# Data Protection for Shared Services

## Part Two: Building the Foundation for Your Shared Services Data Protection Program

May 2017

Smart. Focused. Done Right.®

scottmadden
MANAGEMENT CONSULTANTS

# Building the Foundation for Your Shared Services Data Protection Program

## INTRODUCTION

As a Shared Services Organization (SSO) owner, it is your responsibility to protect your data and mitigate the risk of a data breach. Establishing a data protection program can help you accomplish this. A comprehensive data protection program establishes policies, procedures, and controls that monitor, detect, and even block data transmissions. Technology solutions can prevent distribution or leakage of sensitive data, regardless of whether the leak was intentional or inadvertent.

To effectively build and implement a suitable shared services data protection program, you need an in-depth understanding of the data you need to protect. A comprehensive understanding of your data ensures your program adequately mitigates all relevant risks. First, you will need to define the objectives and scope of your program.

### Define the Data Protection Program

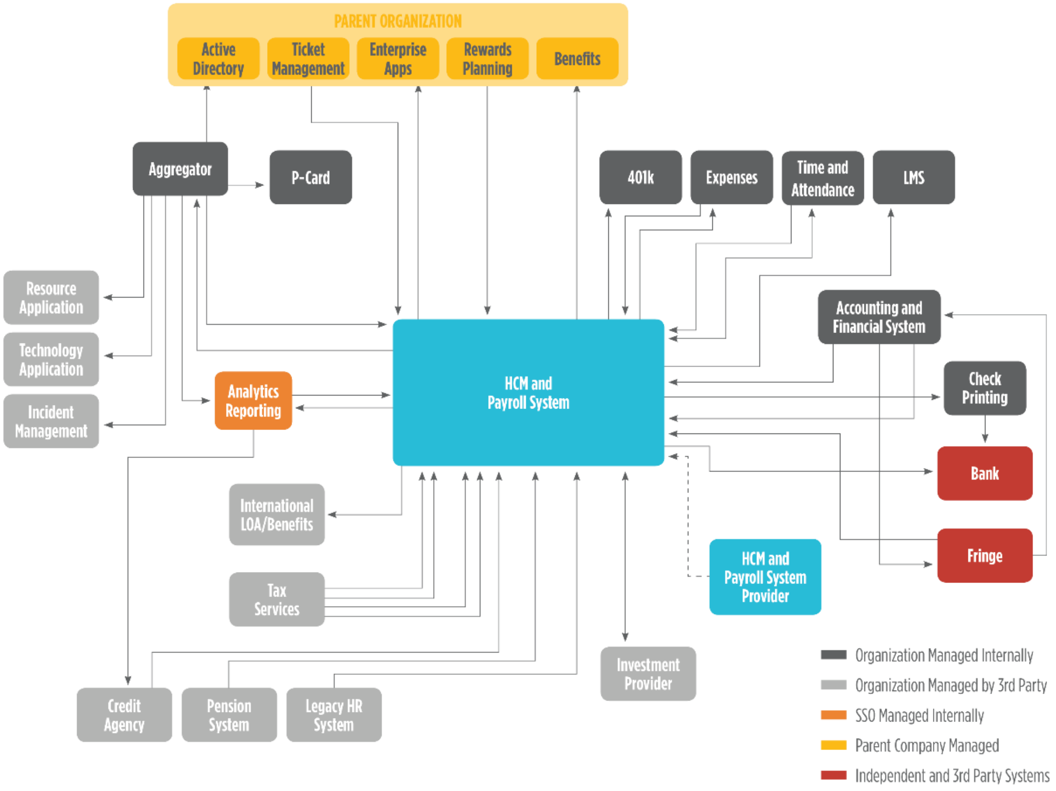
Data protection programs are enabled by technology; however, implementing technology is not enough. An effective data protection program starts with carefully defining the program objectives, securing buy-in from all stakeholders, establishing key performance indicators (KPIs), and establishing a change management plan:

