FEATURE

The Four Questions for Successful DLP Implementation

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

https://bit.ly/2RItFh1

Information is a critical aspect of organizational success. Individuals or organizations with a better understanding of their information and an information management plan have been known to excel over those with a limited grasp of their information resources. Coupled with advancements in digital transformation and technology, information has become a cornerstone of business success, requiring organizations to implement measures that provide assurance of continued value cultivation from information resources.

Data loss prevention or protection (DLP) is conventionally defined as a suite of software applications designed to detect potential data breaches/data exfiltration transmissions and subsequently prevent them by monitoring, detecting and blocking sensitive data while in use, in motion and at rest. This approach to DLP typically classifies sensitive information and prevents its unauthorized disclosure or sharing. DLP applications range from open source to enterprise commercial solutions.

Christopher Nanchengwa, CISA, CRISC, ITIL v3, PRINCE2
Is the information security manager for the Zambia Electronic Clearing House Limited. He has 10 years of experience in information technology management, with the last five focused on information security management. He can be reached at chris.nanch@gmail.com.

Common examples include OpenDLP, MyDLP, and those offered by Symantec, Kaspersky, McAfee and other commercial service providers. Furthermore, these applications are available with either agent or agentless capabilities. This product approach to DLP has one major downside: It focuses on only the technical aspect of data loss. The alternative is to view DLP as a program, that is, a portfolio of measures or undertakings adopted by an organization to ensure the protection of critical and valuable organizational information. This includes various administrative, technical and physical undertakings that span people, technologies and processes. The program approach to DLP enables a holistic view of risk to which information as an asset is exposed and the controls aimed at maintaining the risk exposure within the organization's comfort zone. For the purposes of this discussion, DLP is viewed as a program.

In light of technological developments and associated risk, organizations are mandated to have living DLP programs that ensure the institution of measures or controls that provide reasonable assurance that information value continues to be preserved. Most organizations adopt a framework that ensures a consistent and measurable approach to information security; one such framework is ISACA's COBIT® 5 framework for the enterprise governance of information and technology (EGIT). COBIT 5 proposes 37 processes grouped into five domains (**figure 1**).[1] Five of the processes are of note with regard to information security:

- EDM03 *Ensure risk optimization*
- APO12 *Manage risk*
- APO13 *Manage security*
- DSS05 *Manage security services*
- MEA02 *Monitor, evaluate and assess the system of internal controls*

These processes are further detailed into subprocesses that provide guidance on the protection of information resources. Other industry- and region-specific standards include the Payment Card Industry Data Security Standard (PCI DSS),

managed by the Payment Card Industry Security and Standards Council (PCI SCC); the US Health Insurance Portability and Accountability Act (HIPAA); and the EU General Data Protection Regulation (GDPR).

