Managing Information Security Risks in a Shared Services Organization

scottmadden
MANAGEMENT CONSULTANTS

Smart. Focused. Done Right.®

ScottMadden partnered with a multifunction shared services organization (SSO) in the entertainment industry to assess its security practices. The SSO had a typical design, where confidential data (e.g., salary, social security number, personal address) moved through many systems and was subjected to multiple touch points and delivery options. A security control framework, based on ISO 27001, had been implemented by the enterprise; however, policies and related security controls were incomplete. As with many SSOs, data security often came secondary to gains in operational efficiency and customer service, which were more visible to the business.

Given recent security breaches in the company's industry and feeling a compelling need to drive change, the SSO engaged ScottMadden to work with the team to identify the risks to the organization's information and prioritize mitigating solutions.

The Challenge

SSO employees had a general awareness of information security concepts and their applicability to sensitive information. Consequently, the team had many good processes in place and a general desire to do the right thing. However, they encountered barriers when implementing sustainable improvements in security practices.

The SSO team had a good sense of their risk areas, but they did not fully understand the breadth and pervasiveness of these risks. These unknown risks compounded with the magnitude of data handled by the SSO made it difficult to develop an approach in which they had confidence.

The SSO needed a holistic view of security risks in order to understand how best to utilize its resources on risk remediation

Identifying and remediating risks were hampered by a lack of clarity and alignment between the SSO's business needs and enterprise security standards. Limitations to linking the policy with a process led to recommendations and solutions that were not operationally pragmatic or did not address the SSO's security needs.

When attempts were made to implement risk-mitigating solutions, the SSO often ran into uncertainty over governance and authority among influential stakeholder groups. This yielded conflicting recommendations, limited guidance on the implementation approach and timing, and unanswered questions on budget and support.

As with most organizations, there was a healthy tension between the business and the information security organization. The SSO needed a holistic view of security risks in order to understand how best to utilize its resources on risk remediation and develop pragmatic, sustainable solutions meeting its needs.

How We Helped

Utilizing our expertise in shared services and information security, ScottMadden conducted a maturity assessment of the SSO's information-handling processes. Based on the findings from the maturity assessment, ScottMadden conducted workshops and other activities to validate the assessment and develop actionable solutions. The approach was collaborative in order to enhance the sustainability of the effort and improve the security posture of the SSO. This approach included the five-step process depicted in Figure 1.

Upon completion of the assessment, the recommendations included the following attributes:

- They addressed department-level risks the SSO could control and resolve directly
- They included implementation plans and timelines scoped and developed in collaboration with the SSO
- They addressed enterprise-level risks by problem solving with external stakeholders
- The risks were prioritized according to near-term impact, considering the criticality to the business and the ease of implementation

Results

As a result of the assessment, the SSO was able to realize the following outcomes:

- An enhanced security culture within the SSO as a result of the team working together to develop security solutions
- The creation of a new security position focused exclusively on sustaining security
- Prioritized recommendations tailored to meet the SSO's business needs
- A security road map addressing identified risks and improving information security for both the SSO and the enterprise

ScottMadden knows shared services, and we know information security. We are uniquely positioned to help SSOs protect their important information. Please contact us to learn more about SSO security and how to put in place a program that builds confidence that you are addressing your most urgent data security risks.

Figure 1a: Five-step Process

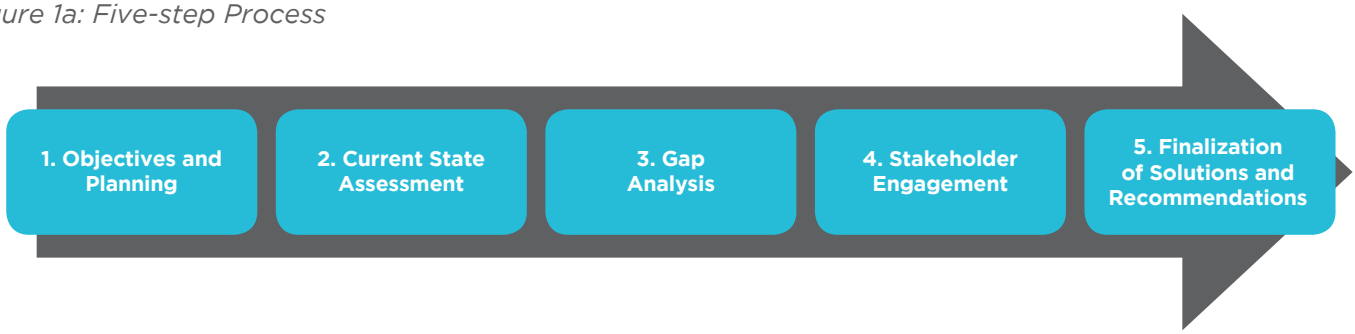

Figure 1b: Five-step Process Details

1. Objectives and Planning

- Confirmed project objectives
- Defined project plan and schedule

2. Current State Assessment

- Screened enterprise security policies for applicability
- Conducted interviews with key employees
- Collected findings and observations

3. Gap Analysis

- Assessed compliance with applicable enterprise security policies and controls
- Developed a maturity assessment
- Identified gaps/risks in security practices

4. Stakeholder Engagement

- Reviewed and validated findings and observations
- Conducted a workshop with key employees to develop solutions

5. Finalization of Solutions and Recommendations

- Developed solution implementation plans and timelines
- Leveraged industry best practices to develop high-level recommendations

Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

LOCATIONS

ATLANTA
3495 Piedmont Road, NE
Building 10, Suite 805
Atlanta, GA 30305
404.814.0020

RALEIGH
2626 Glenwood Avenue
Suite 480
Raleigh, NC 27608
919.781.4191

WESTBOROUGH
1900 West Park Drive
Suite 250
Westborough, MA 01581
508.202.7918