- **Defining Program Objectives.** The objectives for implementing a data protection program are driven by your business's unique data protection needs. When establishing these objectives, ensure that your program defines expected outcomes for data that is important and must be protected
- **Securing Stakeholder Buy-in.** A data protection program cannot be a success without the combined efforts and support of key stakeholders. They should be engaged in the identification of data breach risks. Ensure that there is no disconnect across the stakeholders on the purpose and scope of your program
- **Establishing KPIs.** The right KPIs are essential to measure the success of your data protection program. These KPIs may include the number of data leakage incidents, the extent of process coverage, and the level of application coverage. Establish KPIs early in the planning process to baseline where you stand right now and where you want to be
- **Establishing a Change Management Plan.** A comprehensive data protection program brings significant changes to your SSO operations, employee behavior, and culture. Employees could perceive that the data protection program is intrusive and unproductive; therefore, part of your data protection strategy must be to establish a change management plan to build awareness for the need of your program

### Know Your Data

Identification and classification of data is the most important part of the SSO data protection program. As shown in Figure 1, SSO data is constantly moving through systems, applications, and individuals resulting in an extremely complex SSO information ecosystem. The volume of sensitive data makes SSOs a target. While a high volume of data tends to correlate with increased operational efficiency, it also increases the risk that this data may be compromised. Despite this risk, data security is often overlooked in favor of gains in operational efficiency and customer service.

***Figure 1: Complexity of HR SSO Information Ecosystem***



Due to the sheer volume and diversity of SSO data, it's important to carefully analyze your data to set the policies needed to detect and respond to incidents. As shown in Figure 2, ScottMadden recommends four steps:

- **Step 1: Understand Data Access and Flow.** A key step in planning for an effective data protection program is understanding how the data is accessed and how it flows in and out of your organization
  - **Access**: Most users access data within applications, such as case management, HR information systems, or accounts payable systems. Shared drives, end-user devices, and third-party tools, like cloud storage services, are also used for data storage
  - **Transmission**: SSO application integrations are the primary data transmission media used by the end users. However, some data integrations occur over unsecured pathways (e.g., email) and need to be identified and secured
- **Step 2: Identify Sensitive Data.** Identification of data is a challenging step in designing a SSO data protection program. At any given time, sensitive data is being used, shared, or stored across your servers, databases, workstations, laptops, and internal networks. Your

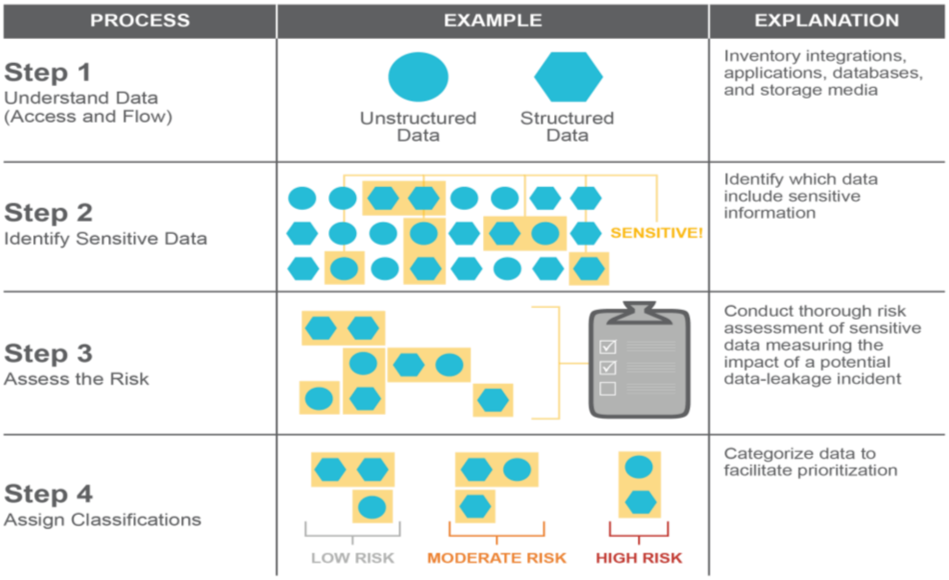
organization’s data can be divided into two broad categories: structured data and unstructured data

- **Structured data** refers to any data that resides in relational databases and spreadsheets, including benefits information, employee payroll information, and personally identifiable information. The structured data has the advantage of being easily entered, stored, queried, and analyzed and is typically managed centrally
- **Unstructured data** consists of all data that cannot be easily organized and includes PowerPoint presentations, word processing documents, PDF files, emails, and images. Unstructured data is managed by end users

Identify structured data by working with SSO centers of excellence to understand what sensitive data is stored in databases and other network locations, how it is managed, and how it is accessed. Identify unstructured data using a variety of discovery tools. This includes special data-loss-prevention products that come with a range of data identification technologies. These products consist of a discovery engine that crawls all the data in your SSO network, indexes it, and organizes it for risk assessment and classification.

- **Step 3: Assess the Risk.** Classify data by assessing the risk associated with it. You can then assign protection measures based on data risk classification. Assess risk using questions such as:
  - Is the data protected by regulations?
  - Is the data critical to business operations, and if so, can it cause financial loss?
  - Is the data important from a privacy perspective?
  - Is the data important to customers and business partners?
- **Step 4: Assign Classifications.** Based on the data risk assessment, assign classifications (high risk, moderate risk, low risk) to the data. These classification levels are often defined by enterprise information security

***Figure 2: Know Your Data***



| PROCESS | EXAMPLE | EXPLANATION |
|---|---|---|
| **Step 1**<br>Understand Data (Access and Flow) | Unstructured Data<br>Structured Data | Inventory integrations, applications, databases, and storage media |
| **Step 2**<br>Identify Sensitive Data | SENSITIVE! | Identify which data include sensitive information |
| **Step 3**<br>Assess the Risk | | Conduct thorough risk assessment of sensitive data measuring the impact of a potential data-leakage incident |
| **Step 4**<br>Assign Classifications | LOW RISK<br>MODERATE RISK<br>HIGH RISK | Categorize data to facilitate prioritization |

## TAKEAWAYS

- Focus on understanding and protecting SSO data risks rather than implementing technical data protection products. A thorough data inventory and assessment will help you develop accurate data protection policies and procedures
- Establish KPIs to measure your data protection program's success. KPIs will help you monitor progress and prove value to your stakeholders
- Spend time on stakeholder buy-in and proactive communication with employees. Implementing a SSO data protection program is not an IT project, but a SSO business initiative that requires both process and employee behavior changes

## NEXT STEPS

Once you have defined your SSO data protection program, obtained stakeholder buy-in, and undertaken the analysis of your data, it's time to consider the processes, policies, and procedures involved in a successful data protection program. For more information, see Part Three: The Core Elements of Your Data Protection Program.

## HOW SCOTTMADDEN CAN HELP

ScottMadden can help you understand and resolve your shared services security issues by improving how you manage and govern cybersecurity. We provide a strategic, outcome-driven approach customized to your organization's needs that entails four key actions: (i) identify the biggest security risks for your operation; (ii) assess the appropriate risk response; (iii) establish success measures for your security program; and (iv) determine how best to get to the desired state.

ScottMadden is recognized as a shared services expert. We understand shared services operations, their risks, and the security practices that work best in these environments. Leveraging institutional knowledge and expertise, our experts can help you achieve your shared services security goals.

Please visit www.scottmadden.com to learn more about the services we offer.

## ABOUT SCOTTMADDEN'S CORPORATE & SHARED SERVICES PRACTICE

ScottMadden has been a pioneer in corporate and shared services since the practice began decades ago. Our Corporate & Shared Services practice has completed more than 1,500 projects since the early 90s, including hundreds of large, multi-year implementations. Our clients span a variety of industries from entertainment to energy to high tech. Examples of our projects include business case development, shared services design, and shared services build support and implementation.

## ABOUT THE AUTHORS

Jon Kerner (jkerner@scottmadden.com), partner and information technology practice area leader, Henry Bell (henrybell@scottmadden.com), director, Harold Lewis (hlewis@scottmadden.com), manager, and Jonathan Harb (jonathanharb@scottmadden.com), senior associate, are located in the Atlanta office. Talha Sheikh (tsheikh@scottmadden.com) is a senior associate in the Raleigh office.

## SOURCES

- ScottMadden Research and Expertise
- 2016 Data Breach Investigations Report, Verizon, 2016: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
- SNL Financial, SNL.com, March 2016
- *2016 Cost of Data Breach Study: Global Analysis*, Ponemon Institute LLC, June 2016
- *Data Loss Prevention*, SANS Institute, August 2008: https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883
- *Understanding and Selecting a DLP Solution*, SANS Institute, December 2007: https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf