ISACA®

Getting Started With Risk Scenarios

Risk

CONTENTS

Introduction

Risk scenarios facilitate communication in risk management by constructing a narrative that can inspire people to act. The use of risk scenarios can enhance the risk management effort by helping the risk team understand and explain risk to business process owners and other stakeholders. Additionally, a well-developed scenario provides a realistic and practical view of risk that is more aligned with business objectives, historical events and emerging threats forecasted by the organization than would be found by consulting a broadly applicable standard or catalog of controls. These benefits make risk scenarios valuable as a means of gathering and framing information used in subsequent steps in the risk management process.

One of the challenges for information and technology (I&T) risk management is to identify the important and relevant risk among everything that can possibly go wrong with I&T or in relation to I&T, given the pervasive presence of I&T and the organization's dependence on it. One of the techniques to overcome this challenge is the development and use of risk scenarios. It is a core approach that brings realism, insight, organizational engagement, improved analysis and structure to the complex matter of I&T risk. Once scenarios are developed, they are used during the risk analysis phase, in which frequency and business impacts are estimated.

ISACA has issued sample risk scenarios to illustrate what a risk scenario looks like in practice. These scenarios are in a convenient Microsoft® Word format to allow practitioners to tailor them to their specific enterprise contexts. This introductory document explains the format of the scenario templates and how to use them.

Getting Started with Risk Scenarios

To use the risk scenario templates, users simply download the zip files (of which this file is a part) and extract the file(s) they want to explore. Files can be saved locally and edited to tailor them to a specific enterprise context. As an enterprise embarks on its risk journey, there are many ISACA resources that can help:

- ***Risk IT Framework, 2nd Edition***[1]—Introduces information and technology risk and contains a brief discussion of risk scenarios and how those can be used as part of a larger enterprise I&T program.
- ***Risk IT Practitioner Guide, 2nd Edition***[2]—Contains a robust discussion of risk scenarios, and the templates included in this toolkit are based on this publication.
- ***IT Risk Starter Kit***[3]—Contains a number of risk-related templates which practitioners can use to build up a risk practice within an enterprise.
- ***ISACA® Journal***[4]—Publishes a multitude of articles related to IT risk.
- **ISACA online forum on risk management**[5]—Participants can share information and ask questions of their peers.
- **ISACA web page**[6] for risk-related topics and resources.

[1] ISACA, *Risk IT Framework, 2nd Edition*, USA, 2020, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9WEAS
[2] ISACA, *Risk IT Practitioner Guide, 2nd Edition*, USA, 2020, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko54EAC
[3] ISACA, *IT Risk Starter Kit*, USA, 2022, https://store.isaca.org/s/store#/store/browse/detail/a2S4w000005EgZbEAK
[4] See https://www.isaca.org/en/resources/isaca-journal.
[5] See https://engage.isaca.org/communities/onlineforums.
[6] See https://www.isaca.org/en/resources/it-risk.

Navigating the Risk Scenario Template

The subject of each scenario can be found in the file name as well as in the title of the scenario itself. Each Word file contains five sections, labeled A to E.

Risk Scenario Template Section A

There are six rows in section A. **Figure 1** describes each of the rows and its purpose.

FIGURE 1: Risk Scenario Template Section A

Row	Description
Risk scenario title	The risk scenario title is a brief but concise description of the risk scenario.
Risk type	The risk type row identifies the process impacted by the risk. These types are ISACA proprietary risk groups. See **figure 2** for more details.
Risk scenario category	The risk scenario category delves deeper into the selected risk type and identifies the business function impacted by the specific risk scenario. See **figure 3** for more details. Theses can also be found in **figure 6.2** of ISACA's *Risk IT Practitioner Guide*.
Risk scenario reference	The risk scenario reference identifies the risk category and the generic scenario. The categories and generic scenarios can be found in ISACA's *Risk IT Practitioner Guide*.
Risk statement	Aligns with the specific risk scenario within the category in **figure 6.2** of ISACA's *Risk IT Practitioner Guide*.
Risk owner and risk oversight	Risk owner: The person (role) in whom the organization has invested the authority and are accountability for making risk-based decisions and who owns the loss associated with a realized risk scenario. Risk oversight: The person (role) who is responsible for risk assessments, monitoring, documenting risk response and establishing KRIs. These can be found in figure 4.2 of ISACA's *Risk IT Framework*.

One approach to risk management is to identify processes or systems that may have areas that are not operating effectively and/or efficiently that could put the enterprise at risk.

ISACA has identified six risk types to identify major processes that may have risk (**figure 2**).

