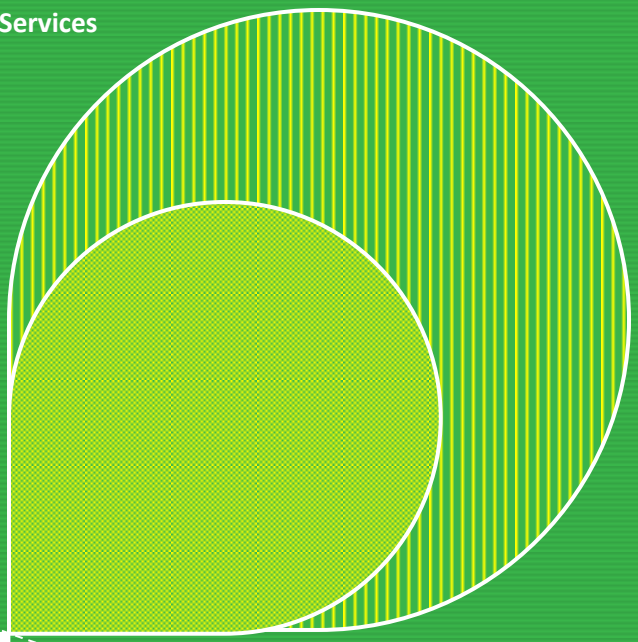
Data Classification – Taking control of your data

By Thiruvadinathan
Happiest Minds,
Infrastructure Management and Security Services



happiest minds

Data Classification - Taking control of your data

Data, the lifeline of business today

In today's business scenario, data has undeniably become the lifeline of any enterprise that looks to create value for itself and its stakeholders. Technology is increasingly becoming the fundamental fabric across organizations, irrespective of industry, in the way they conduct their business. Given the current economic circumstances, cost is undoubtedly a major factor that has redefined business operations and service delivery.

Organizations continue to look for effective ways to reduce operational cost. One of the sure shot ways to improve bottom-line is to manage information/data efficiently. Less is more. Security and compliance requirements also call for identifying, segregating and protecting data.

Protecting data is at the core of compliance whether it's for privacy or financial reporting. Factors such as confidentiality, integrity and availability matter for any company. That makes data classification the core of any successful data security and compliance program.

This article focuses on the key drivers for data classification - a high level process to design and implement a program, the challenges involved and long term benefits.

Enterprise Data Management Program

Certainly, the amount and types of data an organization has to deal with has been growing at an alarming rate. Storing and protecting data without clear knowledge of its utility is a drain on precious organizational resources. Therefore, it makes more sense to use data diligently and efficiently by employing specific mechanisms to identify, create, process, share, store and protect data. This would ensure that the data remain useful, relevant, reliable, complete, accurate, authentic, secure and compliant

Organizations across the globe are increasingly looking at enterprise programs such as:

- Information Life-cycle Management / Information Governance
- Data Loss Prevention
- Digital Rights Management

Organizations implement such programs to prevent and detect data breaches, security incidents, to control access to data, data retention, e-discovery, secure disposal and the cost associated with all these.

Regulatory Compliance

For organizations that are within the purview of regulations such as GLBA, HIPAA, Personal Data Protection Acts, PCI-DSS, and other industry mandates, it is very critical to identify regulated data

and institute necessary procedures to safeguard it throughout its life-cycle. Without the knowledge of and segregation of regulated data, an organization risks shifting off the compliance track or spending more than necessary.

Data classification plays a very critical role in achieving the business objectives of enterprise-wide data protection programs. It is an effective tool in the hands of both business and IT units to focus spend only on data that is critical and sensitive.

Data acts like a moving target

Data, in its many forms, is dictated by the dynamics of business, technology, security, privacy and compliance requirements. It is becoming much harder to identify the kinds of data that exist within the enterprise, where it resides, who has access to it, what is being done to it, and how secure it is. During its lifecycle, data continuously transforms itself and presents myriad challenges in use, interpretation and value, as it moves up the value chain across business functions. Data is, therefore, in a constant state of flux.

In the wake of new and evolving technologies such as Web 2.0, cloud computing, convergence of computing power with mobile devices and social networking, it has become imperative that every business stay on top of its data.

In order for data to remain useful and available at the time and in the form required, there are several measures that a business needs to undertake. Classifying data provides the basis to make decisions and identify such measures.

So, what is Data Classification?

Data classification is one of the most fundamental ingredients of an effective and efficient information security strategy. It directly impacts decisions, procedures and practices on what kind of data is collected, how it is stored, used, protected, shared or disclosed.

In very simple terms, it is an exercise carried out to understand the nature, type, criticality, sensitivity and other attributes of the data in order to distinguish between good and bad data, important vs. non-important data, etc. For example, financial reporting standards require attributes such as existence, completeness, and accuracy. These attributes play a very important role in designing and assessing controls at different layers for SOX compliance.

This understanding eventually helps build or strengthen the quality of the data, and thereby increases its usefulness and reliability, laying a strong foundation to make better and more informed business as well as risk management decisions.

Key steps for beginning a Data Classification program

1. Plan a pilot project for a given business process. Identify a particular business process or function and articulate the key goals of the process. While it is important to cover all the functions to ensure consistency and effectiveness in the application of policies and relevant procedures to safeguard data, it would be equally important to take smaller measurable steps and then build on it.