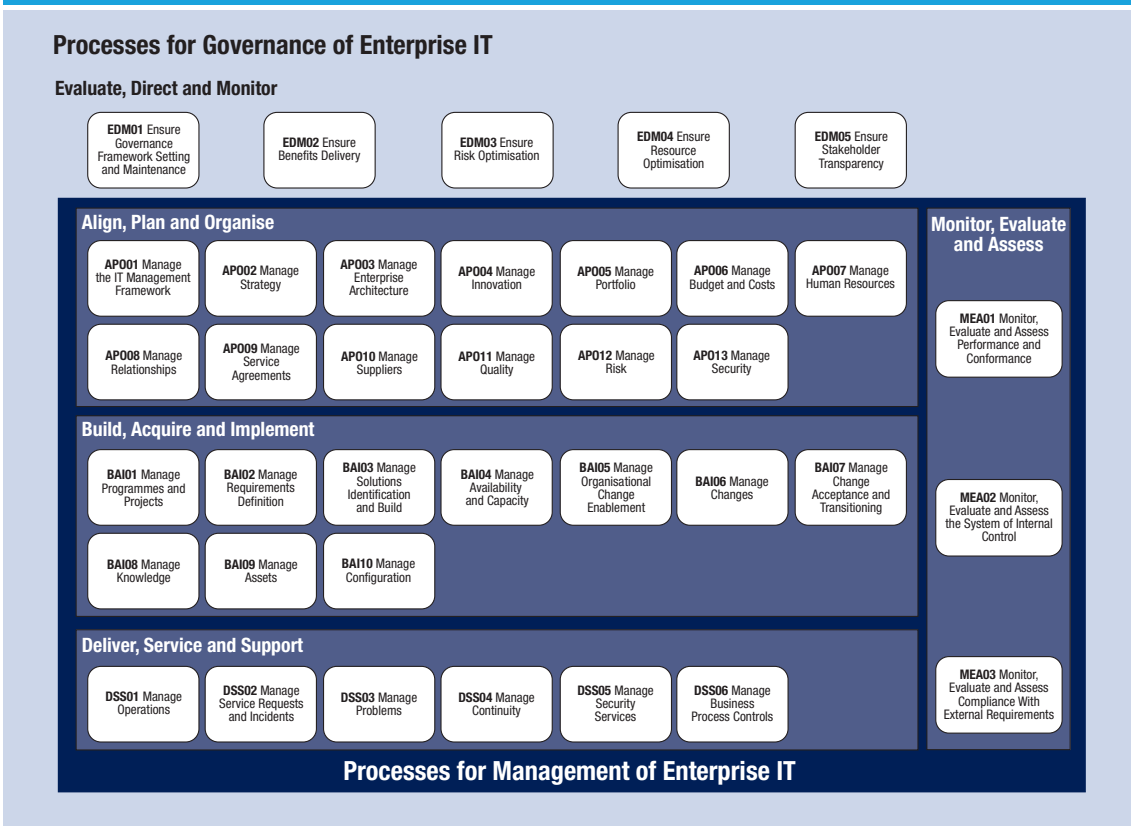
This is a summary of four cardinal questions an entity needs to address to ensure a successful and value-driven DLP program.

Question One: What Information Is of Value to an Organization?

The first and most important step of DLP implementation is the identification and classification of organizational information. Industry best practice proposes two information classification standards for public (government) and private institutions: classification by level of importance and impact of its disclosure or destruction. The classification should follow a risk-based approach. The classification standard for public information interprets the potential risk impact in terms of national security and stability, as depicted in **figure 2**.

Information employed in private institutions is classified in accordance with the impact of risk on the achievement of enterprise objectives; this is usually depicted in monetary form. **Figure 3**

Figure 1—COBIT 5 Processes



Source: ISACA®, COBIT 5, USA, 2012. Reprinted with permission.

Figure 2—Public Information Classification Standard

Classification	Description
Top secret	Disclosure of top-secret data would cause severe damage to national security.
Secret	Disclosure of secret data would cause serious damage to national security. These data are considered less sensitive than data classified as top secret.
Confidential	Confidential data are usually exempt from disclosure under laws such as the US Freedom of Information Act, but are not classified as national security data.
Sensitive but unclassified (SBU)	SBU data are not considered vital to national security, but their disclosure would do some harm. Many agencies classify data they collect from citizens as SBU.
Unclassified	Unclassified data have no classification or are not sensitive.

Enjoying this article?

- Learn more about, discuss and collaborate on information security management ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> THE FIRST AND MOST IMPORTANT STEP OF DLP IMPLEMENTATION IS THE IDENTIFICATION AND CLASSIFICATION OF ORGANIZATIONAL INFORMATION.

contains a typical list of classifications that can be used for enterprises, from highest to lowest.

An organization should identify the different types of its information and group them according to the labels of the guiding standard—private or public. This is normally presented in the form of a table or matrix as depicted in **figure 4**.

Further to the classification of information, an organization should implement protection profiles for the respective information classes and adopt a policy to review on a timely basis the effectiveness and relevance of the classification framework. The protection profiles should define minimum administrative, technical and physical controls for the protection of relevant information; this includes access controls, password and encryption requirements. Over time, different sets of information will either gain or lose value and should be reclassified accordingly.

