ELSEVIER

Security
Executive Council

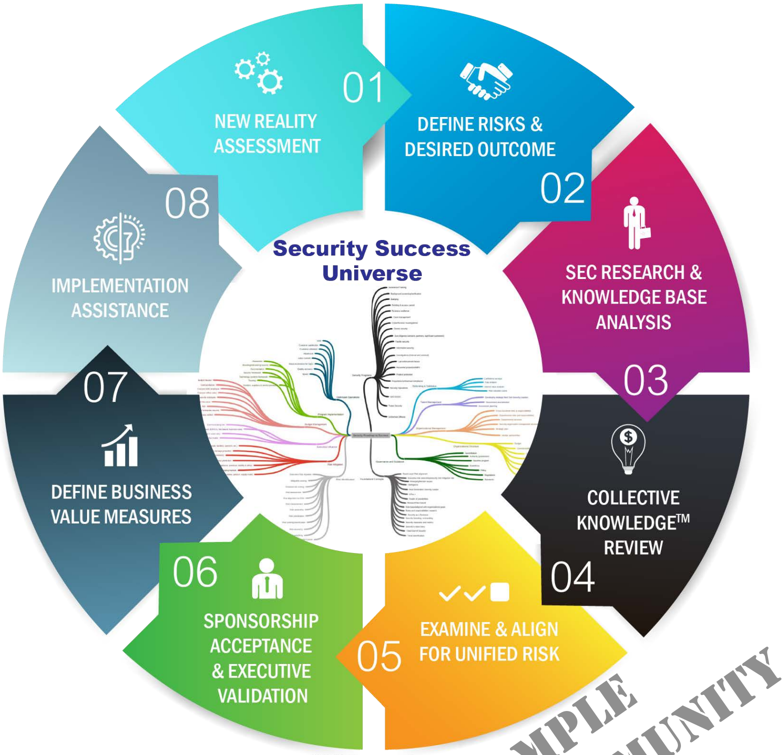
RISK MANAGEMENT PORTFOLIO

Information Protection Playbook

Edited by Greg Kane • Lorna Koppel

THE SEC PROCESS

We walk clients through eight critical steps to reach their goals


01 NEW REALITY ASSESSMENT

02 DEFINE RISKS & DESIRED OUTCOME

03 SEC RESEARCH & KNOWLEDGE BASE ANALYSIS

04 COLLECTIVE KNOWLEDGE™ REVIEW

05 EXAMINE & ALIGN FOR UNIFIED RISK

06 SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION

07 DEFINE BUSINESS VALUE MEASURES

08 IMPLEMENTATION ASSISTANCE

Security Success Universe

01 NEW REALITY ASSESSMENT

The first step is an assessment of your current environment. What needs improving? What are Security's fixed conditions? What recent changes have impacted Security, such as new business directions, new stakeholders, or a merger or acquisition?

DEFINE RISKS & DESIRED OUTCOME 02

An SEC team made up of former CSOs will engage with you to identify the key risks and determine the continuum of desired outcomes depending on your conditions. We map the solution to your C4R – current circumstances, conditions, culture and resources.

SEC RESEARCH & KNOWLEDGE BASE ANALYSIS 03

Once we understand the issues and potential barriers, we search our extensive security knowledge base for resources or research data that can be used as a base or to kickstart direction ideas.

COLLECTIVE KNOWLEDGE™ REVIEW 04

Next, our subject matter experts bring their varied experiences and knowledge together to create a plan to help you reach your desired outcome. We call this Collective Knowledge™.

05 EXAMINE & ALIGN FOR UNIFIED RISK

We help determine which other functions the plan should touch and align with. We use the SEC's Unified Risk Oversight™ model to help plan and communicate the value of cross-functional collaboration.

06 SPONSORSHIP ACCEPTANCE & EXECUTIVE VALIDATION

We assist in communicating the value of the project to the business leader accountable for Security's new vision. This in turn assists in communicating the strategy to senior executives from other functions.

07 DEFINE BUSINESS VALUE MEASURES

Business value metrics are developed for the client team to measure and determine project success for the organization, including key stakeholders.

08 IMPLEMENTATION ASSISTANCE

Last, clients can either take the SEC deliverables and run with them, or we can guide you through the implementation of your plan. At the end of the day, **the SEC is here to help you succeed.**

The SEC Process Outcome: Security Leader and Program Success

Elsevier
The Boulevard, Langford Lane, Kidlington, Oxford, OX5 1GB, UK
225 Wyman Street, Waltham, MA 02451, USA

First published 2013

Notices
Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods, professional practices, or medical treatment may become necessary.

Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information, methods, compounds, or experiments described herein. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-417232-6

For more publications in the Elsevier Risk Management and Security Collection, visit our website at store.elsevier.com/SecurityExecutiveCouncil.

