# Global Information Assurance Certification Paper

# GIAC Security Essentials Certification (GSEC)

**Assignment Version 1.0**
**Option 1**

## Information Classification – Who, Why and How

Submitted by:
Susan Fowler
February 28, 2003

# INFORMATION CLASSIFICATION – WHO, WHY AND HOW


## ABSTRACT

Many companies consider initiatives like risk analysis and information classification, which tie protection measures to business need, to be too expensive and unwarranted. They instead look to information technology support organizations to identify the information that should be protected, the level of protection that should be provided, as well as the technology solution.

Because it is the business community that knows best the importance of the information, this practice often results in inefficient and ineffective technology focused information protection plans that do not specifically address a company's business need.

This paper will clarify who *should* be determining appropriate company protection needs. It will also demonstrate why information classification is a necessary, efficient and effective means to convey business driven information protection requirements. Last, it will offer a method for classifying information to persuade readers from accepting that their company should implement a data classification system to recognizing that it can.


## WHY INFORMATION CLASSIFICATION IS IMPORTANT

Companies need to protect their information today more than ever

The increasing need for companies to protect their customer and financial information is obvious. Signs are prevalent in the news, publications, and in the turn of recent business and world events. For example:

- Information technology has recently been selected as a weapon of choice for terrorists. The potential is there to cripple our economy.
- The Internet is being used more and more for critical business transactions. It is common knowledge among business professionals that transacting business over the Internet without appropriate protection measures puts consumer and company information at considerable risk for fraud and theft.
- New government regulations, like the Gramm Leach Bliley and Health Insurance Portability and Accountability Acts (HIPAA) hold organizations responsible for implementing protection controls for information privacy, access, storage and exchange. Companies that don't comply can be assessed steep financial penalties.

The need is obvious but solutions are not

The complexity of information, sophistication of technology, and the growing number of solutions make pinpointing the most cost effective mix of information protection measures a daunting task. To further complicate matters, once a technology is decided on, it is not unusual for companies to get caught up in the consumer quagmire of whether to invest in a technology that may be obsolete tomorrow.

Management must ensure company information is protected

Neither the extent of appropriate measures nor the right approach for protecting information is easily discernable. What is clear, however, is that senior management is responsible for ensuring that information protection measures are defined, communicated and followed.

Security industry experts have consistently charged senior management with providing clear guidelines for information protection. [1] While the extent to which management is responsible for ensuring protection measures are carried out is debatable, recent indictments of Enron company executives evidence an increasing trend to hold corporate management accountable for losses resulting from irresponsibility and neglect.

It can be done

Increasing political pressure, complexity of information and sophistication of technology make management's charge extremely challenging. Fortunately, the information security industry offers proven approaches for protecting company information through mechanisms like information security policies, information classification and risk analysis.

All of these approaches have common and distinct benefits. This paper will distinguish the three to substantiate why making data classification an integral part of a company's information protection plan provides the most benefit to the majority of companies.

Distinguishing information classification from security policy and risk analysis

Search the Internet on data or information classification, and you'll find references among pages on security policy and risk management. Close examination of this information leaves one wondering where risk management begins and security policy and information classification end.

"A security policy is a high-level plan stating management's intent pertaining to how security should be practiced within an organization, what actions are acceptable, and what level of risk the company is willing to accept." [2] For example, an information security policy might state that risk analysis must be performed or company information must be classified. Considering their non-specific nature, information security policies should be viewed as the minimal requirement for fulfilling an organization's information protection responsibilities.

[1] Harris, Shon, CISSP All in One Certification Exam Guide (New York: The McGraw-Hill Companies, 2002) 35.

[2] Shon 171

Risk analysis balances the value of company assets against loss threats and their probabilities to identify safeguards or countermeasures that mitigate risk to acceptable levels. This quantified approach validates that protection measures mitigate risk. Because the value of information is difficult to determine when it does not generate income, this approach is often impractical for many businesses.