Question Two: Who Is Responsible for the Protection of Organizational Information?

The responsibility for protecting organizational information rests with all stakeholders at different levels of the organization.[2]

Business owners and mission owners (senior management) create the information security program and ensure that it is availed the necessary resources and given appropriate organizational priority.

The data owner (also called information owner) is a manager responsible for ensuring that specific data are protected. Data owners determine data sensitivity labels and the frequency of data backup. An organization with multiple lines of business may have multiple data owners. The data owner performs management duties, while custodians perform the hands-on protection of data.

The system owner is a manager who is responsible for the actual computers that house data. This includes the hardware and software configuration, including updates and patching.

Figure 4—Information Classification Matrix

Information Classification	Examples
Sensitive	Passwords, encryption keys, payment card details
Confidential	Internal market research, audit reports
Private	Policies and procedures
Proprietary	Intellectual property
Public	Contact information

Figure 3—Private Information Classification Standard

Classification	Description
Sensitive	These data are to have the most limited access and require a high degree of integrity. Typically, they are data that will do the most damage to the organization should they be disclosed.
Confidential	These are data that might be less restrictive within the company, but might cause damage if disclosed.
Private	Private data are usually compartmental data that might not do the organization damage, but must be kept private for other reasons. Human resources data are one example of data that can be classified as private.
Proprietary	Proprietary data are disclosed outside the organization on a limited basis or contain information that could reduce the organization's competitive advantage, such as the technical specifications of a new product.
Public	Public data are the least sensitive data used by the organization and would cause the least harm if disclosed. This could be anything from data used for marketing to the number of employees in the organization.

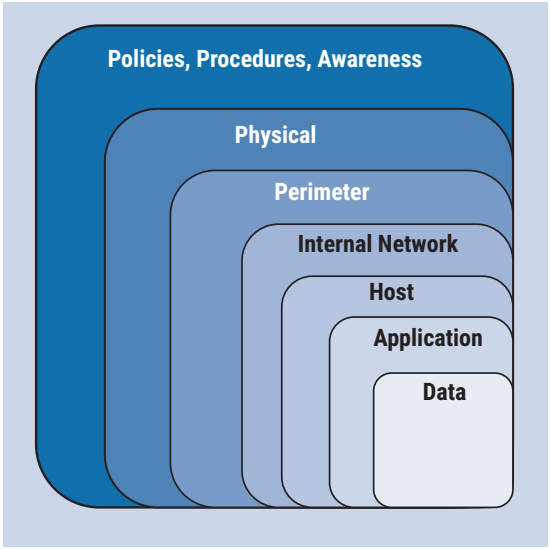
Custodians provide hands-on protection of assets, such as data. They perform data backups and restoration, patch systems, and configure antivirus software. Custodians follow detailed orders and do not make critical decisions on how data are protected.

Users must follow the rules; they must comply with mandatory policies, procedures and standards. For example, users must not write their passwords down or share accounts. Users must be made aware of pertinent risk and requirements. They must also be made aware of the penalty for failing to comply with mandatory directives and policies.

Question Three: How Can Organizational Information Best Be Protected?

To effectively protect organizational information, a holistic approach should be adopted, one that targets information in its various states—in use, in transit and at rest. Industry best practices for information security recommend the adoption and implementation of a multilayered or defense-in-depth (DiD) strategy (**figure 5**).[3]

Figure 5—Defense in Depth



The DiD approach advocates for the implementation of various controls, such as administrative, technical and physical, at each layer of the model. It further advocates for organizations to have defined roles and responsibilities with regard to the protection of information resources.

The DiD layered approach to security ensures the holistic protection of data by implementing several controls ranging from the highest level (policies) to the lowest or elemental level (data).

Information security policies define management's stance with respect to the protection of information resources. They are normally crafted in a high-level business-centric language that sets the tone and defines the culture for data protection. These policies are then translated into procedural terms providing guidance on step-by-step security implementations. To ensure effectiveness, policies and security developments have to be communicated to all employees via a routine awareness exercise.