CONTENTS

CHAPTER 1

Information Protection Function One: Governance

The governance function establishes and maintains a framework to provide assurance that information protection strategies are aligned with business objectives and consistent with applicable laws and regulations. The objectives of the governance function and how they might best be implemented are as follows:

Objective	Implementation
1. Develop the IP strategy in support of business strategy and direction.	Strategic management
2. Obtain senior management commitment and support.	Reporting and communication
3. Ensure the definition and implementation of roles and responsibilities throughout the organization.	Roles and responsibilities
4. Establish reporting and communication channels that support IP governance activities.	Reporting and communication
5. Identify and assess the impact of current and potential legal and regulatory issues.	Regulations and compliance management
6. Establish and maintain policies that support business goals and objectives.	Policies
7. Ensure the development of procedures and guidelines that support the policies.	Procedures and guidelines
8. Develop business case and organization value analysis that support IP program investments.	Portfolio management

IP is fundamentally a management problem, and its effectiveness is significantly impacted by the organization's approach to governance. The implementation of sound IP will require the following seven governance-related implementations.

IMPLEMENTATION ONE: STRATEGIC MANAGEMENT

Strategic management is the process of making and implementing strategic decisions. It is a mechanism used to bring change to organizations to facilitate the movement from what the organization is toward what the

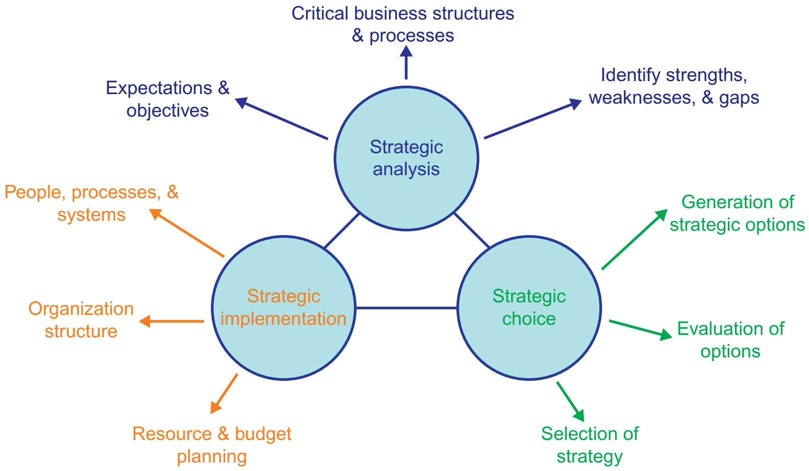

Critical business structures & processes
Expectations & objectives
Identify strengths, weaknesses, & gaps
Strategic analysis
People, processes, & systems
Generation of strategic options
Organization structure
Strategic implementation
Strategic choice
Evaluation of options
Resource & budget planning
Selection of strategy

Figure 1.1 Strategic Management.

organization seeks to become. Creating an IP strategy requires that the organization knows and understands its current resources and capabilities for IP functionality, and also knows and understands the threats that are present in the operational environment. The potential for a value-adding strategy lies in management's ability to identify opportunity for managed change, and to move toward the desired future state with the resources available for such a change. Strategy is the vehicle that uses an organization's objectives to design, develop, and deploy policies that will guide its activities as it moves to achieve its desired future state. As shown in Figure 1.1, there are three main elements of strategic management in this context:

1. Strategic analysis: Understanding an organization's strategic situation
2. Strategic choice: Choosing between courses of action
3. Strategic implementation: Putting the chosen course of action into effect

Major Milestones

Using this model of strategic management, the process can be resolved into six major milestones. Each of these milestones maps to one of the main elements.

	Milestones	Strategic Management Element
1.	Start-up	**Strategic analysis**
2.	Examine existing strategy	**Strategic analysis**
3.	Compare best practice	**Strategic analysis**
4.	Strategic options	**Strategic choice**
5.	Strategy and road map*	**Strategic implementation**
6.	Close-down*	**Strategic implementation**

**Strategy and road map and close-down partly map onto the strategic implementation element of the model. The mapping is partial as the actual roll-out of the implementation of the strategy occurs over several years.*

Six Strategic Management Milestones

1. Start-up

During the start-up part of the process, there is agreement on the details of the work plan. The key deliverables from this part of the work are an agreed scope, plan, and schedule. Key aspects are:

- Create a preliminary definition of the Information Protection Management Group (called the IPM Group hereafter). Who is in the group, how does it operate, and who is the champion representing senior management.
- Agreeing on the scope of the work (i.e., what's in and what's out)—consider various dimensions: the locations, functions, and departments to cover.
- Brainstorming (and possibly using other creative management techniques) and agreeing to an initial set of key issues to address as part of the work.
- Agreeing to the plan—consider timeframes and milestones.
- Agreeing to the work schedule. Consider the candidates to interview (top managers and other key people) and the timescales, and draft a briefing note to give to relevant individuals.

