment of the current business process and IT environment and issues; and consideration of reference standards, best practices and validated emerging technologies or innovation proposals.
APO04.03	Monitor and scan the technology	Perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (e.g., by realizing the enterprise strategy, optimizing

Organisational Structures Enabler	
Reference	**Contribution to Response**
Head of IT operations	Accountable for the proper management and maintenance of the IT infrastructure
Head of architecture	Designing architecture in an optimal way
Culture, Ethics and Behaviour Enabler	
Reference	**Contribution to Response**
Respect the available assets	All staff is required to maintain the assets in an appropriate manner

Information Enabler	
Reference	**Contribution to Response**
Architecture model	Target architecture model
(Updates to) asset inventory	Tracking all assets throughout the enterprise

Services, Infrastructure and Applications Enabler	
Reference	**Contribution to Response**
Configuration management database (CMDB)	Assists in identifying areas for improvement.
People, Skills and Competencies Enabler	
Reference	**Contribution to Response**
Architecture skills	Develop efficient and effective architecture aligned to the business requirements.
Technical skills	Managing the different infrastructure components

Sikt

Examples of risk scenario analysis

08 Infrastructure

0802 System not scalable to meet business growth

Risk Scenario Title	System not scalable to meet business growth
Risk Scenario Category	08 Infrastructure
Risk Scenario Reference	0802
Risk Scenario A small offline trading enterprise operates an online shop, is increasing its customer base and invests heavily in marketing initiatives. All IT equipment is procured by shop personnel who do not have the appropriate technical skills to apply best practices and vendor usage recommendations. The IT infrastructure was stable and available in the past, but when the user base and usage of the system increase, the system availability significantly drops, compromising the service level needed for this vertical market.	
Risk Scenario Components	
Threat Type The nature of the event is in the inappropriate design of the infrastructure caused by **accident/error.**	
Actor The actor that generates the threat that exploits a vulnerability is **internal**—the shop owner (chief executive officer [CEO]).	
Event The event is **interruption** caused by a significant drop of system availability and **ineffective design** of the infrastructure.	
Asset/Resource (Cause) The resources that lead to the business impact are the **process** BAI04 *Manage availability and capacity* and the **IT infrastructure** servers that are not capable of meeting the rising demand.	
Asset/Resource (Effect) The resources affected are business **processes** such as the sales process (online shop), which are often not available, and **applications** because the online shop is not regularly available.	
Time The duration of the event is **extended** because as it needs a long period of time to upgrade or replace the infrastructure. The online shop is not regularly available, so business is missed. Therefore, the timing of occurrence is **critical**. Because the online shop is not available, the detection is **instant**. Because there is momentarily no business, the consequence is **immediate**.	
Risk Type	
IT Benefit/Value Enablement	**P** — Online sales are not available, resulting in lost business.
IT Programme and Project Delivery	**N/A**
IT Operations and Service Delivery	**P** — IT service interruptions
Possible Risk Responses	
• **Risk Avoidance:** Not offering an online shop • **Risk Acceptance:** The shop owner accepts the lost business. • **Risk Sharing/Transfer:** Outsourcing of the IT service and agreed-on service level agreement (SLA) availability with appropriate penalties • **Risk Mitigation:** Outsourcing of the IT service and agreed-on SLA availability. Upgrade of the existing system to increase the IT capability	
Risk Mitigation Using COBIT 5 Enablers	
Principles, Policies and Framework Enabler	

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
Architecture principles	Define the underlying general rules and guidelines for the use and deployment of all IT resources and assets across the enterprise.	Medium	Medium	NO
Change Management policy	Define the rules and guidelines to change infrastructure components in a controlled and safe way.	Medium	Medium	NO

Process Enabler

Reference	Title Description	Effect on Frequency	Effect on Impact	Essential Control	Essential Control
APO02.01	Understand enterprise direction.	Consider the current enterprise environment and business processes as well as the enterprise strategy and future objectives. Consider also the external environment of the enterprise (industry drivers, relevant regulations, basis for competition).	High	High	YES
APO02.02	Assess the current environment, capabilities and performance.	Assess the performance of current internal business and IT capabilities and external IT services, and develop an understanding of the enterprise architecture in relation to IT. Identify issues currently being experienced and develop recommendations in areas that could benefit from improvement. Consider service provider differentiators and options and the financial impact and potential costs and benefits of using external services.	High	High	YES
BAI04.01	Assess current availability, performance and capacity and create a baseline	Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver	Low	High	YES

Organisational Structures Enabler

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
Head of IT operations	Accountable for the proper management and maintenance of the IT infrastructure	Low	Low	NO
Head of architecture	Design architecture in an optimal way.	Medium	Medium	NO

Culture, Ethics and Behaviour Enabler

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
N/A	N/A			

Information Enabler

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
Architecture model	Target architecture model	High	High	YES
Configuration status reports	Track changes to configuration.	Medium	Medium	NO

Services, Infrastructure and Applications Enabler

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
Configuration management database (CMDB)	Assists in identifying areas for improvement	High	High	YES

People, Skills and Competencies Enabler

Reference	Contribution to Response	Effect on Frequency	Effect on Impact	Essential Control
Architecture skills	Develop efficient and effective architecture aligned to the business requirements.	High	High	YES

Sikt

Practical approach to develop risk scenarios

1) Use a lis of example generic risk scenarios to define an initial set of concrete risk scenarios for the organisation
2) Perform a validation against the business objectives for the organisation
3) Refine the selected scenarios based on the validation; categorise them to a level in line with the criticality of the organisation
4) Reduce the number of scenarios to a manageable set
5) Keep all risk in a list so they can be reevaluated in the next iteration and included for detailed analysis if they became relevant
6) Include unspecified event in the scenarios to address incidents that are not covered by the spesific generic scenarios

Sikt

Should we look more into building risk scenarios (my opinion)?

- Descision makers wil more likely understand the risk
- Give the management an idea of what is the positive outcome of doing things right
- Bring knowledge to what controls have effekt on the elements of risk level (likelihood and consequence)
- Risk scenario examples will give you new ideas on risk area
- Should only be used in the big picture, not when assessing risk for a spesific system or process (overarching level)
- It is time consuming