FIGURE 2: Risk Types

ID	Risk Type Definition
1	**Product delivery**—Technology is not sufficient to deliver new products and services to meet business demands.
2	**Service quality**—Inability to service expectations due to technology/data disruptions, failures, degradation, corruption or loss.[7]
3	**Data and system protection**—Damages, disruptions or losses due to misuse of data, technology or associated business processes.
4	**Legal and regulatory compliance**—Insufficient compliance oversight, monitoring and supervision could irreparably damage long-term relationships with regulators and result in regulatory actions, including public sanctions, penalties, delays to new service offerings or avoidable remediation investment.
5	**Workplace safety**—Work environment that is unsafe from a physical facility perspective, psychological perspective (i.e., abusive) or personal safety perspective (i.e., physical violence is present) that could result in financial, regulatory or reputational impact.
6	**Product and service cost**—Inability to deliver IT products and services at a reasonable cost.

[7] Note that 1 and 2 are not orthogonal—i.e., they overlap. Service levels could be a valid business requirement.

When risk scenarios are categorized (**figure 3**), it facilitates the identification of various attributes such as the risk owner and oversight, areas of impact that will ultimately help assess the identified risk.

This is not an exhaustive list of risk categories. Users should feel free to use these or their own categories tailored to their enterprises.

FIGURE 3: Risk Categories

ID	Risk Category Description
1	IT investment decision making, portfolio definition and maintenance: Inability to make the correct IT investments in competitive IT product and service portfolio.
2	Program and projects life cycle management: Inability to execute programs and projects on time, within budget and per requirements.
3	IT cost and oversight: Inability to provide IT services within agreed and reasonable resource limitations.
4	IT expertise, skills and behavior: Inability to recruit and maintain adequate IT staffing levels to support business needs**.**
5	Enterprise/IT architecture: Inability to select, develop, acquire and implement IT systems that integrate with enterprise architecture.
6	IT operations: Inability to provide reliable IT services because of operational IT mishaps.
7	User access rights management: Inability to protect systems from malicious or inadvertent system compromise, misuse or loss.
8	Software adoption and use: Inability of business processes to benefit from newly developed products and services.
9	IT hardware: Inability to continually support and maintain technology systems (including aging and legacy systems) that are supporting business processes.
10	Internal and external security threats (hacker, malware, etc.): Malicious access to and compromise or misuse of technology systems impacting the confidentiality, integrity or availability of technology systems and business information.
11	Third-party/supplier incidents: Inability to meet service level requirements because of failure of third-party suppliers.
12	Noncompliance: Inability to comply with policies, standards, laws and regulations related to technology.
13	Geopolitical issues: Inability to protect against geopolitical issues, such as actions in/by foreign countries.
14	Industrial action: Inability to provide IT services because of industrial action of employees or service providers.
15	Acts of nature: Natural or man-made disasters affecting critical resources.
16	Emerging technologies and innovation: Inability to leverage new technologies to support innovative processes and products.
17	Environmental: Inability to deliver IT services in an environmentally friendly manner or in line with environmental regulations.
18	Data and information management: Inability to achieve and preserve adequate data and information quality and protection.
19	Disastrous events: Events that might threaten employee safety or result in the destruction/theft of physical assets.

Risk Scenario Template Section B

This section covers several attributes needed to assess and respond to risk (**figure 4**). These elements will help determine the criticality of the risk and the appropriate response, both of which are essential components of the risk management process.

FIGURE 4: Risk Scenario Template Section B

Attribute	Definition
Actor/threat community	This field lists the threat actor(s) applicable to the particular scenario. The threat actor acts against an enterprise's asset. Keep in mind that there is a dependency on the asset—not all actors have the means or motivation to act against all assets. Some threat actors are: • Cybercriminals • Hacktivists • Untrained/accidental insiders • Malicious insiders • Acts of nature
Intent/motivation	This row includes one to two sentences that describe the threat actor's intent and motivation behind the loss event. Generally, the threat actor is a company insider and the event is accidental, the description centers around how such an event may occur. If the actor is malicious, the row describes how and why the actor may act against the assets and resources. If the actor is an act of nature, the field explains how the particular event leads to a loss (e.g., high winds cause a power outage, leading to data center downtime).
Threat event	This section includes one to two sentences that describe how, when and where the threat actor acts against the asset. For example, this can include a narrative of how an accident can happen, methods and sequence of events during a cyberattack, or how an act of nature may cause outages.