2. Examine Existing Strategy

When examining existing strategy, a brief report on opinions, observations, comments, and key issues will be completed. The following tasks will be done:

- Understand the business drivers for IP as the motivation for strategies within the organization.

- It is assumed that the members of the project team who are engaged in this process are familiar with the:
  - Statement of the organization's values (sometimes referred to as an organization's operating principles). This might best be described as "the essential nature of the organization's culture."
  - Statement of the organization's vision. This might best be described as "where the organization is headed."
  - Statement of the organization's mission (often referred to as a mission statement). This might best be described as "how will the organization get to where it is headed."

  Many organizations use these core documents to prepare an annual list of strategic objectives.
- Conduct interviews with the organization's top-level managers and other key people to solicit their insights, views, comments, and ideas concerning IP in the organization. The following areas will be explored:
  - What (realistic) position does the organization currently give to IP?
  - What are the main threats to the organization's business over the next three years?
  - How is risk management effected and what is the organization's appetite for risk?
  - What is the organization's attitude toward enforcement of IP polices (soft—with incentives, hard—with sanctions, mix of soft and hard—in what proportions)?
  - Budget provision for IP—historic/current/currently anticipated for the future?
- Study the IP department to understand the department's:
  - Structure and organization (especially how it relates to other areas of the organization).
  - Objectives and targets (i.e., what are its current drivers?).
  - Processes and functions (i.e., what is actually done and achieved?).

3. Compare Best Practice

When comparing best practice, a report on strengths, weaknesses, and gaps will be completed. The following tasks will be done:

- Gather relevant information from various regulations and guidelines, and draw upon relevant experience with other companies. Possible sources of relevant information are:
  - Sarbanes-Oxley Act (United States), European Union's Data Protection Directive, Canada's PIPEDA, OECD's Guidelines on

  the Protection of Privacy, FTC Fair Information Practices, HIPAA, HITECH, GLBA, Safe Harbor, and so on.
  - ISO 27000 series, NIST, COBIT, NFPA 1600, British Standards Institution (BSI), PAS 56:2003 (Guide to Business Continuity Management).
- Undertake the best practice comparison, identifying the strengths and weaknesses of the organization's existing IP organization, practices, and operations as well as the threats and opportunities the organization faces at the present time. Some organizations call this process and the resulting assessment a SWOT analysis.
- Identify and assess any gaps. This would highlight any missing practices, misaligned objectives, and inefficiencies (particular attention will be paid to any areas where potential cost savings could be made and/or critical investment is needed).

4. Strategic Options

During the strategic options part of the process, a report on the strategic options and their change implications will be provided. There is a need to consider "strategic fit" of the options; for example, is the proposed strategy suitable, feasible, and acceptable to the organization? Is it playing to key strengths, exploiting opportunities, capitalizing on distinctive competencies? Will it meet the organization's objectives? Will it fit the organization's management values and culture? Will it be acceptable to the organization's stakeholders? The following tasks, which will require working very closely with key organization staff, will be done:

- Develop and discuss strategic options for the future of IP within the organization. These options may cover such areas as: organization, relationships, processes, standards, skills, resources, technologies, and knowledge base.
- Consider the implications of these options for strategic change within the organization. Explore positive drivers and negative resistance factors for the strategic change.
- Prepare and give a presentation to key people in the organization.
- In coordination with the organization, select the most appropriate strategic options to take forward.

5. Strategy and Road Map

During the strategy and road map part of the process, a documented IP strategy and a road map for its implementation over the next several years will be provided. The following tasks, which will require working very closely with key organization staff, will be done:

- Develop and document the IP strategy for the organization.
- Develop a road map for the next two to three years. This will be a high-level implementation plan for the rollout of the IP strategy for the organization. This document will deal with priorities and timeframes for the various components of the IP strategy. Draft, first-cut budgets, and resource levels will also be proposed wherever possible.
- Prepare and give a presentation to communicate the strategy and road map to key members of the organization.

6. Close-Down

During the close-down part of the process, a brief report will be provided on the lessons learned. The key aspect to include in the report is:

- Reflecting on the work and documenting what went well and any areas of future improvement.

Key Points of the Strategic Management Process

As the governance management process proceeds, keep in mind eight crucial issues that should be addressed:

1. Assure the alignment of IP strategy with the organization's business objectives.
2. Verify that the organization's risk appetite is well understood, and that it accurately reflects management's attitude toward the risk of operating and information systems.
3. Confirm that IP activities are well coordinated with and mutually supportive of business processes.
4. Document the implemented approach to IP investment.
5. Finalize the structure, organization, and placement of the IP group.
6. Define the future structure of the IP group, identify resources that will be needed for those plans, and define the future state skills mix.
7. Plan for the integration and assimilation of IP strategy throughout the organization.
8. Have a defined plan for sustaining the IP strategy.