Information classification is "the embodiment of management's tolerance of information risk." [3] It categorizes data to convey required safeguards for information confidentiality, integrity and availability. These protection measures are usually based on qualified information value and risk acceptance.

Because it doesn't require that safeguards are cost justified, data classification affords a company the flexibility to establish and communicate *specific* information protection measures based on *implied* company values and goals.

In summary, while each approach varies in focus, methodology and benefits, all three have the same basic goal: to formally clarify company required protection measures in consideration of value and risk acceptance. Regardless of focus or approach, formally stating a company's information protection needs is the first step toward satisfying management's information protection responsibilities.

Additional reasons for classifying information

Given that information security policies only begin to satisfy information protection requirements and risk analysis is excessive for most companies, information classification offers a moderate approach that affords maximized benefits. Those benefits are detailed in the remainder of this section.

The most compelling reason to classify information is to satisfy regulatory mandates. For example, the Gramm Leach Bliley and the Health Insurance Portability and Accountability Acts mandate information protection controls for financial and medical organizations, respectively. Although information classification is not specified as a required protection measure, it is implied by special handling requirements for sensitive, medical and financial information.

Some companies also have contractual commitments to protect information according to customer or business partner specifications. The obvious benefit for satisfying regulatory and legal requirements is that it minimizes the risk of financial penalties for non-compliance.

In addition to mandated requirements, industry evaluation criteria imply that there is a need to classify information. For example, the U. S. Government's Trusted Computer System Evaluation Criteria or Orange Book specifies protection requirements related to confidentiality. The continued endorsement of information classification is also evidenced in newly evolving standards, like the Common Criteria, which provides a framework for the development of information security evaluation criteria related to hardware, firmware and software. A specific example of this is the Strength of Function

[3] Christopher M. King, Curtis E. Dalton, and T. Ertem Osmanoglu, Security Architecture Design, Deployment & Operations (The McGraw-Hill Companies, Copyright 2001) 42.

(SOF) criteria, which provides for defining safeguards according to the importance of the information being protected.

In addition to fulfilling legal obligations as well as industry and customer expectations, information classification can also provide opportunity for work and cost savings.

From a confidentially and integrity standpoint, formally documenting information sources and the individuals who are responsible for their protection provides a framework to ensure that the right people are involved in the provisioning process. This relieves administrators from (perhaps inappropriately) deciding whether an application's use should be authorized or whether application monitoring should be performed daily or not at all. Where "public" access has been deemed appropriate, granting access at the company level minimizes administrative overhead and facilitates employee access.

Resource efficiencies can also be realized in the area of availability. For example, the costs for ensuring system availability can vary significantly depending on how quickly the information needs to be recovered. Tape technology solutions afford recoverability within hours while fail-over and system redundant solutions ensure continued information availability, albeit at a much higher cost. Formalized information protection requirements enable system administrators to budget and implement the appropriate technologies according to information importance.

There are two final benefits worthy of consideration. The first is that implementing an information classification system exemplifies an organization's commitment to protecting customer information.[4] Presented strategically, this could provide a competitive advantage over companies who have not taken information protection as seriously.

Last, formalizing your company's information protection requirements through information classification can improve company audit results from two perspectives. It provides auditors with a realistic yardstick against which to measure company compliance (instead of industry best practices), and it gives employees more defined goals to work towards.

Information classification goals

Having established that companies should classify their data, it is important to understand what an effective information classification system should accomplish. That is to categorize information so as to communicate company-endorsed safeguards for information confidentiality, integrity and availability. An effective data classification system should also be easy to understand, use and maintain.

While it is common knowledge that confidentiality, integrity and availability of data are crucial to information security, most data classification systems focus only on confidentiality. The familiar "Private" and "Confidential" information classification labels

[4] Ronald L. Krutz and Russell Dean Vines, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security (John Wiley & Sons, Inc. 2001) 6.

evidence this practice, which likely stems from the fact that U.S. Government computer evaluation criteria historically focused only on confidentiality.

