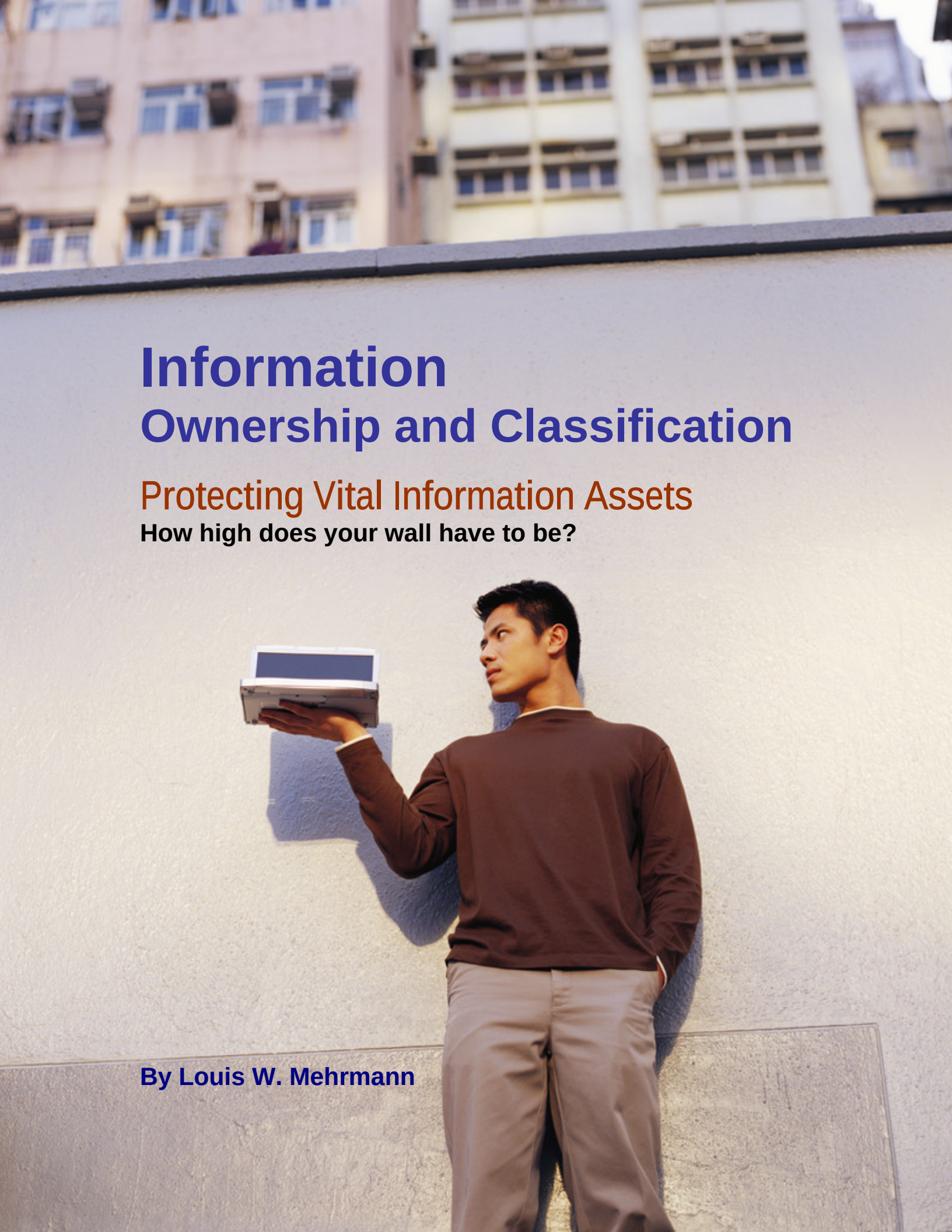
Information
Ownership and Classification

Protecting Vital Information Assets

How high does your wall have to be?



By Louis W. Mehrmann

INDEX

"Prepare for the Worst and Enjoy the Fruits of Your Labor"

- ANONYMOUS

Information is a vital asset for the success of any organization. It is therefore necessary to protect that asset from accidental or intentional, but unauthorized, disclosure, modification, destruction, or inability to process that information

DEFINITIONS:

- **"INFORMATION ASSETS"** is recorded information of value to the organization
- **"DISCLOSURE"** deals with secrecy or confidentiality.
- **"MODIFICATION"** involves integrity.
  The information is actually what it is supposed to be.
- **"DESTRUCTION"** deals with backup and disaster recovery issues.
- **"INABILITY TO PROCESS"** deals with information systems issues.

List Information Assets That If Disclosed Could Benefit Your Competitors

List Information Assets Where Integrity is of Utmost Importance

List Information Assets That If Destroyed Would Do the Most Harm

List Information Assets That Must Be Processed in a Timely Manner

In order to define protection for information assets, it is necessary to assign responsibility for the assets

OWNERSHIP
Defines responsibility

LIST THE OWNERS OF YOUR ORGANIZATION'S INFORMATION ASSETS

_____
_____
_____
_____
_____

Employees and others need to know the level of protection required for a selected set of information.

CLASSIFICATION
Defines protection levels

If you have a Classification Process, then List the Levels used:

_____
_____
_____
_____
_____

Are All of Your Employees Aware of Your Asset Classifications?

YES: _____ NO: _____

Ownership

An owner is that individual manager or representative of management who has the responsibility for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset.

Responsibilities:

- ✓ Identify information and acknowledge ownership
- ✓ Classify the information
- ✓ Specify business controls
- ✓ Authorize access
- ✓ Assign custody
- ✓ Approve application controls
- ✓ Perform or participate in risk assessment & acceptance
- ✓ Develop contingency plans
- ✓ Monitor compliance and review periodically

Identification and Ownership Acknowledgement

All managers have the responsibility to identify "Information Assets" which require a designated owner – and to acknowledge those assets that fall under their control. The manager then has the responsibility either to assign a specific person or to accept ownership personally when appropriate.

Sometimes the individual owner may not be obvious, and management may have to assign ownership arbitrarily. In the absence of other information, it is reasonable to presume that the author is the owner. Still, there should be a "default rule", like "If you have possession of it, and you cannot show evidence of another person as the owner, you are the owner."

Business Controls

The owner should be in a better position then anyone else to understand the overall relationship of the asset to the organization. Therefore, the owner would ordinarily specify requires business controls beyond those already required by the organization.

Access Authorization

Access to information should be limited to authorization by the owner of the information. It is reasonable to delegate responsibility of a specific function as part of the design of the application; for example, the owner of the vendor file may not personally approve every new vendor added to the file. There may be hundreds of managers doing that. The owner *must* be certain that the controls are in place to ensure that only vendors with proper approval and authority are in the file.

Custody

The owner, either directly, or indirectly through application systems design, makes the decision about who should have custody of the information.

Application Controls

The owner must be involved in the application development process and review those controls built into the application that affect the information.

Risk Assessment/Acceptance

When it is not feasible to meet all of the requirements for protection, the one with the best perspective of the overall effect on the business should be the owner. The owner or the owner's management should be the decision maker. The application project team should drive the risk assessment process for new applications and changes to existing applications. The decision to accept a risk should be a valid business judgment. Lack of resources to correct the problem is *not* justification for risk acceptance.

Contingency Planning

The owner should have final responsibility for contingency planning at it relates to their information.

Compliance Monitoring

While the owner may not be technically qualified to monitor the detailed processes, particularly as they relate software and applications, it is still the owner's responsibility to do whatever is necessary to gain a level of confidence that the requirements set down are enforced. This could take the form of a team review on a periodic basis, or ensuring timely internal audits. Some review should take place annually at minimum.

Classification

Classification of information is its systematic labeling to indicate a specific set of protective controls based on its sensitivity to destruction, modification, and disclosure.

Sensitivity to destruction

- Information that the organization requires to continue functioning
- *Examples:* Vital Records, Disaster Recovery Plans

Sensitivity to modification

- **Information where compromised integrity have adverse effects**
- *Examples:* Fraud sensitive programs, payroll, expense, revenue

Sensitivity to disclosure

- **Information of a proprietary nature that if revealed could cause harm**
- *Examples:* New product plans, reorganization plans, price changes

Why Classify?

Except in the smallest of organizations, a formal documented classification system is appropriate for a number of reasons.

- ✓ **Efficiency:**
  If all information were treated the same, the results would be some being overprotected and some being under protected. Lack of classification scheme, requires each user make judgments about how information is to be treated. Since users are likely to know less about the sensitivity of data than owners are, they are not well equipped to make that decision. A classification program should ensure that the person that should know best what it should be makes the decision only once.

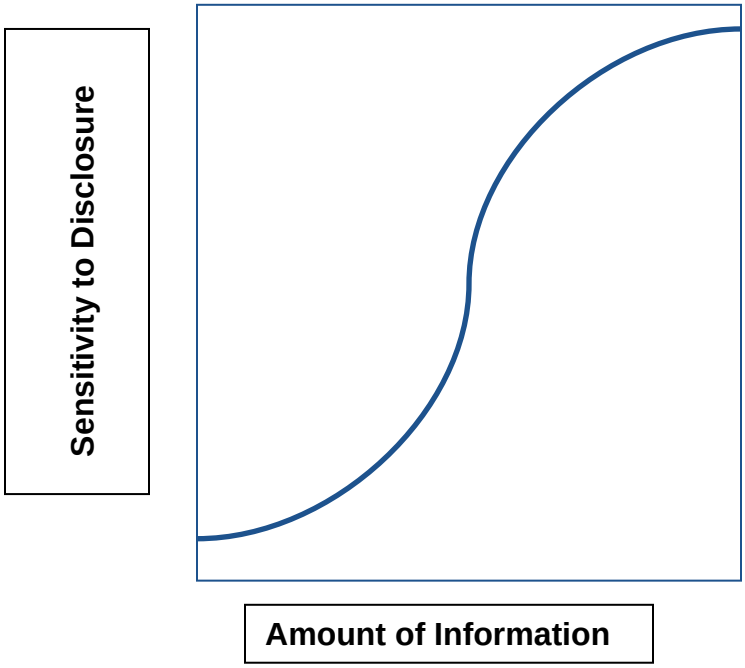
- ✓ **Legal Implications:**
  The owner may be required to show that appropriate action was taken to protect the information If information is destroyed, modified, or disclosed without authorization. One positive step is a formal classification system with evidence that employees are aware of the meaning of each classification and the protective measures that are in place for each classification.

- ✓ **Costs:**
  Either under-protection or overprotection could be very expensive. Under-protection may result in losses above the costs of proper controls, or the controls would not be justified. Overprotection (at its extreme) would require that all assets of the organization receive the same level of protection. Good balance requires cost effective protection against risks and a good classification program can help provide such protection.

Classification System Characteristics

- Classification determines controls and are unique to the organization
- The *number* of classifications, the specific *rules* and *controls*, and various other *requirements* need to be carefully designed to meet the needs of the organization
- Classification is assigned by the owner (or authorized designee)
- Selection of classification is a subjective judgment based on how sensitive the owner thinks the information is
- Based on that judgment, the owner maps the sensitivity against a set of rules for each classification to select the closest fit
- The selection is then based on that closest fit and other considerations (i.e., balancing cost and protection)

Information Characteristic

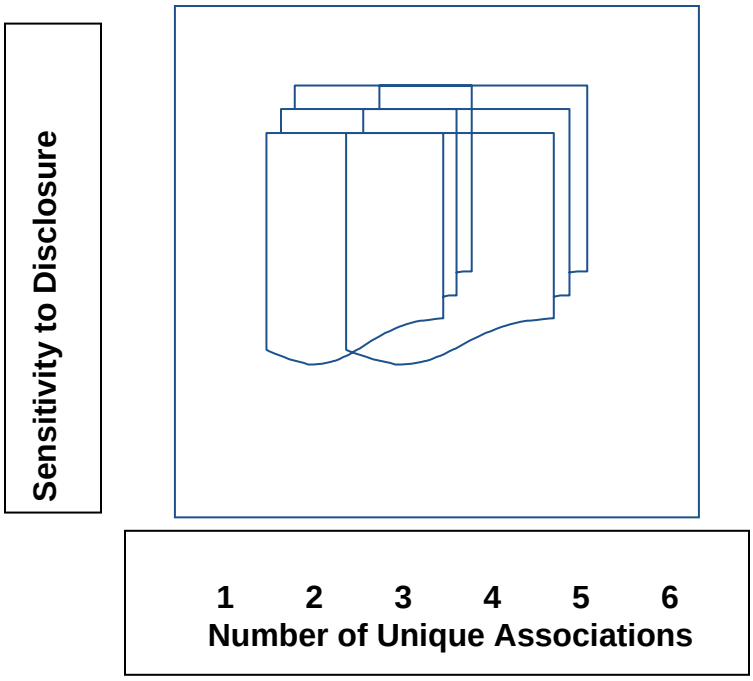


Quantity:

Depending somewhat on the type of information, a small amount may present little risk while a larger amount could be significant.

Example: A product on order for a given customer versus all of the orders for that product for a geographic area, which could give a competitor key marketing information.

Information Characteristic

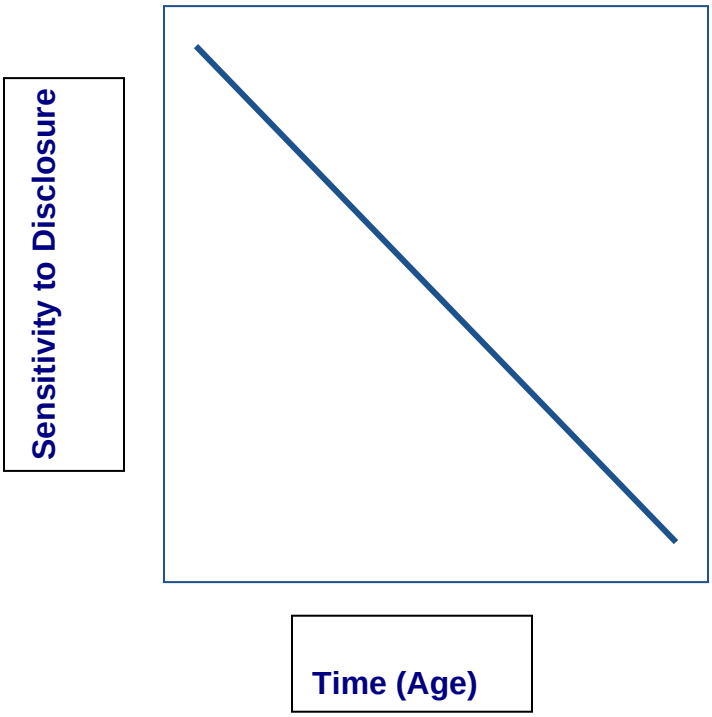


Context:

This deals with the number of unique associations, or the *context* in which you find the information.

Example: A list of engineering drawing numbers for unannounced products may not be very sensitive. However, as we associate that list with additional information such as title of the drawing, the date, an unannounced product's name, and cross reference to other drawings, sensitivity of the data increases.

Information Characteristic

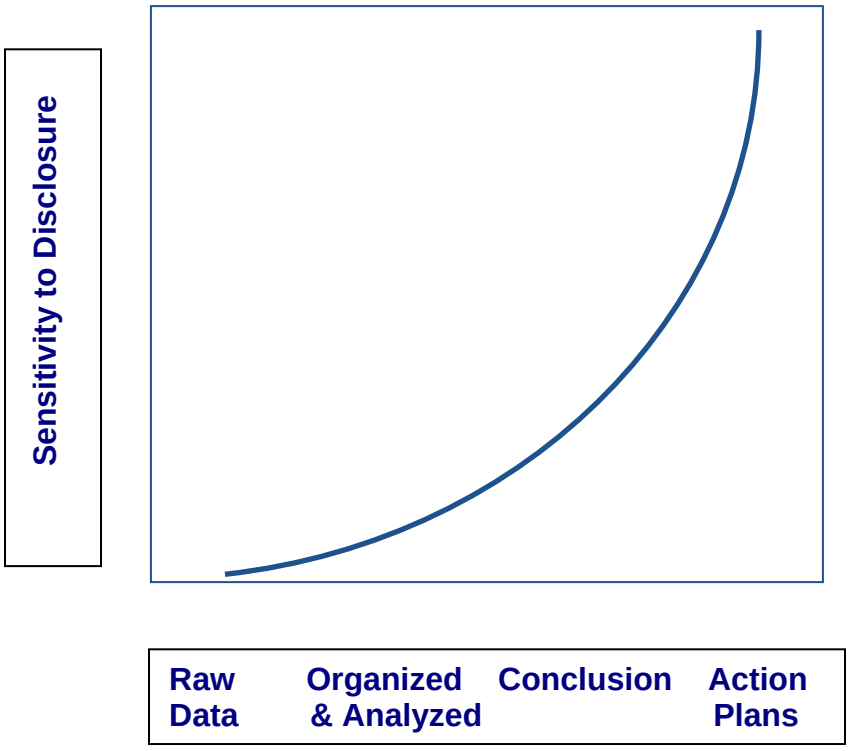


Currency:

Pay attention to timeliness in classification. Older information approaching the time when it could be declassified tends to be less sensitive to disclosure.

Example: The day after the announcement of a new product, information about it is not nearly as sensitive as it was two years prior to announcement.

Information Characteristic



Meaning:

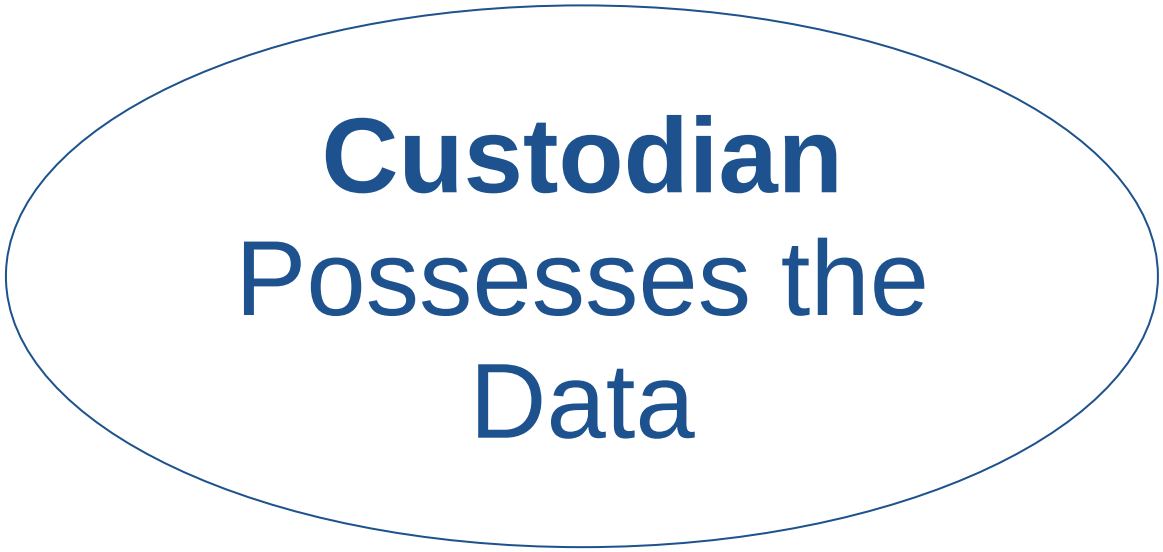
The difference between raw data and the concisely reduced information drawn from it is significant.

Example: Raw data from oil company seismic readers is less sensitive than the correspondence about company plans on the utilization of that data.

Other Important Roles

Custodians:

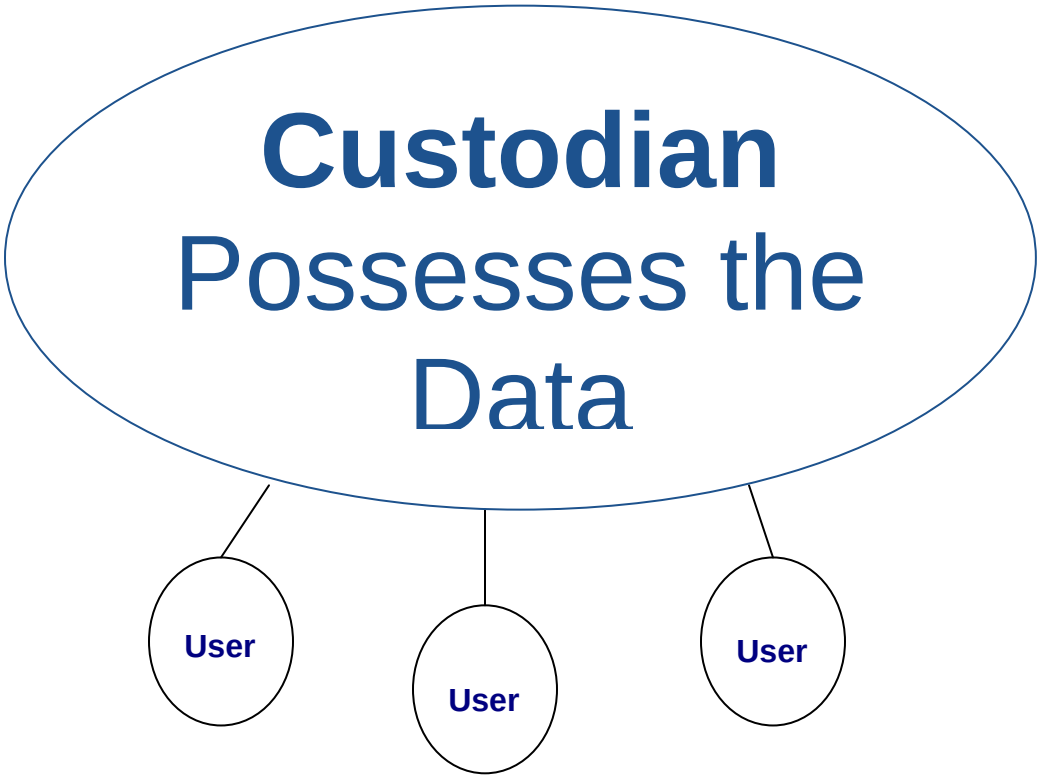
A *custodian* has possession of the information under authorization from the owner and is responsible to follow the controls specified by the owner. From a practical viewpoint, it is reasonable to develop rules jointly if the custodian is the supplier of Information Systems Services.



Other Important Roles

Users:

The *user* has authorized access to the information, and allowed to update it or add new data. *Users* have the responsibility to follow a set of simple and standard procedures issued by the owner and the custodian. Bring any requirements for decisions that fall outside these rules to the attention of management. Reserve the decisions for the owner or custodian.



Other Important Roles

Auditors:

As management's representative for ensuring adherence to policies and standards, the *internal auditor* must include tests for proper classification and labeling in audit reviews. Along with self-assessments by owners, and peer reviews of Information Systems facilities, the auditor is a key player in assuring compliance with policy.

- **Review**
- **Assess**
- **Evaluate**

Document & Report

- **Findings**
- **Recommendations**

Classification Structure

When implementing an ownership and classification process in an organization, consider the structure for the classification scheme relating to information disclosure. Select the structure that best fits the organization. There are three basic schemes:

1. **Levels: In the classification "level" on hierarchical scheme, a set of levels is selected which starts with the lowest level (usually "Public" or "Unclassified") up to the highest, the maximum level of secrecy.**

An example of higher classifications above Unclassified could be:

- ❑ Internal Use Only
- ❑ Confidential
- ❑ Confidential Restricted
- ❑ Registered Confidential

Each classification level would require a corresponding documented set of guidelines followed by both custodians and users.

Classification Structure

2. Categories: The non-hierarchical or "category" classification is for similar, independent collections of protected information resources with similar handling procedures. Different categories have no relationship or dependency on any other categories.

An example of categories could be departments, projects, functions, or other groupings that require closed access.

3. Mixed: Some business use a combination of both hierarchical and non-hierarchical categories. The result is a grid or table with combinations of possible levels and categories. The classification level is usually required with classification category as an option for complete classification.

An example of this mixed scheme is the model used by the Department of Defense, which in some implementations requires all users who access protected information to have a corresponding clearance.

Classification Basics

- Information classification applies to "*All Media*"
- A record is defined as any information captured in reproducible form such as documents, books, photographs, films, sound recordings, documents, magnetic cards, magnetic tapes, floppy disks, Memory Sticks, CD, CD-R, SD, DVD, etc.

Sample Classification Ground Rules

- Classification of information may vary within a record and each page of Information classified according to its content. Classification must appear prominently in a location where binding or stapling will not obscure it.
- The entire record must be prominently and externally classified and when there is information of varying content within a record, classification assigned to the composite must be the highest contained anywhere within the record.
- Transmittal letters and memoranda which obscure the classification when attached to classified records, document binders, tape reels, discs, or any other Container prominently reflect the classification of the attachment.
- Prohibit preprinting classification on blank media unless known in advance that the information required by the form is classified information, such as a personnel profile.

Sample Guidelines

- "For Internal Use Only"
- "CONFIDENTIAL"
- "RESTRICTED"
- "REGISTERED CONFIDENTIAL"

Internal Use Only Sample Guidelines

Description: This classification is for information that, because of its personal, technical, or business sensitivity, must be restricted to use within the organization and for purposes related to the business endeavors or purpose of the organization and records classified but fail to meet the specific need for higher classification.

Examples: Examples include some procedures and guidelines, organization charts, manager's manuals, internal telephone directories, code names when used alone, etc.

Responsibilities During Creation or Generation: Having made the decision that this is the proper classification, ensure that the classification appears on each page, screen, or part (i.e. disk, tape, microform frame, video display, etc.)

Use: Within the organization, there are no controls over the disclosure, transmittal, or copying of Internal Use Only information. Locking away is a local option.

Mail: Internally, no envelope required. If desired, use multi-purpose envelope. Externally, seal in unclassified envelope.

Travel: Travel across national boundaries with *technical information* requires approval of appropriate legal and patent functions.

Disclosure Outside the Organization: Management responsible for the ownership of Internal Use Only information may permit selected distribution outside the organization.

Confidential Sample Guidelines

Description: Information classified Confidential must have one or more of the following attributes:

1. **Provide the organization a competitive edge.**
2. **Be of such nature that unauthorized disclosure would be against the best interests of the organization or an individual.**
3. **Relate to or describe a portion of the organization's business.**
4. **Show operational direction over a short term.**
5. **Be important to the technical or financial success of the business.**

Examples: Various Categories of information exist such as:

1. Summaries of financial data relating to the organization's operations or position, such as cash, inventories, investments, depreciation policies, engineering expenditures, manufacturing costs and royalty payments.
2. Revenue, cost, profit, or other financial results to one of the organization's divisions or subsidiaries
3. Disclosure of overall product or feature structure and unannounced product designation
4. Maintenance, performance, or servicing characteristics of a product
5. Information on a product's interfaces with other products
6. Information defining special processes or criteria used in a product's manufacture
7. Information concerning personnel matters, including that which relates to a specific individual such as correspondence or forms about salary, appraisal, or career path

Responsibilities During Creation or Generation: Having made the decision that this is the proper classification, ensure that the classification appears on each page, screen, or part (i.e. disk, tape, microform frame, video display, etc.)

Use: Secure Confidential information under a standard, security approved lock. If It may be copied, assign only to users with a business need to know. Ensure distribution lists are valid reflecting current need to know status.

Transmission: Limit the transmission of confidential information over unencrypted and controlled networks, message systems and facsimile devices. Encryption is required for telegrams and other external services involving handling and store and forward operations. Transmission should occur only if the recipient site maintains required security controls. Avoid facsimile transmission of personnel data (if required, sending and receiving locations must ensure that only authorized personnel can view or receive messages.

Mail: Used sealed envelopes and mark the envelopes with the "Confidential" classification. Use double envelopes by inserting the envelope bearing the confidential classification into a second envelope with no classification.

Telephone Calls: Verify the business need to know and identity of the recipient prior to releasing "Confidential" information to other employees.

Meetings: Announce that the subject is Confidential, verify attendee's need to know, and ensure meeting area physical security. Presenters must indicate what is appropriate for recording.

Travel: Avoid traveling with confidential information. When possible, mail the information ahead. Individuals transporting confidential records are responsible for their protection while in their custody. Travel across national boundaries with *technical information* requires approval of appropriate legal and patent functions.

Disclosure Outside the Organization: Requires prior approval of authorized functional executive, with execution of an approved by legal and patent department Confidential Disclosure Agreement.

Restricted Sample Guidelines

Description: Confidential Restricted information must have one or more of the following attributes:

1. **Provide the organization a *significant* competitive edge**
2. **Be of such nature that unauthorized outside disclosure would cause damage to the organization**
3. **Relate to or describe a very significant portion of the organization's business**
4. **Show operational direction over an extended period of time**
5. **Be extremely important to technical or financial success of a product**

Distribution is limited to employees with an *explicit* business need to know

Examples:

1. Consolidate revenue, cost, profit, or other financial results for the entire organization
2. Announcement or first customer ship dates for a new product
3. Market requirements, technologies, product plans, revenues, customer demands and similar accumulated information contained in executive presentations
4. Forecast assumptions and forecasts for some products
5. Other significant technical or business information where a history of access is not required
6. Concentrations of information classified Confidential

Responsibilities during Creation or Generation: Having made the decision that this is the proper classification, ensure that the classification appears on each page, screen, or part

Use: Access granted or assignment made only to users with a predetermined need to know. History of access not maintained. Ensure each distribution list is current. Users may not copy Confidential Restricted except with the approval of the owner of site authorizer. Confidential Restricted information protected under a special security department lock.

Transmission: Encryption is required for all electronic transmission except when the transmission is entirely by wire and the wire remains entirely within one of the organization's facilities. Transmission should occur only if the recipient site maintains required security controls.

Mail: Used sealed envelopes and mark the envelopes with the "Confidential" classification. Use double envelopes by inserting the envelope bearing the confidential classification into a second envelope with no classification.

Telephone: Only discuss confidential restricted on an internal all-cable network. Otherwise, voice encryption is required. Also, ensure the business need to know and identity of the recipient.

Meetings: Announce that the subject is Confidential, verify attendee's need to know, and ensure meeting area physical security. Presenters must indicate what is appropriate for recording.

Travel: Avoid traveling with Confidential Restricted information. When possible, mail the information ahead. Individuals transporting Confidential Restricted records are responsible for their protection while in their custody. Travel across national boundaries with *technical information* requires approval of appropriate legal and patent functions.

Disclosure Outside the Organization: Requires prior approval of authorized functional executive, with execution of an approved by legal and patent department Confidential Disclosure Agreement.

Registered Confidential Sample Guidelines

Description: Registered Confidential information must have one or more of the following attributes:

1. **Provide the organization *significant* competitive edge**
2. **Be such that outside disclosure would cause significant damage to the organization**
3. **Relate to or describe a major and very significant portion of the organization's business**
4. **Show strategies and major direction over an extended time period**
5. **Be vital to the technical/financial success of a product**

Distribution is limited to employees with an *explicit, predetermined* business need to know.

Examples:

1. Operating plans, marketing plans or strategies, drawings and documentation regarding unannounced products
2. Descriptions of unique parts or materials, technology intent statements, new technological studies, etc
3. New technology strategic plans
4. Consolidated scheduling data for key new products
5. Concentrations of Confidential Restricted information

Responsibilities during Creation or Generation:

1. A Registered Confidential control number is assigned by the local recorder of registered information and is recorded on each page along with classification and page number
2. A Registered Confidential cover sheet is prepared
3. A current distribution list is required reflecting recipients and/or persons authorized to access the data
4. Rough drafts, charts, preliminary copies, etc., are turned over to the recorder

Distribution: The originator of Registered Confidential information may select optional methods of distribution.

1. Reproduction may be made on a one-copy-per- user basis, with access limited to that person
2. A reduced number of Registered Confidential records sent to sites with Registered Records control centers, which provide a library share service. Initial distributions are reduced and minimal reference copies are maintained
3. If the recipient sites concur, reproducible masters may be sent for local reproduction and control
4. A Registered Confidential document may be divided into sections or chapters and recorded and accounted for as separate documents if the end use requires that separate sections or chapters be available for different users

Use: Access granted or assignment made only to users with a *documented, confirmed need to know*. The recorder must maintain a record of access and assignment.

Some sites establish Registered Records control centers. Authorized users withdraw documents as needed. The control center provides secure housing, record keeping, and updating services and maintains a sufficient number of copies required to meet business reference needs.

When not in use or attended, Registered Confidential data housed separately from other records and kept under a secured approved lock. Users must be able to account for these records at all times and should record disclosures on a Registered Confidential Disclosure Log. Physical audits occur at least once a year. Report any loss immediately to the recorder.

Users may not copy, transfer accountability, send to storage, or destroy Registered Confidential records. The recorder must perform these functions.

Transmission: Transmission of Registered Confidential information requires specific involvement of the recorder of registered information at each location, or it requires documented pre-authorization by an appropriate level of management.

Encryption is required for all electronic transmissions except when transmission is entirely by wire and the wire remains entirely within one of the organization's facilities.

Classify information access passwords to Registered Confidential databases as Registered Confidential and must be released via the recorder. Recorders must obtain receipts, physical terminal security exists, and users alerted to their responsibility for registering Registered Confidential output.

Keep a history of every person who has accessed Registered Confidential files on information systems, and give the history to the recorder of registered information.

Telephone Calls: Do not discuss registered confidential information by telephone unless voice encryption capability exists. Where it exists, the discloser of Registered Confidential information to another employee must verify the need to know and identity of the recipient.

Meetings: Ensure that the physical area is secure, announce that the subject under discussion is Registered Confidential, and verify attendees' need to know. Attendees are required to sign a register reflecting the date of the meeting and Registered Confidential subject discussed. The recorder must receive the attendance register. The presenter is responsible for indicating what is eligible for annotation and what is not. The recorder must control the release of any Registered Confidential records to the attendees.

Travel: It is not permissible to travel with Registered Confidential information. The recorder can arrange to have the required Registered Confidential data available at the destination. Exceptions are to be in writing by a general executive, and individuals transporting Registered Confidential records are responsible for their protection while in their custody. Additionally, travel across national boundaries with technical information requires appropriate legal and patent function approvals.

Disclosure Outside the Organization: Prior approval is required by a general executive of the organization, at a level not less than division president or general manager, before Registered Confidential information is disclosed outside the organization. Execute a Confidential Disclosure Agreement, approved by the appropriate legal and a patent operation department, prior to the disclosure.

Conclusion

Information and data ownership and its classification, along with many other important management issues should be included in a number of programs in the organization with the goal of having them become part of the fabric of the organization on a day-to-day basis.

As a part of an ongoing education program, all management and employees trained in their responsibilities for ownership, and in the organization's classification system and controls for the program to be effective.

Finally, a reminder:

Ownership answers the question:

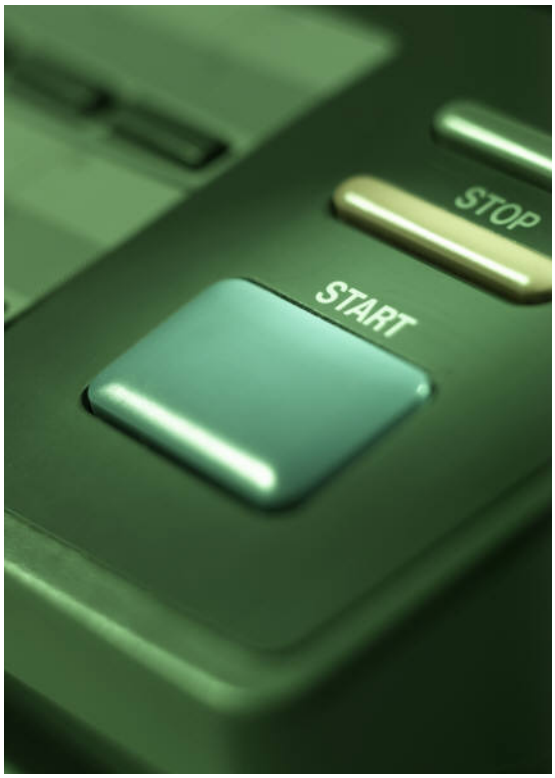
WHO IS RESPONSIBLE?

Classification answers the question:

HOW MUCH PROTECTION IS APPROPRIATE?

Approach to Implementation of Ownership and Classification

1. Establish organization policy
2. Show need
3. Identify organization and functional coordinator‘s
4. Involve affected people
5. Develop organization standards
6. Designate asset ownership
7. Establish information asset classes and controls
8. Educate all employees on the concept and guidelines
9. Implement the processes
10. Periodically test and audit the system



Sample Policy Statement

The following is an example of paragraphs related to ownership and classification for inclusion in an organization-wide statement. It should be simple, straight forward, and tailored to each organization's specific need, including the number of classifications and their names.

All information belonging to (name of organization) shall have a designated OWNER, an individual who acts for the organization with responsibility for the information until obsolete or passed to a new owner. A CUSTODIAN, who has authorized possession of the information – and may be the supplier of Information System Services, follows the owner-designated controls. The USER must follow the specific rules as stated in (title of standards document).

(Name of Organization) information will be classified on the basis of sensitivity to disclosure in one of the following categories:

- *Public or Unclassified*
- *Internal Use Only*
- *Confidential*
- *Confidential Restricted*
- *Registered Confidential*

For definitions, examples, and detail control requirements, see (title of standards document).

References: Specific references to other pertinent documents of (name of organization).

Information Asset Worksheet

Information Asset	Owner	Classified	Labeled	Custodian Identified	Users Specified	Audit Complete

IMPLEMENTATION CHECKLIST

Check these process steps for implementation status

.

In Place	Process Action	Needs Work
	We have justified an ownership/classification process	
	We have identified the information owners	
	We have involved the owners in our planning process	
	We have identified custodians and users	
	We have documented an implementation Policy	
	We have identified training necessary to complete implementation	
	Our implementation plan places minimum stress on people	
	We have communicated our intent to all employees	
	We have tested this program wherever practical	
	We are confident that our program will meet our present and future needs	
Of Ten	**How Did You Do?** **Are You Ready to Implement?**	Of Ten

REVIEW THE OWNERSHIP PROCESS

- ❑ Have we adequately identified our critical information assets?
- ❑ Have we analyzed our ability to protect our proprietary information?
- ❑ Have we provided for adequate protection?
- ❑ Have we considered needs and opportunity to enhance our procedures?
- ❑ Have we gained the support of all employees to protect our assets?

About the Author:

Louis W Mehrmann
Biography

Summary

"Lou" Mehrmann is a retired free lance Business Management Consultant with over 45 years of customer focused interrelationships and business process experience. He began his business career when he joined IBM immediately after serving in the U.S. Navy during the Korean "Conflict" where he earned his Dolphins aboard the Submarine U.S.S. Sennett (SS408) as an Electronics Technician.

Lou has 35 years of diversified IBM experience; in field, headquarters, line, staff, and management positions; in service, marketing, and corporate business functions. His major strengths are in business process planning/management, process problem/causal analysis, solution design/implementation, and standards. He has specialized knowledge in Information Systems Management, Data Security, Audit Practices and Procedures, and Baldrige Quality Assessments. He is a creative, energetic results oriented professional, whose work ethic, example, and exceptional rapport with younger employees build strong team commitment

After retiring from IBM, Lou spent:

- Two years as a consultant with the IBM Credit Corporation base lining, entitling, and reengineering their field marketing process.
- One year consulting with medical practitioners performing office work flow time/motion studies, evaluating staff assignments, making staffing recommendations, and in the evaluation of overhead expenses and recommended cost reductions.
- Five years as a consultant, again with the IBM Credit Corporation designing, implementing, and managing an end-user Customer Satisfaction Program.
- Two years with DBA Business Transformation Services doing self-study course evaluations and recommendations, learning activity identification to support specific skills, career path roadmap definition and design, and in evaluation of participation by business unit and profession in the career planning process.

About the Author:

Louis W Mehrmann

Accomplishments

Initiated, developed, implemented information systems management briefings, seminars, planning sessions to address customer concerns about complexity, reliability, availability issues resulting in eased transition to new applications, decreased pent up demand and increased productivity. Lou conducted sessions for several hundred customers including more than a dozen Fortune 500 establishments.

Lou designed, developed, and published twelve customer data control documents for IBM. (Security Assessment Questionnaire, Security Controls and Procedures, Risk Assessment, Contingency Planning, Dial-Up Security, Information Ownership and Classification, Personal Computer Security, Control of Off-Site Terminal and Software Usage, Information Systems Network Security, Fire Suppression in DP Operations, Bibliography of Security, Audibility, Control Publications, and a Detailed Three Phase Project Plan for Implementing System Network Control Centers).

Lou counseled over 3000 IBM customers nationwide via seminars relating to security, audibility, and control of information systems to address data integrity and corporate Data Asset Protection issues. This resulted in heightened customer awareness and implementation of improved protection methodologies.

Developed and initiated three new corporate audit programs for IBM; (Personal Property Taxes for M&D Sites, Buy America Procedures and Controls, Import Process Controls) which identified a lack of business process controls over several critical business functions exposing the corporation to significant financial loss opportunities. Resulted in major changes to worldwide sourcing logistics system and strengthening of associated internal controls. Participated in 12 audits, acted in capacity of Auditor in Charge for 11 additional audits, Mentored and trained six new audit team players.

Facilitated documentation and analysis of IBM field technical support process that identified significant redundancies. Resulted in initiation of major process re-engineering project to affect ten times (10X) improvement in process effectiveness and efficiency.

Developed, implemented, and managed an End-User Customer Satisfaction program for IBM Credit Corporation. Established closed loop process to identify and correct systemic root causes of customer dissatisfaction. This resulted in 8% (87%-95%) improvement in overall customer satisfaction and designation as “Best of Breed” within IBM parent company.

About the Author:

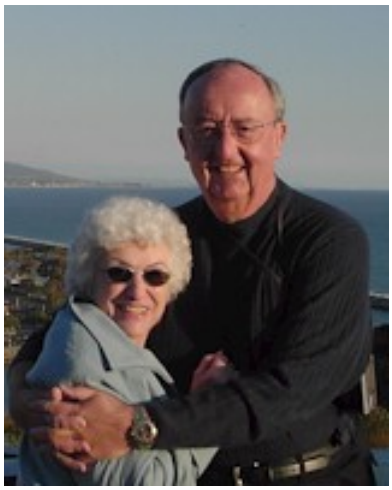
Louis W Mehrmann

Personal

Lou is a prostate cancer survivor, having both surgery and radiation after diagnosed less than one year after retiring from IBM. Since that time, both Lou and his wife Gloria have been actively involved in promoting cancer awareness in a variety of ways. Lou developed and provided the American Cancer Society (ACS) a presentation on prostate cancer that is readily available to deliver to any organization with an interest in the subject.

Lou personally presented to over 100 business, fraternal, university and church organizations in Southwest Virginia. He has been actively involved with the American Cancer Society as a committee Chairman for cancer education and on the local ACS board of directors. Lou is also an active member of the planning committee for the local Man-to-Man prostate cancer support group sponsored by ACS. In recognition of his dedicated service, Lou was selected and participated for several years in the Department of Defense (DoD) Prostate Cancer Research Program as a consumer advocate to evaluate proposals from medical professionals competing for research funding.

In response to requests, Lou and Gloria established a volunteer program for cancer advocates to support the Southwest Virginia Cancer Center. As a couple, they became active participants in the Man-to-Man program and selected to participate in the American Cancer Society National Cancer Awareness Education Council. They developed several training modules to teach selected leaders how to establish, organize, and run successful Man-to-Man functions for ACS. They personally trained new Man-to-Man leaders in several cities across the mid-south region of ACS.

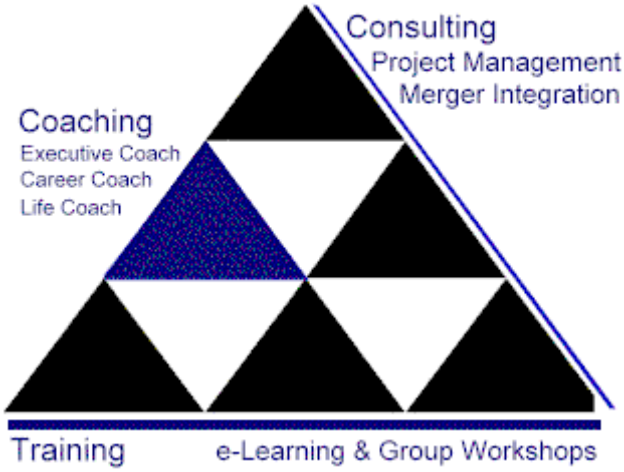


About WWW.EXECUTIVEBLUEPRINTS.COM

Time is Money

More Impact, Less Interruption

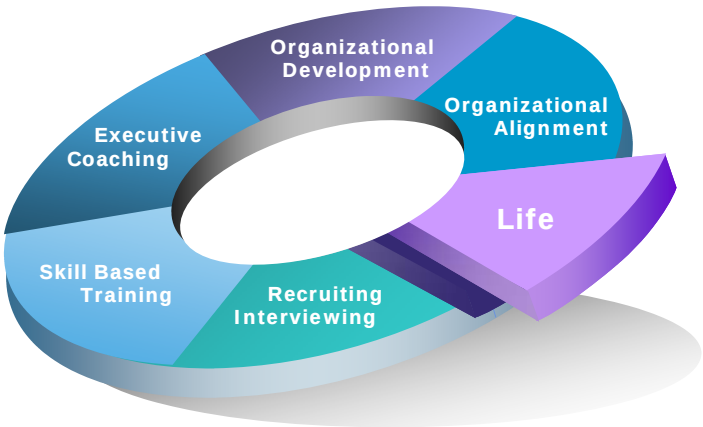
Fast Paced, Results Based
Consulting, Training and Coaching



The foundation of every organization is the talent of the people within it.

Executive Blueprints, Inc is dedicated to supporting leadership by providing proven blueprints for success and individual resource development. Services include preparing a customized library of training and reference materials, consulting and management coaching.

Executive Blueprints uses experienced executive talent with customized materials to enhance personnel at all levels of an organization. From Executive Coaching to Management Development, Associate enhancement and New Hire selection techniques, we are dedicated to help measure and achieve success. Let us help you reach your goals with the right tools for continuous self-improvement.



Executive Blueprints, Inc is not engaged in rendering legal or financial advice. These tutorials are not a substitute for the advice of an attorney or accountant. If you require legal advice, you should seek the services of an attorney. If you require financial advice, you should seek the services of an accountant.