

Information Asset Classification Sample Methodologies

The Security Classification Process

(1) Identify information assets

Examples of information assets include, but are not limited to:

- Employee related information including employee records, job applications, and records of interview;
- Procurement records such as RFP specifications, evaluation of proposals, contracts, pricing details, and performance reports;
- Agency documentation such as policies, strategic plans, correspondence, legal advice, financial and audit reports, system documentation, user manuals, training material, operational and support procedures, business continuity plans, system architecture drawings, and risk analyses; and
- Client information including service level agreements, service contracts, client contact records

Information spanning multiple media types or formats must ensure classification requirements are applied to all types of format, to ensure overarching classification control is maintained.

Please note that information asset is not used within this framework to refer to the technology that is used to store, process, access and manipulate information. Information technology assets that are not considered information assets include:

- Software including application and system software, development tools and utilities, and the associated licenses; and
- Physical assets such as computing equipment, storage media, power supplies, air conditions and other technical equipment that may impact the confidentiality, availability or integrity of information resources.

(2) Identify the owner of the information assets

Each agency is responsible for ensuring that information has a security classification and is authorized by the information owner. Information should be classified by the information owner or delegate at the earliest possible opportunity and as soon as the originator or owner is aware of the sensitivity of the information asset.

In the case of information externally generated and not otherwise classified, the agency officer who receives the information should approach his or her own agency information owner or delegate to classify the information and guide its control within the agency.

(3) Impact assessment of information assets

When determining the correct information security classification level for an information asset or domain, a range of considerations needs to be made. Where information can be security classified according to legislation, regulation, policy, contractual or other predetermined means, it should be so classified. For agency information for which the security classification cannot be so determined, an impact assessment matrix should be used to assess the impact of the information asset being compromised, and to guide the determination of the information security classification.

(4) Determine the security classification of the information asset

The highest security classification level determined by the impact assessment must be applied to that asset. When an information asset is classified, it may be possible to determine a specific date or event after which the consequences of compromise might change. An event may trigger an increase or decrease in the sensitivity of the information.

(5) Document security classified information assets in a register

Agencies should establish and maintain a register to record the security classification of each information asset. This register is ideally maintained in a central location and should cover all security classified information assets of an agency so it can be readily accessed. As a minimum, the register should include:

- Name or unique identified or asset or group of assets
- Description of information asset (i.e. what it is about);
- Location of information asset;
- Information owner;
- Security classification of the information asset;
- Date of security classification with details of the authority for the classifier (i.e. who approved the classification)
- Reason for the security classification of the information asset (particularly important to support review and reclassification of the information asset at a later time; should include legislative, regulatory, policy or other reference where applicable, or a copy of the impact assessment date); and
- Date to review security classification (if known).

Additionally, the following information is desirable for highly sensitive or confidential information assets:

- Users and usage of the information;
- Number of copies in circulation and their location; and
- Disposal details where information has been disposed of.

It should be noted that electronic document and records management systems generally contain functionality to record classification metadata for information they manage and may be capable of automatically populating and maintaining a security classified information register for the information they control.

(6) Education and awareness

The ongoing education and awareness of all employees in the importance of security classifying information is critical to the success of the overall agency security environment. The agency should ensure that all employees who create, process, or handle security classified information have a clear understanding of the agency classification policies and procedures and of their responsibilities.

(7) Maintain security classification information register – continuous review

As environments and circumstances change, information owners may choose to review security classifications to ensure that the protection being afforded the information is cost-effective and commensurate with the level of risk. Information owners should use the security classification information register to annually review the security classification of information assets.

Assignment of Impact Levels and Security Categorization

(1) Mapping Information Types to Security Controls and Impact Levels

1. Identify information systems. An information system may be a general support system, a major application, or a local or special purpose system. Agencies should develop their own policies regarding system identification for security categorization purposes. The system is generally bounded by a security perimeter.
2. Identify information types. The user should identify all of the information types that are input, stored, processed, and/or output from each system.
3. Select provision impact levels. The user should select the provision impact levels for each identified information type.
4. Review and adjust provisional impact levels. The user should review the appropriateness of the provision impact levels recommended for the user's information types based on the organization, environment, mission, use, and connectivity associated with the system under review. After reviewing the provisional impact levels, adjustments should be made to the impact levels as appropriate.
5. Assign system security category. The user now establishes the level of confidentiality impact, integrity impact, and availability impact associated with the system under review. The adjusted impact levels for information types are reviewed with respect to the aggregate of all information processed in or by each system. In some cases, the consequences of loss of confidentiality, integrity or availability of the information aggregate can be more serious than that for any single information type. In addition, a system's access control information and the system software that protects and invokes it can both affect the integrity and availability attributes of a system and even access to other systems to which the system under review is connected.

