



Data leakage prevention  
Quantifying the risk

All organisations hold sensitive data that their customers, business partners, regulators, shareholders and the Board expect them to protect. Despite this, high profile security breaches involving personal and corporate data continue. The impact of regulatory intervention combined with negative publicity and public perception is prompting organisations to take immediate measures to understand the sensitive information they hold, how it is controlled and how to prevent it from being leaked.

The key questions any organisation needs to answer are:

- What is our confidential data?
- Where is our confidential data logically and physically stored?
- How is it being used?
- How is the risk of a leak being minimised?

### Giving you answers

We use powerful technology solutions that help answer these questions and, through a short risk assessment, will quantify the risk you may be facing in relation to data leakage. We configure the technology to monitor your network for various types of data that are being stored or sent in violation of your policies.

The assessment can look at the following 3 scenarios:

#### 1. Data in use

Monitor user interactions with data to identify, for example, attempts to transfer sensitive content to a USB drive.

#### 2. Data in motion

Analyze data traffic over the network to identify sensitive content being sent via email.

#### 3. Data at rest

Scan and inspect data repositories to identify where sensitive content is being kept.

### Sample risk assessment output

Priority data	Severity of loss	Stored data		Data usage	
		Frequency	Risk	Frequency	Risk
Source code	High	High 721 incidents	Very high	High 256 incidents	Very high
Customer data	High	High 10,178 incidents	Very high	High 2,178 incidents	Very high
M & A plans	High	Very high 78 incidents	Very high	Medium 9 incidents	Medium
PCI	High	Medium 7939 incidents	Medium	Medium 132 incidents	Medium
Pricing data	High	High 624 incidents	High	High 124 incidents	High

● Low risk     
 ● Medium risk     
 ● High risk     
 ● Very high risk

We follow a 4-step process:

#### **Step 1: requirements gathering**

First, we work with you to identify your top data security and privacy priorities:

- Determining high-risk information, senders and destinations;
- Brainstorming potential worst-case-scenario data loss events;
- Identifying data types, file servers and policies to be monitored; and
- Identifying priority compliance regulations.

Participants in this step typically include key decision makers and information owners, executive sponsors, project managers, security analysts and network engineers.

#### **Step 2: policy definition**

Based on the information gathered in step 1 - including data prioritisation by type, exposed data on file shares, sender and recipient - we configure the tools to be run on the identified areas according to your requirements.

#### **Step 3: confidential data monitoring**

The next step is the monitoring of your confidential data across the identified areas, be that endpoint, network or storage systems. This provides quantifiable results on your organisation's current level of confidential data risk by data type, file share, sender, recipient, policy and network protocol. In most cases, the chosen solution can be up and running within 30 minutes and the assessments are run over a two to four week period.

#### **Step 4: reporting**

Following the discovery and monitoring phase, our team gathers with the key decision makers and information owners from your organisation for a one-hour executive-level meeting to review the results of the project, examine the risk assessment reports and discuss next steps. We deliver the following reports at the

conclusion of the risk assessment in an executive presentation:

#### ***Data loss risk assessment summary***

Identify areas of Very High, High, Medium, and Low risk of data leakage across endpoint, network and storage systems by data type, based on your evaluation of potential severity and your actual frequency of data loss.

#### ***Industry benchmark comparison***

Benchmark your actual data exposure and loss metrics against industry averages so you can learn how your organisation ranks in terms of overall risk.

#### ***Compliance scorecard***

Measure your risk of non-compliance with regulation, laws and standards such as Payment Card Industry Data Security Standard (PCI DSS).

#### ***Business case for data loss prevention***

An executive-level report that quantifies the frequency, severity and risk of loss by data type and can help build the business case for ongoing remediation. This might include further technology deployment or tactical controls reviews.

#### **Why Deloitte?**

Technology risk issues are widely recognised as having a significantly adverse impact on business, resulting in not just financial losses, but damage to reputation and operational downtime as well. Deloitte is uniquely positioned in the marketplace to deliver a broad range of objective and comprehensive technology risk services in a concise way, leveraging its global network, research, proven methodologies, preferred practices and client experience. Our Technology Services practice draws on the resources of a highly skilled and experienced team of professionals both locally and worldwide. We provide a full range of internally and externally focused technology risk services covering all aspects of business process risk, IT risk, data quality and integrity risk, IT project risk and information security risk.

## Here to meet your needs

### Malta contacts:

#### Ashraf Fahmy

Leader Enterprise Risk Services  
Tel + 356 23432000  
asfahmy@deloitte.com.mt

#### Raphael Aloisio

Leader Financial Advisory  
Tel + 356 23432000  
raloisio@deloitte.com.mt

#### Ivan Spiteri

Manager Financial Advisory  
Tel + 356 23432000  
ispiteri@deloitte.com.mt

Deloitte Place, Mriehel Bypass, Mriehel BKR3000, Malta  
Telephone: (+356) 2343 2000  
Facsimile: (+356) 2134 4443  
[www.deloitte.com/mt](http://www.deloitte.com/mt)

#### About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte Malta refers to a civil partnership constituted between limited liability companies, and its affiliated operating entities; Deloitte Services Limited and Deloitte Audit Limited. The latter is authorised to provide audit services in Malta in terms of the Accountancy Profession Act.

A list of the corporate partners, as well as the principals authorised to sign reports on behalf of the firm, is available at [www.deloitte.com/mt/about](http://www.deloitte.com/mt/about).

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 169,000 professionals are committed to becoming the standard of excellence.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.