This limited focus has understandably minimized information classification's perceived relevance and importance.

While taking a comprehensive approach makes implementing data classification more challenging, the importance of this is evident in the fact that companies expend more resources ensuring information is available and correct than protecting it from inappropriate access.

## IMPLEMENTING INFORMATION CLASSIFICATION

Approach for classifying information

There are many ways to implement an information classification system. Except for the military, there are no set formulas. The key is to facilitate employee compliance of company endorsed information protection measures.

To successfully implement information classification, a company must transition from recognizing that it should classify its data to recognizing that it can. Toward that end, this paper will demonstrate a six-step, common sense approach to data classification, assembled from recurring suggested activities and supporting concepts encountered throughout my research.[5] [6] [7]

The proposed approach was tested against a sampling of information sources to serve as an example for this paper. The results of each step are provided in Attachments 1 through 5.

Step 1. Identify all information sources that need to be protected.

Common approaches for gathering data include written surveys, questionnaires and personal interviews. One research source also proposed the use of an expert system for information classification.[8] (This idea sounded promising until follow-up research revealed no vendor offerings tailored to information classification.)

If information sources haven't been compiled for other initiatives, the best sources might be developers, operating system and database administrators, business champions, and departmental and senior managers.

During the information gathering process, consideration should be given to how recent trends in distributed computing and widespread use of desktop productivity tools

---

[5] F. Christian Byrnes and Dale Kutnick, Securing Business Information: Strategies to Protect the Enterprise and Its Network (Intel Press, 2001 and 2002) 109.

[6] F. Krutz and Vines 4-15.

[7] F. Byrnes and Kutnick 31-109.

[8] Walter Cooke, http://www.uncle.com/es4dsc.html

might challenge the identification (and consistent protection) of information in its various forms.

Completion of this step should produce a high level description of company information sources, where the data resides, existing protection measures, data owners (i.e., individuals responsible for establishing policy), data custodians (i.e., individuals responsible for maintaining the information), and the type of resource (i.e., file, application, backup tape).[9]

Information can be listed separately or can be grouped when the same set of protection measures apply to the group, also referred to as a domain. Four common domains are: geography, organization, technology, or application lifecycle.[10] Examples where domain level classes might apply are similar operating systems or all applications under development that don't need to be recovered immediately.

The information identified in this initial stage will be expanded and made more granular in subsequent steps and iterations. Attachment 1 provides examples of information sources initially identified in Step 1.

Having compiled all known sources of information, the next step is to identify desired protection measures.

Step 2. Identify information protection measures that map to information classes

Information protection goals can be obtained from various sources. For example, a company's security policy as well as existing organizational structure and informal data segregation approaches. This information may also come from technical support teams, information custodians, business champions and managers. There may also be regulatory and legal requirements to consider.

Some common, industry-recognized information protection measures are highlighted below. Their applicability to your company depends on its business needs and information protection goals.

Authentication

The most common safeguard for confidentiality is the requirement for authentication. Authentication helps to ensure that an individual is who he claims to be by requiring the user to be identified.

The strength of authentication is determined by the quantity of identifying validations provided and/or the sophistication of identifying technology. Single authentication usually requires that an individual provide an id and password. Double authentication might require that an individual provide an id and password and a secret key. An example of sophisticated authentication technology would be retina scans.

Role based access

Another common safeguard is to require that information access be provided based on business need or job function. This approach implies that someone, like a data owner or manager, validates and authorizes business need. Access Control Lists

[9] Shon 104.

[10] Byrnes and Kutnick 31-50.

(ACL) are system features that support granular access levels such a read, change, or delete.

Encryption

Encryption formats information so that it cannot be inappropriately viewed or altered without detection. Login processes and financial transactions are commonly encrypted, but this mechanism can be used to ensure privacy of sensitive or personal information as well. Creative deployment of encryption technology may also help to ensure that confidential information in various formats is consistently protected.