FIGURE 4: Risk Scenario Template Section B (*cont.*)

Attribute	Definition
Assets/resources	This field describes the thing of value that is under consideration in the risk scenario. The asset can be tangible (hardware) or intangible (reputation). There can be more than one asset under consideration.
Consequence	This section includes one to two sentences that describe the effect or result of the adverse outcome if the loss event occurs.
Impact dimensions	There are six potential impact dimensions:[8] • Productivity • Cost of response • Replacement cost • Competitive advantage • Reputation • Fines and judgments A checkbox appears for each form of loss that is relevant to the scenario. Additionally, for each applicable form of loss, there is a short description of how the overall loss event results in the form of loss.
Timing	This field includes a bulleted list of the following: • Any critical time periods (e.g., month end) in which the loss event would be especially impactful • Any knowable time lags—period of time between the event occurring and discovery and how it affects losses • Description of anything that could aid or hinder the detection of the event

Risk Scenario Template Section C

When scoping and analyzing a risk scenario, it is important to identify the extent or scale upfront. For example, one might want to assess the typical scenario and not worry about extreme cases. Or someone might want to focus entirely on the worst case (or tail risk). Another might want to analyze multiple versions ranging from best to worst cases. Regardless of the focus, making this choice upfront and clearly communicating it to anyone involved in the analysis of (or providing input to) the scenario are critical to the process. It is also important to make this choice clear in any reports relied on by management and any decisionmakers.

Section C details the worst, typical and best-case scenarios, along with assumptions (**figure 5**).

FIGURE 5: Risk Scenario Template Section C

Severity	Description
Extent of scenario: Worst case	Includes one to two sentences that describe the attributes of a worst-case version of this scenario. This might also be referred to as an outlier, extreme but plausible, or tail risk. If you are measuring the potential outcomes as a distribution of potential loss, this could be a magnitude that falls in the 98th or 99th percentile. Often this describes the lowest frequency/probability and the highest impact version of the scenario.
Extent of scenario: Typical or most likely case	This field includes one to two sentences that describe the attributes of a typical or most likely version of the scenario. Often this describes the most frequent or likely version of the scenario.
Extent of scenario: Best case	This field describes the attributes of a best-case version of this scenario. Often this describes the version of the scenario with the least probable impact. There is still some loss, but the event progresses as favorably as can be expected.
Assumptions	This row in section C of the risk scenario template captures the various aspects of the scenario being assumed during scenario scoping and analysis. For example, a type of actor or target asset might be excluded from the scope, a certain time frame for the event is assumed, or the scenario is analyzed in the context of a particular version of a regulation. Anything relevant to the scoping that has not already been captured in another section of this template should be listed here. This serves as a reference during the analysis process, but also as an artifact after analysis is complete to help someone better trace the analysis or audit the process.

[8] The impact dimensions are based on the FAIR™ Institute's six forms of loss. See Suarez, T.; "A Crash Course on Capturing Loss Magnitude with the FAIR Model," 20 October 2017, https://www.fairinstitute.org/blog/a-crash-course-on-capturing-loss-magnitude-with-the-fair-model#:~:text=In%20the%20FAIR%20model%20for,everything%20seems%20simple%20and%20straightforward.

Risk Scenario Template Section D

Typically, IT risks can be mitigated by a large number of controls.

To create a readable and maintainable risk register, ISACA suggests identifying a reasonable number of the most important controls and, where necessary, aggregating them.

In section D (**figure 6**), these most important controls relating to the risk can be listed. The controls provided all come from COBIT®[9] but other sources of controls can be entered by the user.

For each control, the following information is entered:

FIGURE 6: Risk Scenario Template Section D

ID	Control Attribute	Description
2	Control description	This field includes a full description of the control and its anticipated (or observed) effect on the risk.
3	Control type	Controls can be classified into different types; such a classification can help assess whether the applied range of controls is sufficiently holistic—for example, not all controls are focused on policies. Many classifications are possible, including: • The governance system component types of COBIT, which distinguish among process practices, organizational structures, information flows (reporting), culture and behavior, skills, policies, applications and infrastructure • Preventive/detective/corrective controls • Any internal classification system an enterprise has developed
4	Effect on impact	The estimated effect that this control has on impact. The effect is expressed as a qualitative indicator, with possible values of Yes/No. It is recommended that an enterprise's risk management practices include some guidance on the thresholds for these qualitative values to ensure consistency across the IT risk register.
5	Effect on frequency	The estimated effect that this control has on frequency. The effect is expressed as a qualitative indicator, with possible values of Yes/No. It is recommended that an enterprise's risk management practices include some guidance on the thresholds for these qualitative values to ensure consistency across the IT risk register.
6	Essential control	Some controls are more important than others, and these are typically labeled essential controls. In this field, a Yes/No value should be entered.
7	Reference	This field is for a reference to the control. References can be anything that helps the user better understand or better position the control. Possible references can include: • A reference to a particular governance or management objective in the COBIT framework, or a process practice or activity contained therein that explains the control in more detail. • A reference to another relevant standard or framework where the control is sourced from or where it is better explained. • A reference to a control in an enterprise's own control catalog.

Risk Scenario Template Section E

In this section, the user can define a set of key risk indicators (KRIs) (**figure 7**).

Any measurement that can be used to describe and track a risk is an indicator of that risk. Risk indicators are specific to each enterprise. Development and selection of KRIs depend on a number of parameters in the internal and external environment, such as the size and complexity of the enterprise, whether it is operating in a highly regulated market and its strategic objectives.

[9] ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, 2018, https://store.isaca.org/s/#/store/browse/detail/a2S4w000004Ko9ZEAS

For each KRI, the following information can be entered:

FIGURE 7: Risk Scenario Template Section E

ID	KRI Attribute	Description
2	Indicator	Describes KRI, best expressed as a measurable element of information
3	KRI description	Describes source for KRI: • Who will be responsible for providing the KRI information? • In which form will the data be collected (automated or manually)? • What is the frequency by which the data will be collected?
4	Lag/lead	Indicates whether KRI reflects: • Actual occurrence of the risk (lagging indicator) • Potential increased likelihood or impact of the risk, typically because of control deficiencies or important context changes (leading indicator) It is recommended that a mix of leading and lagging indicators be defined.

Acknowledgments

ISACA would like to recognize:

Board of Directors

Pamela Nigro, Chair
CISA, CGEIT, CRISC, CDPSE, CRMA
Vice President, Security, Medecision, USA

John De Santis, Vice-Chair
Former Chairman and Chief Executive Officer, HyTrust, Inc., USA

Niel Harper
CISA, CRISC, CDPSE, CISSP
Chief Information Security Officer, Data Privacy Officer, Doodle GmbH, Germany

Gabriela Hernandez-Cardoso
Independent Board Member, Mexico

Maureen O'Connell
NACD-DC
Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA

Veronica Rose
CISA, CDPSE
Senior Information Systems Auditor–Advisory Consulting, KPMG Uganda, Founder, Encrypt Africa, Kenya

David Samuelson
Chief Executive Officer, ISACA, USA

Gerrard Schmid
Former President and Chief Executive Officer, Diebold Nixdorf, USA

Bjorn R. Watne
CISA, CISM, CGEIT, CRISC, CDPSE, CISSP-ISSMP
Senior Vice President and Chief Security Officer, Telenor Group, USA

Asaf Weisberg
CISA, CISM, CGEIT, CRISC, CDPSE, CSX-P
Chief Executive Officer, introSight Ltd., Israel

Gregory Touhill
CISM, CISSP
ISACA Board Chair, 2021-2022
Director, CERT Center, Carnegie Mellon University, USA

Tracey Dedrick
ISACA Board Chair, 2020-2021
Former Chief Risk Officer, Hudson City Bancorp, USA

Brennan P. Baybeck
CISA, CISM, CRISC, CISSP
ISACA Board Chair, 2019-2020
Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA

Rob Clyde
CISM, NACD-DC
ISACA Board Chair, 2018-2019
Independent Director, Titus, Executive Chair, White Cloud Security, Managing Director, Clyde Consulting LLC, USA

About ISACA

For more than 50 years, ISACA® (www.isaca.org) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams that effectively drive IT audit, risk management and security priorities forward. ISACA is a global professional association and learning organization that leverages the expertise of more than 150,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide. In 2020, ISACA launched One In Tech, a philanthropic foundation that supports IT education and career pathways for under-resourced, under-represented populations.

DISCLAIMER

ISACA has designed and created *Getting Started With Risk Scenarios* (the "Work") primarily as an educational resource for professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

RESERVATION OF RIGHTS

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA

Phone: +1.847.660.5505

Fax: +1.847.253.1755

Support: support.isaca.org

Website: www.isaca.org

Provide Feedback:

www.isaca.org/getting-started-risk-scenarios

Participate in the ISACA Online Forums:
https://engage.isaca.org/onlineforums

Twitter:
www.twitter.com/ISACANews

LinkedIn:
www.linkedin.com/company/isaca

Facebook:
www.facebook.com/ISACAGlobal

Instagram:
www.instagram.com/isacanews/