Data Classification: ITAM solution Identification and Data Classification.

Vincent Kiweesi

Data Classification

April 28, 2023

The paper is to justify why data classification should be made a part of the project and it is importance The paper will cover definition, application, and benefits of data classification, its potential cost and compliance benefits, proposed classification categories, data retention, document and data destruction, and data classification's integration with the new ITAM solution are all covered in the paper.

**Definition**

Data classification is the process of categorizing data into proper groups so that it can be used and protected more effectively. Simply put, the classification procedure facilitates finding and retrieving data. It is important in risk management, compliance, and data security (*Data classification policy template*).

The Scope outlines the categories of data that must be sorted as well as who is in charge of handling, protecting, and classifying the data appropriately.  
Any type of data, including written material and digital data saved on any form of media, is protected by this policy. It includes each staff member of the company as well as outside agents who have permission to access the data (Juliana De Groot on Wednesday February 8).

Benefits of data classifications may include.

The visibility into your organization's sensitive data provided by data classification allows you to identify your attack surface risk clearly. Using this knowledge, you may build a data protection strategy that prioritizes your most sensitive and at-risk data first.  
  
 Frequently, businesses have huge amounts of data but have no idea what data they have, where it is stored, or how it is being managed. This will only lead to disaster. By taking control over your data, categorization enables your company to fully understand the data it possesses and how it is being used.

The company will be better able to implement data privacy policies that make sure you comply with legal and regulatory compliance requirements once you are able to classify data depending on the data privacy standards it must comply with. Data classification additionally keeps a thorough record of how information was used, assisting in revealing to regulators that data is being properly managed and documented (*How data classification benefits your security strategy*).

**● How it could help the company from both a cost and compliance perspective**

**○ List specific compliance regimes such as Sarbanes-Oxley, export controls, and GDPR**

Data classification enables the business to identify and prioritize its most important data assets, as well as to apply the right safety measures and access controls to sensitive and private data. Data breaches can be expensive in terms of financial loss and reputational harm; therefore, this lowers their risk. Data classification enables the business to abide by data protection rules and laws like GDPR, Sarbanes-Oxley, and export restrictions. This lessens the possibility of expensive fines and legal action (*Data classification policy template*).

Sarbanes-Oxley (SOX) mandates that companies maintain accurate internal financial controls and financial records. The organization can identify financial data that is subject to SOX by using data classification, and then put the necessary security measures in place to secure it (*The sarbanes oxley act*).

Export Controls Laws governing export controls impose limitations on the transfer of particular technologies, goods, or services to particular nations. The company can identify data that is subject to export control rules and make sure it complies with these requirements by classifying data(*Ethics, compliance and audit services*).

 The General Data Protection Regulation (GDPR) mandates companies to safeguard the personal information of EU residents and extra territorial effect. The company can identify personal data by classifying it, then put in place with the necessary safeguards to protect it, like encryption, access control, and monitoring (Juliana De Groot on Wednesday December 28 et al.).

* **Proposed classification categories and what they might include.**
* Confidential information  
    
  Consider your company's most valuable assets to be its confidential data. This information might seriously affect your organization's brand and finances if it were to escape your control. Any information that gives your company a competitive edge is considered confidential information. Confidential information is frequently used by companies as the foundation for the rest of their administrative, physical, and technology controls (Johnson, 2022).
* Internal data  
    
  Information considered to be internal poses a moderate risk or potential harm to the company. Along with company rules and other standards, this list also contains confidential information and sensitive credentials (Johnson, 2022).
* Public data  
    
  Any information that is posted on (or intended for) your corporate website is considered public data. Because public material is already intended for the public, there are essentially no repercussions if it is leaked. Some companies might designate a fourth category called "Restricted" for information like credit card numbers, intellectual property, protected health information, etc. and use the term "Confidential" to describe the data that could have an impact on business operations (such vendor contracts and employee evaluations). Whatever category scheme you decide on, try to keep it plain to make category decisions for your data classification policy as simple as possible. Too many selections will ultimately irritate your users and raise the possibility of inaccurate information being labelled (Johnson, 2022).
* **Data retention: why it’s important and how it might be implemented.**