> "TO EFFECTIVELY PROTECT ORGANIZATIONAL INFORMATION, A HOLISTIC APPROACH SHOULD BE ADOPTED, ONE THAT TARGETS INFORMATION IN ITS VARIOUS STATES."

Physical security includes all measures taken to protect data in their physical/tangible form and the physical technology housing the data. These measures include controls aimed at remediating both natural and unnatural risk, including physical access controls, closed circuit television (CCTV) and fire prevention/mitigation systems.

Perimeter security focuses on enforcing entry and exit security at the network point of contact with outside networks that are presumed to be unsafe. These include the Internet and supplier, customer and partner networks. A firewall is typically employed to enforce perimeter security; firewalls can be classified into three broad groups depending on the complexity of their operations: packet filters, stateful and proxy firewalls. Organizations need to implement firewalls in line with their respective perimeter risk.

Internal network security measures include implementations strategically configured on the internal network to analyze traffic and alert/respond to insights. A network intrusion and detection or prevention system (NIPS) is one such system that studies traffic flowing among network-attached devices, with the capability to detect and respond to security anomalies. Another such implementation is a security information and event manager (SIEM), a software application installed on a network to collect and analyze machine-generated data. Machine-generated data are digital information created by the activity of computers, mobile phones, embedded systems and other network devices. This information includes application, server, business process logs; call detail records; and sensor data. SIEMs gather, analyze and present their results via dashboards and alerts; they support and enhance data-driven decisions supporting the protection of information resources.

Host security measures aim at protecting data against threat actors that target host or client machines including servers, desktops and mobile devices. These measures include host-based intrusion detection systems with file integrity management capabilities that scan and assess the integrity of system files; others include endpoint malware detection and remediation applications and access control provisions.

Application security provisions are intended to ensure that applications installed on host machines employ secure methods of accessing and utilizing data. This is achieved by ensuring that applications meet and continue to meet industry security quality standards including the Trusted Computer System Evaluation Criteria (TCSEC), Information Technology Security Evaluation Criteria (ITSEC) and International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 15408, The Common Criteria. This is achieved via a continuous and robust vulnerability program with recertification and accreditation of business systems and applications.

Data security measures protect raw data that are either stored or in transit. This calls for the implementation of encryption schemes that convert data from a readable to a nonreadable form. A number of encryption schemes, ranging from symmetric to asymmetric implementations, exist; organizations should employ strong encryption schemes that have a high work factor—schemes that present very difficult challenges to attempts to reverse the encryption process.

Figure 6 provides a summary of proposed controls or measures.

Question Four: How Effective Is the DLP Program?

To effectively monitor and manage the performance of a DLP program, several metrics have to be defined and managed.[4]

Figure 6—Security Control Summary

DiD Layer	Controls/Measures
Policies, procedures, awareness	Data classification matrix, information security policy, acceptable use policy, access control policy, information security awareness program, capability maturity management
Physical security	Closed circuit television (CCTV), access control, fire control, guards
Perimeter	Firewall, spam filters
Internal network	NIPS, SIEM, access control, DLP applications
Host	Host-based intrusion detection systems (IDS), endpoint malware detection and prevention systems, access control, vulnerability management, DLP applications
Application	Secure systems development life cycle (SDLC) management, vulnerability management
Data	Access control, encryption

A key risk indicator (KRI) is a measure used by management to indicate the risk level of an activity. They are metrics used by organizations to provide an early signal of increasing risk exposures in various areas of the enterprise. As part of its information communications and technology (ICT) and organizational risk management exercise, an organization should actively track its information risk and ensure that it is kept within acceptable thresholds in line with the organization's risk appetite. A risk register is used to document and report identified risk.