(2) Information Type Identification

The following is a suggested methodology that can be employed for identification of information types:

- Identify the fundamental business areas (management and support) or mission areas (mission-based) supported by the system under review;
- Identify, for each business or mission area, the operations or lines of business that describe the purpose of the system in functional terms;
- Identify the sub-functions necessary to carry out each area of operations or line of business;
- Select basic information types associated with the identified sub-functions; and where appropriate,
- Identify any information type processed by the system that is required by statute, executive order, or agency regulation to receive special handling (e.g., with respect to unauthorized disclosure or dissemination). This information may be used to adjust the information type or system impact level.

"Business areas" separate government operations into high-level categories relating to the purpose of government, the mechanisms the government uses to achieve its purposes, the support functions necessary to conduct government operations, and resource management functions that support all areas of the government's business. "Business areas" are subdivided into "areas of operation" or "lines of business."

"Areas of operation" or "lines of business" describe the purpose of government in functional terms or describe the support functions that the government must conduct in order to effectively deliver services to citizens. Lines of business relating to the purpose of government and the mechanisms the government uses to achieve its purposes tend to be mission-based. Lines of business relating to support functions and resource management functions that are necessary to conduct government operations tend to be common to most agencies.

"Sub-functions" are the basic operations employed to provide the system services within each area of operations or line of business.

Although this guideline identifies a number of information types, only a few of the types identified are likely to be processed by any single system. Also, each system may process information that does not fall neatly

into one of the listed information types. Once a set of information types is identified, it is prudent to review the information processed by each system under review to see if additional types need to be identified for impact assessment purposes.

(3) Selection of Provisional Impact Levels

Agencies can assign security categories to information types and information systems by selecting and adjusting appropriate values for the potential impact of compromises of confidentiality, integrity, and availability. Those responsible for impact selection and subsequent security categorization should apply the criteria to each information type received by, processed in, stored in, and/or generated by each system for which they are responsible. The security categorization will generally be determined based on the most sensitive or critical information received by, processed in, stored in, and/or generated by the system under review.

(4) Review and Adjustment/Finalization of Information Impact Levels

Particularly where security categorization impact levels are adopted as provisional levels, the agency should review the appropriateness of the provisional impact levels in the context of the organization, environment, mission, use, and connectivity associated with the system under review. The confidentiality, integrity, and availability impact levels may be adjusted one or more times in the course of the review. Once the review and adjustment process is complete for all information types, the mapping of impact levels by information type can be finalized. The impact of compromise of information of a particular type can be different in different agencies or in different operational contexts. Also, the impact for an information type may vary throughout the lifecycle.

(5) System Security Categorization

Once the impact levels have been selected for individual information types processed by a system, it is necessary to assign a system security category. Determining the security category of an information system requires additional analysis and must consider the security categories of all information types resident on the information system. For an information system, the potential impact values assigned to each of the respective security objectives (confidentiality, integrity, availability) are the highest values for any one of these objectives that has been determined for the types of information resident on the information system.

Information systems are composed of both programs and information. Programs in execution within an information system (i.e., system processes) facilitate the processing, storage, and transmission of information and are necessary for the organization to conduct its essential mission-related functions and operations. These system-processing functions also require protection and could be subject to security categorization as well. However, in the interest of simplification, it is assumed that the security categorization of all information types associated with the information system provide an appropriate worst case potential impact for the overall information system, thereby obviating the need to consider the system processes in the security categorization of the information system.

The impact level for a system will generally be the highest impact level for the security objectives (confidentiality, integrity, and availability) associated with the aggregate of the system information types. An information system usually processes several information types (e.g., privacy, medical, proprietary, financial, contractor sensitive). Each of these information types is subject to security categorization. Various stakeholders (e.g., management, operational personnel, or security experts) may need to be involved in decisions regarding system-level impact assessments. Information aggregation, critical system functionality and other factors should be considered in making system-level impact decisions.

Guidelines for Assignment of Impact Levels to Mission-Based Information

(1) Mission-based Information

Mission-based information types are, by definition, specific to individual departments and agencies or to specific sets of departments and agencies.

(2) Identification of Mission-based Information Types

Government acquires, generates, processes, and stores a wide variety of information types. The first step in mapping types of government information and information systems to security objectives and impact levels is the development of an information taxonomy, or creation of a catalog of information types. One issue associated with the taxonomy activity is the determination of the degree of granularity. If the categories are too broad, then the guidelines for assigning impact levels are likely to be too general to be useful. On the other hand, if an attempt is made to provide guidelines for each element of information processed by each government agency, the guidelines are likely to be unwieldy and to require excessively frequent changes.

Much government information and many information systems are used directly for the provision of services. One approach to establishing mission-based information types at an agency level is to begin by documenting the agency's business and mission areas. Then the major sub-functions that are necessary to the conduct of each business and mission area can be defined. For example, one mission conducted by an agency might be law enforcement. Sub-functions that are part of the agency's law enforcement mission might include criminal investigation and surveillance, criminal apprehension, criminal incarceration, citizen protection, crime prevention, and property protection. Each of these sub-functions could also represent an information type.

The owner of each system, or an individual designated by the owner, is responsible for identifying the information types stored in, processed by, or generated by that system. In the case of mission-based information, the responsible individuals, in coordination with management, operational, and security stakeholders, should compile a comprehensive set of lines of business and mission areas conducted by the agency, as well as the functions and sub-functions necessary to conduct agency business and/or accomplish agency missions. Each sub-function of a line of business or mission area corresponds to an information type.

(3) Impact Assessment for Mission-based Information

Direct service missions provide the primary frame of reference for determining the impact levels and security objectives for mission-based information and information systems. The consequences of unauthorized disclosure of information, breach of integrity, and denial of services are defined by the nature and beneficiary(ies) of the service being provided or supported.

Using impact selection criteria for the security objectives and types of potential losses, the entity responsible for impact determination must assign impact levels and consequent security categorizations for each mission-based information type identified for each system. The final system security categorization is based on the impact levels for each information type stored in, processed by, or generated by the system.

A factor specific to the confidentiality objective is information subject to special handling. Regardless of other considerations, some minimum confidentiality impact level must be assigned to any information system that stores, processes, or generates information subject to statutory and regulatory specifications.

Impact Levels by Type for Management and Support Information

(1) Management and Support Information

Much government information and many systems are not employed directly to provide services to citizens, but are primarily intended to manage resources or support delivery of services:

- Support functions necessary to conduct government (support delivery of services); and
- Resource management functions that support all areas of government's business (management of resources)

The support delivery of services and management of resources business areas are common to most government agencies.

(2) The first step in mapping types of management and support information and information systems to security objectives and impact levels is to identify the information types stored in, processed by, or generated by the system.

(3) The next step is to select the levels of impact and consequent security category for each application information type. System security categorization is based on the impact levels associated with each security objective for each type of information stored in, processed by, or generated by the system plus additional factors governing determination of system level impact.

(4) Services Delivery Support Information

These service support functions are the day-to-day activities necessary to provide the critical policy, programmatic, and managerial foundation that support state government operations. The direct service missions and constituencies ultimately being supported by service support functions comprise a significant factor in determining the security impacts associated with compromise of information associated with the support delivery of services business area.

- **Controls and Oversight** information is used to ensure that the operations and programs of the government and its external business partners comply with applicable laws and regulations and prevent waste, fraud, and abuse.
 - Corrective Action
 - Program Evaluation
 - Program Monitoring
- **Regulatory Development** information supports activities associated with providing input to the lawmaking process in developing regulations, policies, and guidance to implement laws.
 - Policy and Guidance Development
 - Public Comment Tracking
 - Regulatory Creation
 - Rule Publication
- **Planning and Resource Allocation** information supports the activities of determining strategic direction, identifying and establishing programs and processes to enable change, and allocating resources (capital and labor) among those programs and processes.
 - Budget Formulation
 - Capital Planning
 - Enterprise Architecture
 - Strategic Planning
 - Budget Execution
 - Workforce Planning