The process of preserving data for future reference or compliance needs is known as data retention. The organization can comply with legal standards like SOX or GDPR and protect institutional knowledge by retaining data, which is important. The types of data that must be retained, the retention periods, and the means of storage and retrieval should all be outlined in data retention rules. To ensure uniform administration of all data types, the new ITAM system should include data preservation policies (Mimecast).

Data and document destruction is the process of securely removing information from storage that is no longer required. To prevent data breaches or unauthorized access to sensitive information, proper document and data deletion is important also for the company to create document and data destruction policies that outline the techniques and steps for securely destroying data. The ITAM solution's document and data destruction policies should include automatic deletion practices (Lowe, 2022).

**● How data classification would integrate with the new ITAM solution**

The new ITAM solution should incorporate data classification to offer a complete asset management system that includes data assets in addition to physical and software assets. A data classification module that enables users to classify data based on defined groups or build custom categories should be included in the ITAM solution. To maintain consistent management of data assets, the ITAM system should also include data retention, document retention, and data destruction policies (IAITAM, 2021).

References

*Data classification policy template*. Netwrix. (n.d.). Retrieved April 28, 2023, from https://www.netwrix.com/data\_classification\_policy\_template.html#:~:text=Scope,on%20any%20type%20of%20media.

*Ethics, compliance and audit services*. UCOP. (n.d.). Retrieved April 28, 2023, from https://www.ucop.edu/ethics-compliance-audit-services/compliance/export-control/export-laws.html#:~:text=Export%20control%20laws%20are%20in,transfers%20of%20export%20controlled%20technologies.

*How data classification benefits your security strategy*. RSS. (n.d.). Retrieved April 28, 2023, from https://www.cavelo.com/blog/benefits-of-data-classification

IAITAM, I. (2021, July 12). *Bringing it asset management and cybersecurity closer*. IAITAM. Retrieved April 28, 2023, from https://iaitam.org/bringing-it-asset-management-and-cybersecurity-closer/

Johnson, B. (2022, December 2). *3 classes of data in your data classification policy*. StrongDM. Retrieved April 28, 2023, from https://www.strongdm.com/blog/data-classification-policy#:~:text=Data%20classification%20generally%20includes%20three,protecting%20your%20most%20critical%20information.

Juliana De Groot on Wednesday December 28, Lord, N., & Brook, C. (n.d.). *What is the General Data Protection Regulation (GDPR)? everything you need to know*. Digital Guardian. Retrieved April 28, 2023, from https://www.digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection

Juliana De Groot on Wednesday February 8. (n.d.). *What is data classification? A data classification definition*. Digital Guardian. Retrieved April 28, 2023, from https://www.digitalguardian.com/blog/what-data-classification-data-classification-definition

Lowe, A. (2022, April 14). *Data destruction: 4 tips for staying compliant*. Access. Retrieved April 28, 2023, from https://www.accesscorp.com/blog/data-destruction-tips-for-staying-compliant/#:~:text=What%20is%20Data%20Destruction%3F,rendering%20the%20original%20material%20unreadable.

Mimecast. (n.d.). *Data retention: Importance of data retention policy*. Mimecast. Retrieved April 28, 2023, from https://www.mimecast.com/blog/why-you-need-a-data-retention-policy/#:~:text=A%20data%20retention%20policy%20defines,critical%20data%20at%20employees%27%20fingertips.

*The sarbanes oxley act*. The Sarbanes Oxley Act. (n.d.). Retrieved April 28, 2023, from https://sarbanes-oxley-act.com/#:~:text=The%20Sarbanes%20Oxley%20Act%20gives,for%20registered%20accounting%20firms%3B%20and