Information KRIs should be traceable to enterprise risk; this calls for the cascading of enterprise goals into IT and, subsequently, information goals. The objectives of enterprise information management are aimed at ensuring the continual cultivation of value from information via the preservation of the information's confidentiality, integrity and availability. In other words, information-related risk can be summarized into three generic risk areas:

- The risk that organizational information will be inappropriately disclosed
- The risk that organizational information will be inappropriately altered
- The risk that organizational information will be inappropriately destroyed or withheld

Indicators of the prevalence of the previously mentioned risk areas will vary from organization to organization depending on the organization's operational and infrastructure configurations, which determine the organization's surface of exposure to risk actors. The organization should maintain a program that tracks risk across the different states of data—in use, in transit and at rest. The DiD approach discussed earlier ensures a holistic approach to tracking risk (**figure 7**).

Key indicators of compromise (KICs) are incidents observed on a network or computer system that, with high confidence, indicate a network, host computer or system intrusion. Typical KICs are virus signatures and IP addresses, MD5 hashes of malware files, or URLs or domain names of botnet command and control servers. After KICs have been identified in a process

Figure 7—Key Risk Indicators Examples

DiD Layer	Key Risk Indicators
Policies, procedures, awareness	• Lack of information security policy • Lack of data classification matrix • Lack of protection criteria for classified data • Lack of defined operating procedures • Period since last policy review • Number/percentage of employees who miss awareness training
Physical security	• Physical controls not reflective of asset value • Lack of review of physical controls • Number of physical breaches/attempts since last review
Perimeter	• Lack of effective firewall system. • Firewall rules not reflective of business requirements • Period since last review of firewall rules • Period since last vulnerability/penetration test • Number/percentage of intrusion attempts since last review
Internal network	• Lack of NIPS and SIEM • Number/percentage of unresolved incidents • Lack of access control and review
Host	• Number/percentage of unpatched/out-of-date systems
Application	• Number/percentage of nonbusiness applications • Number/percentage of security-noncompliant systems/applications
Data	• Lack of access control and review • Number/percentage of weak encryption use

of incident response and computer forensics, they can be used for early detection of future attack attempts using intrusion detection systems and antivirus software. Efficient and effective monitoring of these KICs demand the implementation of centralized event log management and SIEM; this enhances an organization's threat intelligence capabilities.

> "DIGITAL TRANSFORMATION—WHILE ENHANCING BUSINESS PROCESSES—HAS INCREASED THE RISK EXPOSURE SURFACE OF ORGANIZATIONAL INFORMATION."

Other general performance management metrics include key goal indicators (KGIs) and key performance indicators (KPIs).

As a best practice, organizations need to track relevant indicators and provide assurance of information security to stakeholders. To a large extent, minimum measures to be implemented are dictated by respective standards such as PCI DSS, HIPAA and GDPR, which, in some cases, may demand the implementation of DLP solutions. Most DLP applications leverage their performance on the effective management and reporting of KICs.

Conclusion

Information is a critical aspect of enterprise performance and, to a large extent, a critical success factor for modern organizations. Information not only enables organizations to gain a competitive advantage over their competitors, but its proper management may be considered a determinant for survival. Digital transformation—while enhancing business processes—has increased the risk exposure surface of organizational information. Organizations need to ensure that risk associated with information is identified and managed in a systematic manner and, subsequently, safeguard the continued cultivation of value from information resources.

Editor's Note

ISACA recently released COBIT® 2019 *(www.isaca.org/COBIT)*. COBIT 2019 is an evolution of COBIT® and incorporates Risk IT, similar to the approach in COBIT® 5. A COBIT 2019 Risk Focus area is in development and is expected to be released in 2019.

Endnotes

1 ISACA®, *COBIT® 5: Enabling Processes*, USA, 2012, *www.isaca.org/COBIT*
2 Conrad, E.; S. Misenar; J. Feldman; *Eleventh Hour CISSP: Study Guide*, Syngress Eleventh Hour, USA, 2016
3 Layer Seven Security, "Defense in Depth: An Integrated Strategy for SAP Security," 2013, *https://layersevensecurity.com/resources/sap-security-whitepapers/*
4 Cannon, D. L.; B. T. O'Hara; A. Keele; *CISA Certified Information Systems Auditor Study Guide, 4th Edition*, John Wiley & Sons, USA, 2016