Administrative controls

Administrative controls are also used to ensure the integrity of information. These controls are often presumed to be implemented but may not be because of high administrative overhead. Examples of these are formal change controls, separation of duties, rotation of duties and cross training.

Technology control

There are also technology specific controls like virus protection; disk, system and application redundancy; and network segregation.

Assurance

Validating that systems are safeguarded is also a level of protection. Examples are policy compliance monitoring, code walkthroughs, intrusion detection, system performance monitoring, transactional monitoring, administrative monitoring, and file access monitoring.

Attachment 2 provides those protection measures selected for example.

With protection measures identified, the next step is to identify information classes.

Step 3. Identify information classes.

Information class labels should convey the protection goals being addressed. Classification labels like Critical and Sensitive have different meanings to different people so it is important that high-level class descriptions and associated protection measures are meaningful to the individuals who will be classifying the information as well as those who will be protecting it.

With that stated, the classes should be identified intuitively during the first iteration as it is almost certain that subsequent classification and protection mapping steps will significantly change the class labels initially identified.

Attachment 3 details the information classes that were considered throughout implementation of the classification example.

Step 4. Map information protection measures to information classes.

Before information can be classified, the protection measures (identified in Step 2) must be mapped to the information classes (identified in Step 3) to reflect company protection goals.

For the example classification the first iteration was premised on one data class that identified four varying degrees of protection for confidentiality, integrity, availability

and assurance. These four degrees were Proprietary, Discretionary, Internal and Public. This model did not work well and had to be reworked several times. The iterative process it took to accomplish this is detailed in Step 6.

Attachment 4 represents the final class and protection measure mappings that ultimately accommodated the classification of all information sources and protection goals.

Step 5. Classify information

In this step, the classification labels and protection measures (mapped in Step 4) must be applied to the sources (identified in Step 1). The main objective is to validate that the protection measures associated with the classification are appropriate for the information source. This step challenges all assumptions made in previous steps.

If the information classes and associated safeguards (identified in Step 4) do not accommodate classification of all information sources (identified in Step 1), proceed to Step 6.

Step 6. Repeat as needed

This is where the iterative process of adjusting classes, protection levels and sources begins. For example, the initial one class model referenced in Step 4 accommodated the classification of only three data sources. The next iteration resulted in a class model that combined confidentiality and integrity yet segregated availability. This model also did not accommodate the classification of all information sources.

Attachment 5 represents the class model that did accommodate the classification of all information sources in consideration of confidentiality, integrity, availability, compliance and recovery protection goals. It also identifies those individuals responsible for defining information protection needs (data owners) as well as those individuals who are responsible for ensuring that safeguards are implemented (data custodians).

## SUMMARY

Information classification is an iterative and an on-going process.

A company's information security policy should state that data classification is expected.

Standards and procedures must be implemented to ensure that the introduction of each new information source triggers the information classification process and that retiring information sources and/or related classifications are removed.

Supporting manager, data owner, custodian and information consumer organizational roles and responsibilities must be identified, incorporated into performance plans and communicated through on-going security awareness initiatives.

If this sounds like too much work, consider this. Without data classification, information protection decisions are being made every day at the discretion of security, system, and database administrators. An information classification system helps to ensure that those decisions satisfy *company* instead of individual information protection goals.

BIBLIOGRAPHY

Byrnes, F. Christian and Kutnick, Dale, Securing Business Information: Strategies to Protect the Enterprise and Its Network, (Intel Press, 2001 and 2002)

Common Criteria
http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF
http://www.commoncriteria.org/docs/PDF/CCPART2V21.PDF
http://www.commoncriteria.org/docs/PDF/CCPART3V21.PDF

Cooke, Walter, "An Expert on a Disk: Automating Data Classification Work Using Expert Systems," W. J. Cooke & Associates Ltd., Bermuda, 1995
http://www.uncle.com/es4dsc.html

Department of Defense Trusted Computer System Evaluation Criteria, December 1985
http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

Harris, Shon, CISSP All in One Certification Exam Guide (New York: The McGraw-Hill Companies, 2002)

HIPAA Implementation Guidelines, Guidelines for Classifying Data, General Administrative Overview
http://www.calhipaa.com/main/classification_sample1.htm

King, Christopher M., Dalton, Curtis E. and Osmanoglu, T. Ertem, Security Architecture Design, Deployment & Operations, The McGraw-Hill Companies, Copyright 2001

Krutz, Ronald L and Vines, Russell Dean, The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, Inc. 2001

Lee, Rich, "Network Security: Determining Your Risk Index," Novell Systems Research, August 1996
http://developer.novell.com/research/appnotes/1996/august/02/index.htm

Warigon, Slemo, Association of College and University Auditors LEDGER, Vol.41, No. 2., April 1997, pp. 3-7. "Data Warehouse Control and Security"
http://www.all.net/books/audit/kits/dw.html

**ATTACHMENT 1 – Page 1**

## Step 1 - Identify all information sources that need to be protected.

| Information Source | Information location | How information is protected now (access approvals needed, monitoring, backups) | Data Owner (persons who know value of information to company) | Data Custodians (persons responsible for safeguarding information) | Format of the information (database, file, application) |
|---|---|---|---|---|---|
| Customer Database | Windows1 | • Must log in<br>• Access given per job function<br>• Monitoring? | Customer Service VP | • Database Admin<br>• Security Admin | Database |
| Product Database | Unix1 | • Manager approves access | Customer Service VP | • Database Admin<br>• Security Admin | Database |
| Financial Database | Unix2 | • Must log in<br>• CFO approves access<br>• Monitoring? | Controller | • Database Admin<br>• Security Admin | Database |
| HR Database | Unix2 | • VP of HR approves access<br>• Backup? | HR VP | • Database Admin<br>• Security Admin | Database |
| Customer/ Product Admin Application | Web1 | • Manager approves access | Customer Service Manager | • Web Support<br>• Customer Service | Web |

**ATTACHMENT 1 – Page 2**

## Step 1 - Identify all information sources that need to be protected.

| Information Source | Information location | How information is protected now (access approvals needed, monitoring, backups) | Data Owner (persons who know value of information to company) | Data Custodians (persons responsible for safeguarding information) | Format of the information (database, file, application) |
|---|---|---|---|---|---|
| Accounts Payable Application | Web2 | • Manager approves access<br>• Monitoring? | AP Manager | • Web Support | Web |
| Accounts Receivable Application | Web2 | • Manager approves access<br>• Monitoring? | AR Manager | • Web Support | Web |
| Payroll | Web2 | • Manager approves access<br>• Monitoring? | Payroll Manager | • Web Support | Desktop |
| Privileged account passwords | Various systems and databases | • Encrypted<br>• Manager approves<br>• Access based on job function<br>• Event monitoring | System and Database Support Administration | • ? | System |
| Word and Excel Files | Fileserver1 | • Don't know | Employee | • Windows Support<br>• Security Admin | Documents |
| Business Partner X customer list | Customer Database | • Product Management can see but cannot be published to customers or employees. | Product Manager | • ? | Data in a database |

**ATTACHMENT 2**

| Step 2 - Identify information protection measures that will map to information classes. |
|---|
| Individual access versus Role Based Access versus Discretionary Access |
| Various Levels of Authorization |
| Various Levels of Authentication |
| Violation Logging |
| Intrusion Detection |
| System backup, redundancy |
| Update constrained by application |
| Code walkthroughs |
| Change Management |
| Separation of Duties for Financial Operations |
| All copies of information are accounted for and destroyed prior to disposal |
| Transaction logging |
| Cross Training |
| Virus Protection |
| System Event Logging |
| Off Site Disaster Recovery |

**ATTACHMENT 3**

| Step 3 - Identify information classes |
| --- |
| Confidentiality |
| Availability |
| Integrity |
| Proprietary |
| Highly Sensitive |
| Function Sensitive |
| Business Restricted |
| Owner Restricted |
| Owner Discretion |
| Company Use |
| Internal Use |
| Public Use |
| Business Critical |
| Business Sensitive |
| Not Essential |

**ATTACHMENT 4 – Page 1**

## Step 4 – Map protection measures to information classes.

### SENSITVITY AND CONFIDENTIALITY

These information classes provide varying degrees of protection against information being inappropriately disclosed with Highly Sensitive being the most protective and Public Use being the least. These measures are designed to

- promote customer trust
- ensure compliance with legal, contractual and regulatory obligations
- ensure no customer has unfair advantage and
- protect against financial loss and fraud.

| Company Protection Criteria | Highly Sensitive | Function Sensitive | Owner Discretion | Company Use | Public Use |
|---|---|---|---|---|---|
| Authentication (ensuring person is who they claim to be) | • User Id, strong password<br>• Encrypted Login | • User Id, strong password<br>• Encrypted Login | • User Id, strong password | • User Id, strong password | • No authentication required |
| Provisioning (who authorizes and method for providing access) | • Senior Management or Data Owner authorization<br>• Individual access | • Manager authorization<br>• Role Based | • Authorization and administration delegated to creator or owner | • Access automatically provided to employees | • Access automatically provided to all information system users |

## Step 4 – Map protection measures to information classes.

### INTEGRITY AND APPROPRIATE USE

This information class provides varying degrees of protection for information integrity geared toward appropriate use with High being the most effective and Low being the least.

- ensure information validity
- promote customer trust
- ensure compliance with legal, contractual and regulatory obligations
- ensure no customer has unfair advantage and
- protect against financial loss and fraud.

| High | Medium | Low |
|---|---|---|
| • Update per Data Owner specifications<br>• Separation of Duties for Financial Operations.<br>• All copies of information are accounted for and destroyed prior to disposal<br>• Subject to Change Control<br>• Code Walkthroughs required<br>• Encrypt all information transactions<br>• Encrypt at rest information | • Update per Data Owner specifications.<br>• Subject to Change Control<br>• Code Walkthroughs required<br>• Encrypt Internet transactions. | • No integrity or appropriate use controls. |

**ATTACHMENT 4 – Page 3**

## Step 4 – Map protection measures to information classes.

### AVAILABILITY

This information class safeguards information availability in varying degrees with High being the most effective and Low being the least.

| High | Medium | Low |
|---|---|---|
| • No tolerance for service interruption during core business hours.<br>• Cross Training of business operations personnel required<br>• Virus protection required | • Must be recovered within 8 business hours<br>• Cross Training of business operations personnel required<br>• Virus protection required | • Virus protection required |

**ATTACHMENT 4 – Page 4**

## Step 4 – Map protection measures to information classes.

### COMPLIANCE

This information class validates information safeguards in varying degrees with High being the most and Low being the least.

| High | Medium | Low |
|---|---|---|
| • Regular capacity monitoring<br>• Regular violation monitoring<br>• Regular transaction log monitoring of sensitive functions<br>• Regular event log review<br>• Network and system intrusion detection | • Violation logs available for review.<br>• Transaction logs available for review.<br>• Capacity monitoring on request.<br>• Event logs available for review.<br>• Network and system intrusion detection | • Auditing not enabled; log review not available.<br>• No monitoring |

**ATTACHMENT 4 – Page 5**

## Step 4 – Map protection measures to information classes.

### BUSINESS CONTINUITY

This information class identifies whether information must be available to maintain business at a designated temporary location in the event of a disaster.

| Recovered | Not Recovered |
|---|---|
| • Recovery at hot site | • No hot site recovery |

**ATTACHMENT 5 – Page 1**

| Step 5 – Classify Information | | | | | |
|---|---|---|---|---|---|
| Information Source | Location | Information Classifications | Data Owners | Data Custodians | Type of Information |
| Customer Database | Windows1 | • Function Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance Medium<br>• Recovered | Customer Service VP | • Database Administration<br>• Operations Support<br>• Security Administration | Database |
| Product Database | Unix1 | • Function Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance Medium<br>• Recovered | Customer Service VP | • Database Administration<br>• Operations Support<br>• Security Administration | Database |
| Financial Database | Unix2 | • Highly Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance High<br>• Recovered | Controller | • Database Administration<br>• Operations Support<br>• Security Administration | Database |
| HR Database | Unix2 | • Highly Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance High<br>• Recovered | HR VP | • Database Administration<br>• Operations Support<br>• Security Administration | Database |
| Customer and Product Administration Application | Web1 | • Function Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance Medium<br>• Recovered | Customer Service Manager | • Web Support<br>• Operations Support<br>• Security Administration | Web Application |
| Accounts Payable Application | Web2 | • Function Sensitive<br>• Integrity Medium<br>• Availability High<br>• Compliance Medium<br>• Recovered | AP Manager | • Web Support<br>• Operations Support<br>• Security Administration | Web Application |

**ATTACHMENT 5 – Page 2**

| Step 5 – Classify Information | | | | | |
|---|---|---|---|---|---|
| Information Source | Location | Information Classifications | Data Owner | Data Custodian | Type of Information |
| Payroll | Web2 | • Function Sensitive<br>• Integrity High<br>• Availability Medium<br>• Compliance High<br>• Recovered | Payroll Manager | • Web Support<br>• Operations Support<br>• Security Administration | Client Application |
| Privileged account passwords; security configuration and rule settings | All systems and databases | • Function Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance High<br>• Recovered | System and Database Support Administration | • Database Administration<br>• Operating System Support<br>• Operations Support<br>• Security Administration | System |
| Employee proposals for Process improvements | Fileserver1 | • Owner Discretion<br>• Integrity Low<br>• Availability High<br>• Compliance Low<br>• Recovered | Employee | • Windows Support<br>• Operations Support<br>• Security Administration | Documents |
| Business Partner X customer list. | Customer Database | • Owner Discretion<br>• Integrity High<br>• Availability Medium<br>• Compliance High<br>• Not Recovered | Product Manager | • Database Administration<br>• Operations Support<br>• Security Administration | Database information |
| Legal Contracts | Fileserver1 | • Function Sensitive<br>• Integrity High<br>• Availability Medium<br>• Compliance Medium<br>• Recovered | Legal Manager | • Windows Support<br>• Operations Support<br>• Security Administration | Documents |

**ATTACHMENT 5 – Page 3**

| Step 5 – Classify Information | | | | | |
|---|---|---|---|---|---|
| Information Source | Location | Information Classifications | Data Owner | Data Custodian | Type of Information |
| Purchasing Correspondence | Fileserver1 | • Function Sensitive<br>• Integrity Low<br>• Availability Medium<br>• Compliance Low<br>• Recovered | Purchasing Manager | • Windows Support<br>• Operations Support<br>• Security Administration | Documents |
| Development Applications | Webserver1 | • Function Sensitive<br>• Integrity High<br>• Availability Low<br>• Compliance Low<br>• Not Recovered | IT Management | • Windows Support<br>• Operations Support<br>• Security Administration | Application |
| Default Unix Servers | All Unix Servers | • Function Sensitive<br>• Integrity High<br>• Availability High<br>• Compliance Medium<br>• Recovered | Infrastructure Management | • Unix Support | Operating System |
| Default Windows File Servers | All Windows File Servers | • Function Sensitive<br>• Integrity Low<br>• Availability Medium<br>• Compliance Low<br>• Not Recovered | Departmental Management | • Windows Support<br>• Operations Support | Files |
| Production Windows Application Servers | All Windows Application Servers | • Function Sensitive<br>• Integrity Medium<br>• Availability High<br>• Compliance High<br>• Recovered | Infrastructure Management | • Windows Support<br>• Operations Support | Operating System |

Last Updated: May 25th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |