Data Classification & Monitoring

Jim Kreiser, CISA, CRMA, CFSA
Principal – Business Risk Services, State & Local Government IT & Risk Services Leader

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Learning Objectives

At the end of this session, you will:

1. Determine what data classification means for your organization, and what policies should apply.
2. Identify practices and standards related to classifying data and applying roles/responsibilities.
3. Discuss various standards and requirements that may be relevant to how your organization applies data classification.

Intro Question

What do you think when you hear the term “data classification?”

A. Something to make your data more secure
B. Approach to ownership and responsibility of data
C. Something to make your data easier to access and identify
D. Something to protect your data

What is Data Classification?

According to Techopedia.com:

- "Data classification is a diverse process that involves various methods and criteria for sorting and categorizing data into various types, forms or any other distinct class. Data classification enables the separation and classification of data according to data set requirements for various business or personal objectives."

According to Digital Guardian:

- "…the process of organizing data by relevant categories so that it may be used and protected more efficiently."

Regardless of definition – we need to find a workable approach that addresses categorization, aligns with business objectives, and enables more efficient use and protection of data.

Why is Data Classification Important?

- Having proper data classification allows your organization to apply accurate controls based on a pre-defined data category.
  - *Example: An online pamphlet. You want it to be viewable by everyone, you just don't want anyone to edit it. That would take a different level of access. Applying the right level of security required prevents this from happening based on the data classification.*
- Classifying your data can save you time, allowing you to focus on what data is important. It's an important first step in protecting your information security and protecting your company. Taking the time by defining your data classifications and putting the right controls in place can be the difference between a data breach or not.

Other Drives for formal Data Classification?

- *Ensure compliance with data protection requirements*
- *Improve data security practices and policies*
- *End user awareness*
- *Improve efficiency in accessing/retrieving data*
- *Assign roles for data ownership and accountability*
- *Help clarify contractual requirements*
- *Enhance compliance with regulatory requirements or other standards*
- *Help align and foster effective data use, reporting, and access for business objectives or initiatives*
- *Assist in assessment of data disclosure (Right to Know, Sunshine Laws, etc.)*

Broad Strategies

- Need to consider and identify where data resides, as well as where (and with whom) it is transmitted or shared.
  - In today's specialized economy and global marketplace; most organizations have multiple vendors, providers, etc. where data is shared, transmitted, or stored.
  - Determining what types of sensitive data exist within your organization can present challenges. It is an effort that should be organized around business processes and driven by process owners.
- Another important strategic consideration is the process for categorization.
  - Data Classification is NOT an information technology (IT) or information security activity. It is a business data management activity driven by "risk levels".
  - The flow of data into and out of the organization is a key consideration. What about mobile devices? What about emails, printed material, etc.?
  - IT will be involved, but should be responsive based on risk and business objectives.

Consideration Strategies

- Complete a risk assessment of sensitive data.
  - Ensure a clear understanding of the organization's regulatory and contractual privacy and confidentiality requirements. Define your data classification objectives through an interview-based approach that involves key stakeholders, including compliance, legal and business unit leaders.
- Develop a formalized data classification policy.
  - Granular classification schemes tend to cause confusion and become unmanageable. Four to five classification categories are reasonable. Solidify employee roles and responsibilities. Policies and procedures should be well-defined, aligned with the sensitivity of specific data types, and easily interpreted by employees.

Risk Assessment

Data Classification can even assist in the alignment of data owners regarding risk assessments and risk management of datasets. This may help define policies and procedures at category levels for data risk.

Unauthorized Access	Medium	High	High	Immediate Response
Malware	Medium	High	High	Immediate Response
Phishing Attempt	Low	Medium	Medium	High
DDoS Attack	Low	Medium	Medium	High
	Public	**Internal**	**Confidential**	**Restricted**

Risk Assessment

Category	Public	Sensitive	Confidential	Regulatory
I - System Access/ Data Loss	Medium	High	High	Regulatory Response
II - Malware	Medium	High	High	Regulatory Response
III - Acceptable Use Violation	Medium	Medium	High	High
IV - Attempted Information Gathering	Low	Medium	Medium	High
V - Disruption of Service	Low	Medium	Medium	High
VI - Unknown	Medium	Medium	High	High
VII - Exercise				

Data Classification

Complexity?

