Risk Assessment Toolkit: The Guidebook

Step-by-Step Guidance for Building a Full Risk Assessment Process

To learn more about this full research or to inquire about membership, contact us:

+1-866-913-8101
IT.Support@executiveboard.com
www.cebglobal.com/IT

CEB Information Risk Leadership Council
A Framework for Member Conversations

The mission of The Corporate Executive Board Company (CEB) and its affiliates is to unlock the potential of organizations and leaders by advancing the science and practice of management. When we bring leaders together, it is crucial that our discussions neither restrict competition nor improperly share inside information. All other conversations are welcomed and encouraged.

Confidentiality and Intellectual Property

These materials have been prepared by CEB for the exclusive and individual use of our member companies. These materials contain valuable confidential and proprietary information belonging to CEB, and they may not be shared with any third party (including independent contractors and consultants) without the prior approval of CEB. CEB retains any and all intellectual property rights in these materials and requires retention of the copyright mark on all pages reproduced.

Legal Caveat

CEB is not able to guarantee the accuracy of the information or analysis contained in these materials. Furthermore, CEB is not engaged in rendering legal, accounting, or any other professional services. CEB specifically disclaims liability for any damages, claims, or losses that may arise from a) any errors or omissions in these materials, whether caused by CEB or its sources, or b) reliance upon any recommendation made by CEB.
# TABLE OF CONTENTS

## INTRODUCTION

- How to Use the Risk Assessment Toolkit • 1
- Terms and Definitions • 2
- Overview of the Risk Assessment Toolkit • 3
- How the Risk Assessment Process Works • 4
- How the Guidebook is Structured • 5

## RISK ASSESSMENT PROCESS STEPS

- Chapter 1: Project Intake • 6
- Chapter 2: Risk Triage • 10
- Chapter 3: Risk Assessment • 16
- Chapter 4: Control Selection • 21
- Chapter 5: Risk Decision • 26
- Chapter 6: Decision Tracking • 30

## APPENDIX

- Technical Details: Risk Triage • 35
- Technical Details: Risk Assessment • 38
- Technical Details: Control Selection • 40
## HOW TO USE THE RISK ASSESSMENT TOOLKIT

The Risk Assessment Toolkit provides step-by-step guidance, tools, and templates to implement a full risk assessment process that uncovers and mitigates business project risks.

### Suggested Use by Role

<table>
<thead>
<tr>
<th>Security Role</th>
<th>Suggested Use</th>
</tr>
</thead>
</table>
| **Head of Security Function**                      | ✓ Read the introduction section of the Risk Assessment Toolkit Guidebook.  
     | ✓ Read each chapter’s executive summary for a high-level understanding of each process step.  
     | ✓ Hand off implementation responsibilities to a security staff member.                                                                        |
| **Security Staff Building the Risk Assessment Process** | ✓ Read the Risk Assessment Toolkit Guidebook to understand how each tool and template works.  
     | ✓ Build the tools and templates into your organization's existing GRC environment or use the native Excel and PDF tools.  
     | ✓ Customize the tools and templates over time to refine the risk assessment process.                                                          |
| **Security Staff Running the Risk Assessment Process** | ✓ Read the introduction section of the Risk Assessment Toolkit.  
     | ✓ Read each chapter’s executive summary and “Run” section to understand how each process step works.                                           |

*We recommend implementing the toolkit’s tools and templates into a GRC tool. This approach automates routine security processes and improves standardization. For more guidance on GRC tools, see these resources: GRC Tools Peer Review Poster, GRC Tool Evaluation Template, and State of GRC Tool Deployments.*
## TERMS AND DEFINITIONS

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project</strong></td>
<td>A planned set of interrelated tasks to be executed over time within cost and other limitations to achieve a defined business goal; oftentimes, the business builds teams around discrete projects.</td>
</tr>
<tr>
<td><strong>Project Owner</strong></td>
<td>The individual in the business or IT who plans and leads the interrelated tasks associated with a project; project owners are the individuals whom the business ultimately holds responsible for delivering the project on time and at cost to achieve the project’s defined business goal.</td>
</tr>
<tr>
<td><strong>Technical Risk</strong></td>
<td>The possibility that a technical vulnerability can be exploited—leading to a data breach—or that a lack of compliance with technical requirements (e.g., from regulatory bodies, governments) can harm the organization.</td>
</tr>
<tr>
<td><strong>Business Risk</strong></td>
<td>The possibility that the business will fail to meet defined goals (in the private sector, this is usually defined in terms of revenue growth or cost savings; government and nonprofit organizations may have a different set of defined goals; business risks include losses, unrealized gains, reputational harm, etc.—in short, anything that impedes the organization’s profitability or pursuit of its goals.</td>
</tr>
<tr>
<td><strong>Control</strong></td>
<td>Any measure (e.g., process, technology tool, training) that, if implemented, helps to identify or reduce risk; together, a group of controls forms a control framework. Note that not all controls apply equally to all projects; rather, each project, based on its risk profile, may require certain controls over others.</td>
</tr>
</tbody>
</table>
OVERVIEW OF THE RISK ASSESSMENT TOOLKIT

Risk Assessment Process Steps

Project Intake → Risk Triage → Risk Assessment → Control Selection → Risk Decision → Decision Tracking

Step-by-Step Implementation Guidance

Risk Assessment Toolkit Guidebook

Supporting Tools and Templates

- Project Intake Form
- Risk Triage and Assessment
- Conversation Guide
- Risk Acceptance Form
- Risk Register

© 2014 CEB. All rights reserved.
HOW THE RISK ASSESSMENT PROCESS WORKS

Project Intake
- Identify business projects and direct them into the risk assessment process.

Risk Triage
- Determine data sensitivity and potential high-level risks.

Risk Assessment
- Identify specific business risks against a formalized control framework.

Control Selection
- Explain identified risks to the project owner and propose mitigating controls.

Risk Decision
- Establish formal business ownership of risks and risk decisions.

Decision Tracking
- Centrally track mitigated and unmitigated risks in a central risk register.

Key Steps
- The project owner completes the project intake form.
- The project owner completes a detailed risk assessment questionnaire that caters to the relevant risk areas identified during risk triage.
- Security reviews the project’s unmitigated risks identified by the risk assessment questionnaire.
- The project owner formally agrees to adhere to all control decisions and accepts responsibility to implement and maintain controls where appropriate.
- Security formally tracks all risk decisions in a central risk register.
- Security uses the risk register to identify risk trends, track exceptions granted, schedule follow-up risk reviews, and create risk metrics.
HOW THE GUIDEBOOK IS STRUCTURED

Each process step has a chapter with the following components:

**Chapter introduction that outlines a defined goal and a description of the process step**

- Review the purpose and goals of each process step.
- Understand how each process step works and what success looks like.

**Detailed guidance on using the tools and templates to set up the process step**

- Set up and customize each process step.
- If desired, build the process step into your existing GRC environment.

**Detailed guidance on using the tools and templates to run the process step**

- Use the tools and templates to run each process step.

**Tips, tricks, and additional research to improve and customize the process step over time**

- Learn tips and tricks to improve the performance of each process step.
- Identify ways to customize and refine each process step over time.
- Consult additional CEB research on conducting best practice risk assessments.
Thank You for Your Interest in CEB Research!

If you’re a member, please log into your account to access the full study.

If you would like access to this full study, please contact CEB to learn more.

Member Login

Contact CEB