2. Identify data that the process requires, depends on, creates, disseminates and reports about.

3. Determine attributes such as sensitivity and criticality of data. This is where alignment with businesses is important to establish data ownership. For example, factors that influence the organization's perception of data attributes can be vision, mission, business goals and strategy, customers, competition, credit rating, and regulatory and contractual compliance requirements.

4. Identify the regulatory requirements such as PCI, GLBA, HIPAA, Data Protection Acts, Identity theft, etc, that are applicable to your business; define the nature and type of data that is required to be protected for each of the regulations.

5. Identify the requirements for security viz., Confidentiality, Integrity, and Availability (CIA). Integrity of data can be the foremost quality that should be preserved since protecting the confidentiality or availability of inaccurate data is futile.

6. Determine the impact to the process if any of these security requirements are compromised. The impact must be calculated by business and data owners in conjunction with other stakeholders.

7. Determine the applicable classes or levels of classifications such as Public, Internal, Confidential, Top Secret, Private, etc.; and develop criteria for classifying data into different levels.

Ensure that classification is in line with your organizational information security policy and business requirements. A meaningful classification may also help redefine your efforts in GRC as a whole.

Steps to be taken following a successful classification policy

Implementing the policy has its own challenges and can be a long-drawn out process. Implementing classification retrospectively is a mammoth task. Going back in time to identify and secure regulated and business sensitive data is equally important.

1. Determine how classified data will be collected, verified, created, processed, shared, stored, transmitted, archived and disposed.

2. Define security requirements for each of the stages. This is about controls for business applications such as those for existence, completeness, authorization, etc. For example, PCI data when stored or transmitted along with Primary Account Numbers (PAN) must be protected and encrypted; magnetic stripe and PIN data must never be stored; similarly, SOX places more stress on controls needed to prevent and detect actions that will harm the integrity of data.

3. Engage with the data owners, custodians and users to raise awareness and monitor internal compliance; external compliance can fall in place, naturally.

4. Build a strong case for the management to sponsor an enterprise-wide roll-out.

Challenges in designing a data classification program

1. Remember that your organization is unique and avoid any tendencies to implement a policy that works elsewhere.
2. A data classification initiative can become a complex project when it is rolled out across the enterprise at the first instance. The key would be to take small steps.
3. Some of the teething issues can be how and where to start, what data needs to be looked at, etc. Start small with a pilot project and build on it.
4. The role of security & IT professionals should not be confused. Their role is to facilitate decision-making by the business stakeholders and steer the project on course.
5. Lack of a well-defined management's intent and policy on information security protection
6. Lack of alignment with the requirements of business data owners for CIA
7. Lack of alignment with legislative, regulatory and contractual compliance requirements for business and personal data

Key Success Factors

- An effective mechanism to locate and determine critical and sensitive data for mission success
- Identification of relevant regulatory and statutory requirements for data protection
- Identification control deficiencies, excessive controls leading to effective and efficient security investments in controls, monitoring, review, etc.
- Determination of Recovery Point Objective (RPO) of data and enable assessment of business impact and risks

- Identification of minimum security requirements for the data when stored, in use, and transmitted, user access control, retention and disposal requirements, audit, review, monitoring, etc.
- Increased ability to respond effectively and efficiently to data discovery requirements arising out of any legal proceedings.
- Increased ability to understand newer dimensions of the data i.e. metadata to identify new opportunities for data use

To learn more about the **Happiest Minds Customer Experience Offerings,** please write to us at **business@happiestminds.com**

About Happiest Minds

Happiest Minds is a next-generation IT services company helping clients differentiate and win with a unique blend of innovative solutions and services based on the core technology pillars of **cloud computing, social computing, mobility and analytics.** We combine an unparalleled experience, comprehensive capabilities in the following industries: **Retail, Media, CPG, Manufacturing, Banking and Financial services, Travel and Hospitality and Hi-Tech** with pragmatic, forward-thinking advisory capabilities for the world's top businesses, governments and organizations. Founded in 2011, Happiest Minds is privately held with headquarters in Bangalore, India and offices in the USA and UK.

Corporate Office Happiest Minds Technologies Pvt. Ltd. Block II, Velankani Tech Park 43 Electronics City Hosur Road, Bangalore 560100, INDIA Phone: +91 80 332 03333 Fax: +91 80 332 03000	**United States** 116 Village Boulevard, Suite 200 Princeton, New Jersey, 08540 Phone:+1 609 951 2296 2018 156th Avenue NE #224 Bellevue, WA 98007 **United Kingdom** 200 Brook Drive, Green Park, Reading Berkshire, RG2 6UB **Phone:** +44 11892 56072 **Fax:** + 44 11892 56073

About the author

Thiruvadinathan A (thiruvadinathan.a@happiestminds.com) is the Technical Director and Practice Lead for IT Governance, Risk Management, Security & Compliance services. He credits his rich experience in the field to his global clientele across industry verticals gained in the last 16 years. One of his recent achievements is having successfully led Happiest Minds Technologies to meet the stringent requirements of ISO27001 global standard.