Data Classification need not be a complex or arduous process.

- Most often, organizations utilize 3-4 categories.
  - Examples include:
    - Internal Use/Business Use
    - Restricted/Confidential
    - Critical
    - Sensitive
    - Public

Consideration Strategies

- Identify and classify data
  - Only after you know where your data is stored can you identify and then classify it so that it's appropriately protected. Consider the penalties associated with a loss or breach. For example, what fines can be levied per record for a HIPAA breach involving protected health information? Insight into the potential costs associated with the compromise of a data set will enable you to set expectations for the cost to protect it and which classification level to set.

Samples

- Definitions for each can vary, but often are synonymous:
  - Critical: Mishandling could result in criminal or civil penalty. Such as theft, invasion of privacy, or similar
  - Restricted: Regulatory, legal, or contractual limitations exist. Access is generally granted on specific authorization and need.
  - Business Use/Internal Use: Operational data, intellectual property
    Restricted; Business Use; Public
  - Public: Data that if requested, or by other directive, could be read/shared with the public. Data that if disclosed, would not be a serious threat to the organization in a reputational or financial manner
- Some models may look like:
  - Restricted; Business Use; Public
  - Critical, Restricted, Internal Use, Public
  - Confidential, Business, Public

Samples

A robust/mature model may look like below:

Data Classification Levels		
Tier	**Type of Data**	**Definition**
1	Open	Data readily available to the public.
2	Public	Data not protected from public disclosure.
3	Government	Data that is not highly sensitive and may be distributed without restriction by law.
4	Confidential	Data protected from disclosure by law, regulation or contract.
5	Restricted	Data that unauthorized disclosure could potentially cause major damage.

As discussed, the models do not need to be this delineated or structured. Your organization should establish a model and definitions that fit your needs, services, and roles.

What To Do With Data Categories?

- Align Data Risks with Business Risk and Objectives
  - For Governments – align data risks with initiatives, projects, or directed services/operations
- Confirm policies and procedures are consistent and supportive of data classification definitions and standards
  - Does the Acceptable Use policy align with Data Classification definitions/assignment?
  - Does the disclosure monitoring and information security policy align with Data definitions?
  - Does IT have data stored, restricted, and accessible in manners consistent with Data definitions?
- Data Catalog
- Asset Handling
- Continuous Monitoring

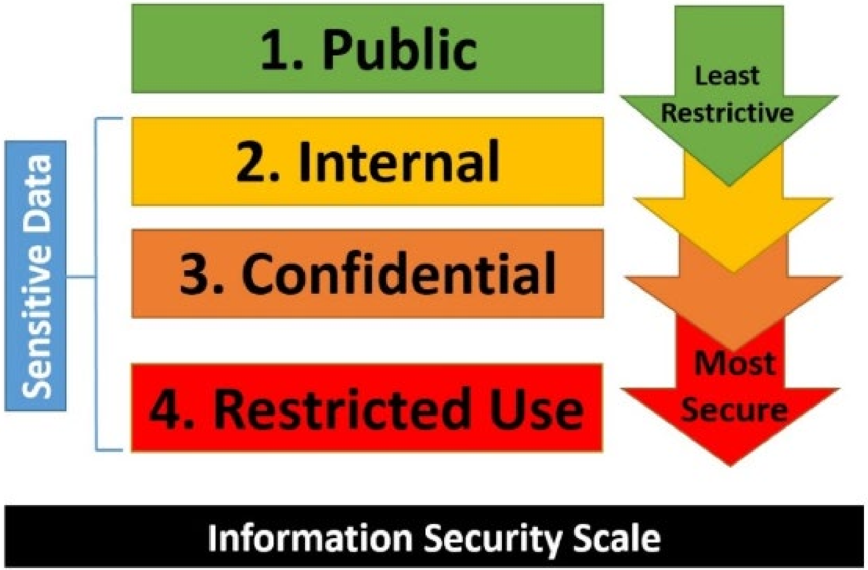
Question

You received credit card information for processing a payment, what type of information is this?