- Management Improvement
- **Internal Risk Management and Mitigation** information supports all activities relating to the process of analyzing exposure to risk and determining appropriate counter-measures. Risks to much information associated with internal risk management and mitigation activities may inherently affect the resistance to compromise/damage and recovery from damage with respect to a broad range of critical infrastructures and key assets.
 - Contingency Planning
 - Continuity of Operations
 - Service Recovery
- **Public Affairs** information supports activities involving the exchange of information and communication between the government, citizens and stakeholders in direct support of citizen services, public policy, and/or state interest.
 - Customer Services
 - Official Information Dissemination
 - Product Outreach
 - Public Relations
- **Revenue Collection** information includes the collection of government income from all sources.
 - Debt Collection
 - User Fee
 - State Asset Sales
- **Legislative Relations** information supports activities aimed at the development, tracking, and amendment of public laws through the legislative branch of government.
 - Legislation Tracking
 - Legislation Testimony
 - Proposal Development
 - Legislative Liaison
- **General Government** information supports the general overhead costs of the state government, including legislative and executive activities; provision of central fiscal, personnel, and property activities; and the provision of services that cannot reasonably be classified in any other service support area. Generally, all activities closely associated with other service support areas or information types shall be included in those service support areas or information types rather than listed as part of general government. This service support area is reserved for central government management operations; most agency-specific management activities would not be included here. However, unlike other service support functions, some general government information types are associated with specific organizations.
 - Central Fiscal Operations
 - Legislative Functions
 - Executive Functions
 - Central Property Management
 - Central Personnel Management
 - Taxation Management
 - Central Records and Statistics Management
 - Income Information
 - Personal Identity and Authentication

- Entitlement Event
- Representative Payee

(5) Government Resource Management Information

The government resources management information business area includes the back office support activities that enable government to operate effectively. Many departments and agencies operate their own support systems. Others obtain at least some support services from other organizations. Some agencies' missions are primarily to support other government departments and agencies in the conduct of direct service missions. Security objectives and impacts for administrative and management information and systems are determined by the nature of the supported direct services and constituencies being supported.

- **Human Resources** information supports all activities associated with the recruitment and management of personnel.
 - Benefits Management
 - Personnel Management
 - Payroll Management and Expense Reimbursement
 - Resource Training and Development
 - Security Clearance Management
 - Staff Recruitment and Employment
- **Administrative Management** information supports the day-to-day management and maintenance of the internal infrastructure. Administrative information is usually routine and is relatively low impact. However, some administrative management information is either very sensitive or critical.
 - Facilities, Fleet and Equipment Management
 - Help Desk Services
 - Security Management
 - Travel Information
 - Workplace Policy Development and Management
- **Information Technology Management** information supports the coordination of information technology resources and systems required to support or enable a citizen service. Impacts to information associated with the operation of information technology systems generally need to be considered even when all mission-related information processed by the system is intended to be available to the general public. The relevant issues may be different for integrity and availability than for confidentiality.
 - System Development
 - Lifecycle/Change Management
 - System Maintenance
 - Information Technology Infrastructure Management
 - Information Technology Security
 - Record Retention
 - Information Management
- **Financial Management** information supports the aggregate set of accounting practices and procedures that allow for the accurate, efficient, transparent, and effective handling of all government revenues, funding, and expenditures. Confidentiality impacts associated with financial management information are generally associated with the sensitivity of specific projects, programs, and/or technologies that might be revealed by unauthorized disclosure of information. Integrity breaches such as successful frauds can affect agency image. Permanent loss/unavailability of financial management information can cripple agency operations.

- Assets and Liability Management
- Reporting and Information
- Budget and Finance
- Accounting
- Payments
- Collections and Receivables
- **Supply Chain Management** information supports the purchasing, tracking, and overall management of goods and services.
 - Goods Acquisition
 - Inventory Control
 - Logistics Management
 - Services Acquisition

National Institute of Standards and Technology, "Guide for Mapping Types of Information and Information Systems to Security Strategies", Special Publication 800-60 (June 2004)

An Approach to Data Classification in an ILM Framework

Abstract

Data classification is a critical component in any information lifecycle management (ILM) strategy. This document outlines an eight-step data classification methodology that can be used on any data generated in an organization. The following data classification process can help your organization obtain the analytics required to fully and systematically apply the ILM cube framework

(1) Determine Information Classification Inputs

- Security Protection – Based on security organization requirements. What degree of access to the data does your organization need? How isolated does the data need to be?
- Performance – Based on input from application developers. Those who actually create the applications that generate, store, and retrieve the data must specify input/output and nominal response times for that data. In other words, how quickly does the data need to be accessed?
- Availability – Based on application user requirements. For those who need to access the data to perform daily duties, continuity of delivery is a primary concern. The delivery is normally outlined in service level agreements that describe the guaranteed availability of data. Those SLAs will help guide you as to the data's criticality.
- Recoverability – Based on operations and disaster recovery requirements. Recoverability describes just what data your organization needs to be able to get back in the event of a problem. There are four common components to recoverability:
 - Recovery time objectives
 - Recovery point objectives
 - Recovery capability objectives
 - Granularity of recovery
- Scalability – Based on infrastructure and budgeting organization's requirements. Scalability addresses the anticipated growth of the file or database being stored. Will the amount of data be very dynamic or largely static?
- Application Profile – Based on business owner's requirements. The application profile takes into account the use to which your organization puts the data being stored. For example, identify whether it is internal, customer-facing, or part of a business-to-business relationship. Depending on the data's use, it may be subject to internal information policies and standards or even to regulatory compliance. If data is mission-critical, consider assigning it a higher rating.
- Lifecycle – Based on aging patterns established by developers. This last element addresses the value of the information as it decays over time.

(2) Identify Business Owners

In identifying business owners, apply a line-of-business focus, and always keep in mind that data ownership is not an IT responsibility. However, gathering data about business functions, applications, and how the application uses IT is key. To ensure an actionable plan, stakeholders at several management levels must be part of the process.

(3) Inventory Applications by Business Unit and Type

Inventory is a two-step process:

1. Inventory and categorize applications by department.
2. Organize the categories in terms of the inputs chosen from Step 1.

Poll the application owners and – if it hasn't already been done – create an application requirements analysis. The analysis should cover IT facilities and application systems.

(4) Use Business Impact Analysis Methodology to Assign Data Value

A business impact analysis is an excellent way to define and measure the information value of data to your organization, as well as to establish business continuity requirements. You can use a formal business impact analysis or informal classification process to:

- Identify the critical applications and quantify, in monetary terms, the impact of loss
- Identify critical business functions and the computer systems required to support them
- Identify the impact on other systems and lines of business if the computer systems required to support these critical business functions are not available
- Quantify the monetary impact if critical business functions cannot be performed due to a loss of required systems (cost per hour of downtime)
- Identify intangible impacts that would result if critical business functions cannot be performed due to a loss of required systems (e.g., loss of public confidence, violations of regulations and tariff agreements, damage to future business)
- Determine the recovery time frames required of the systems supporting their critical business functions in the event of a loss of these systems
- Identify the adequacy of existing business continuity plans, systems and processes for each critical business function and application

(5) Establish Data Management Goals

Begin by setting up a cross-functional information lifecycle management steering group. The team should clearly define an unambiguous and simple set of data classification goals. These goals should produce a framework and model that can then be used to drive information lifecycle management strategies. To help with goal setting, first create a high-level classification matrix – a horizontal view of the application of enterprise data, business processes, business objectives, and logical state and physical state classifications. Questions to ask include:

- How many different types of business data does the organization support?
- What are the possible logical groupings of data?
- What is the longest duration we must keep information?
- What storage assets do we possess?

(6) Define Lifecycle Classification and Data Management Process

(7) Set Initial Classification and Lifecycle

Sun Microsystems, "An Approach to Data Classification in an ILM Framework" Application Note (October 2005)

Information Inventory Checklist

This is intended to be a list of questions which agencies should consider in their information inventory planning.

- (1) What information is **collected** from other agencies?
- (2) What particular **technologies** or **methods** (business systems) are used to collect the information?
- (3) Is the information collected specifically, or is it a by-product of some other operation?
- (4) Is the information **collected** by a different function or process other than the business operation or process that produces it?
- (5) What is the **frequency** with which the information is collected / stored / accessed / used / disposed?
- (6) **Who** collects / supplies the information?
- (7) Are there any **constraints** or difficulties associated with the collection of the information?
- (8) What **business rules** or constraints are associated with the information?
- (9) What **metadata** and conceptual information exists?
- (10) How is the information **described**? What is its definition?
- (11) What physical **form** does the information take?
- (12) What is the **type** of information (text, number, formatted / unformatted)?
- (13) At what **physical location** is the information held?
- (14) What is the size of or how much **storage** is required by the information?
- (15) Who are the **users** of the information? What organizational sections or **business units** are they in? Are they external users? What business function or functions does the information support?
- (16) At what **organizational levels** do the information users work?
- (17) At what organizational level is the information relevant (e.g., is it operational, monitoring or strategic)? Is the information targeted and **used** by the correct organizational level?
- (18) What **resources** are used to collect / store / access / use / dispose of the information?
- (19) What **budget** allocation is associated with information collection / storage / access / use / disposal? (Who pays for it, what fund?)
- (20) Who is the **custodian** of the information within the agency?