- The answer may depend. PCI and PII data is most typically sensitive/confidential data… but whether it is internal, external, and how it was received may have an impact.

Info Security & Vendors

Use the policy to drive expectations with IT on data security, as well as hold vendors and partners accountable for handling of data.



Consideration Strategies

- Enable controls
  - Establish baseline cybersecurity measures and define policy-based controls for each data classification label to ensure the appropriate solutions are in place. High-risk data requires more advanced levels of protection while lower-risk data requires less protection. By understanding where data resides and the organizational value of the data, you can implement appropriate security controls based on associated risks.
- Monitor and maintain
  - Be prepared to monitor and maintain the organization's data classification system, making updates as necessary. Classification policies should be dynamic. You need to establish a process for review and update that involves users to encourage adoption and ensure your approach continues to meet the changing needs of the business.

Applicability with Data Monitoring

- The standards and classifications/policies developed should (or will) impact Confidentiality, Availability, and Integrity of data.
- Monitoring would include areas of focus such as:
  - Confidential or Sensitive data at Rest & In Transit.
  - Encryption strategies, and monitoring of decrypted data or access (valid and invalid)
    - Alerts for unauthorized access types, escalation?
  - Security baselines and templates should be developed, and notification of any changes to templates noted/monitored
  - Masking tools or products to confidential data
  - Alerts or logging of access to intellectual property or other mission critical data
  - Other examples (changes to financial data?)

Applicability with Data Monitoring

- Each organization must also determine the level of resources and commitment to monitoring controls and activities.
- Establish metrics, baselines, and criteria for security and quality. These should be in accordance with the data classes/types – but also with organizational objectives and "uses".
- What about monitoring of data quality/integrity? Or do we focus on compliance and security monitoring?
  - QA procedures?
  - Review of data, reporting, images, etc. for quality, validity, completeness, etc.
- Data Classification policy(ies) should drive the controls and requirements as well.
- Many systems and tools also… we try not to guide or recommend specifics

What Standards Apply?

Some general standards on data classification do exist overall, including:

- International Organization for Standards (ISO) 27002
- National Institute of Standards & Technology (NIST) 800-60

Other Standards for data will be driven by the nature and type of data:

- HIPAA
- PCI (Account/customer/credit)
- GDPR (EU Citizens)
- State and Federal – (SSN, Taxpayer- https://www.irs.gov/pub/irs-pdf/p4557.pdf).
- Many Other (Higher Education, etc.)

What Steps to Take

Here are some steps to consider getting started with Data Classification (not limited to):

- Receive input from key stakeholders/C-suite
- Define the purpose and scope
- Intra/Inter-Organizational dependencies
- Identify the population of data
- Data classifiers and tagging
- Determine interfaces and connections to data (third party, etc.)
- Identify the data classifications that are relevant
- Develop the policy
  - What procedures will be deployed for monitoring
  - How frequently will data mapping/classification be updated
  - Who will own the policy
  - What security and provisions should IT enforce over data
- Define roles and responsibilities
- Context

Examples

Many illustrative examples exist online. One particular published framework from Indiana University is a nice outline https://datamgmt.iu.edu/types-of-data/classifications.php:

Critical Information Examples:

- SSN
- Domain Passwords
- I9 Paperwork
- Patient Record

Restricted Information Examples:

- Employee Home Address
- Detailed Floor Plans

Public Information Examples:

- Employee Name
- Building Addresses

Jim Kreiser, CRMA, CFSA, CISA
Principal
James.Kreiser@CLAconnect.com
717-857-2613

CLAconnect.com

WEALTH ADVISORY | OUTSOURCING | AUDIT, TAX, AND CONSULTING