Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# EnterpriseOne Security Solution for Real Estate Management

This paper will discuss the business request from Real Estate Management to Information Security to create a security model for production implementation.

Copyright SANS Institute

Author Retains Full Rights

AD

# EnterpriseOne Security Solution for Real Estate Management

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Ruben A. Amely-Velez
Location: Denver, Colorado

Paper Abstract: This paper will discuss the business request from Real Estate Management to Information Security to create a security model for production implementation.

© SANS Institute 2005, Author retains full rights.

# Table of Contents

Abstract/Summary ..... 2
Introduction ..... 2
Phase 1: The Role of Information Security ..... 3
Phase 2: Infrastructure Considerations ..... 3
- Network Security (client/server environment) ..... 3
- OS/Host Security ..... 3
- Database Security ..... 4
- Application Security ..... 4
- Physical Security ..... 5

Phase 3: EnterpriseOne Security Considerations ..... 5
- EnterpriseOne "Application Security" ..... 6
- Process Flows and Checklists ..... 11
- What is next? ..... 11

Conclusion ..... 13
References ..... 14
- Cited Internet Sources/URLs ..... 14
- Other Internet Sources/URLs ..... 14
- Cited Printed Works (Books) ..... 15
- Other Reference Material (Books) ..... 15

# List of Figures

Figure 1: REM Roles Application Security Model ..... 7
Figure 2: REM Role-Based Security Equation ..... 10

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005 Author retains full rights.

## Abstract/Summary

"PeopleSoft® EnterpriseOne is a complete suite of modular, pre-integrated industry-specific business applications designed for rapid deployment and ease of administration. It is ideally suited for organizations that manufacture, construct, distribute, service, or manage products or physical assets."[1] This paper will discuss the business request from Real Estate Management (REM) to Information Security (IS), and the process to create a role-based security model for PeopleSoft EnterpriseOne.

The REM group was to manage all U.S. vendor leases using EnterpriseOne Real Estate Management Module. The business requirements included that the infrastructure for this new security solution would be housed in the Data Center. The new system needed to be set up as a separate scaled-down version of the current production system. Typical EnterpriseOne environments were selected: development, prototype, mirror (production code run with non-production data), and production. The new system was intended to be used by REM users only, with a user base of about thirty users, five of whom had the ability to do application data updates; the remaining users had application data inquiry only.

IS requirements included creating a security model, user profiles, security groups/roles, and security records to be administered through the Security Administration/Operations group. New EnterpriseOne security needed to be set up and maintained for all environments.

## Introduction

A security model is a framework that enables users to conduct business in a secure environment. It focuses on security requirements and how these are measured against IS policies, procedures, and standards and how IS security requirements applies to business requirements. Furthermore, it details how the security is implemented for the new system in order to mitigate risk.

From a security perspective, finding equilibrium between data protection, security controls, and application-user-friendliness, while creating a layered (defense in-depth), approach for the security model can be overwhelming. Users may negatively perceive the new application security controls, which mitigate risks, as business "intrusive, and interruptive". The Business side is always worried about "How much it is going to cost." The IT organization may perceive security as a "roadblock" that will prevent the full use of technology features. A phased approach can simplify all tasks and help share the multiple responsibilities that will detail creating the security model. The main goal is to maintain confidentiality, integrity, and availability of the system.

[1] http://www.peoplesoft.com/corp/en/products/ent_one/index.jsp



© SANS Institute 2005 Author retains full rights.

The first two phases are briefly discussed. Phase 1 examines the leading role of IS and how it influences the security set-up for the enterprise. Phase 2 involves infrastructure considerations and how technology is used to support a security strategy. Phase 3, the creation of the EnterpriseOne security model, is the focus of this paper and will be discussed in detail.

## Phase 1: The Role of Information Security

In most business organizations, phase one is already in place. Every enterprise that attempts to function in today's business environment must have some type of IS organization. IS provides "policy, strategy, governance"[2], vision, leadership, and awareness. It also reports on the "health" of security for the enterprise.

IS defines security policies, security standards, security procedures, and security guidelines for the enterprise:

- *Security Policies* - regulate how the organization manages, protects, and assigns resources to achieve its security objectives[3]
- *Security Standards* – define what the rules are to perform a task and evaluate its success[4]
- *Security Procedures* - describe how to actually get the work done[5]
- *Security Guidelines* – recommend how management would like its employees to behave[5]

## Phase 2: Infrastructure Considerations

### Network Security (client/server environment)

Network Security implements and organizes ongoing administration, maintenance, support and security measures to mitigate security risks (threats). These include but are not limited to hardware and software, services, installation, configuration and management of security/security devices for the network.[6]

### OS/Host Security

Today's operating systems provide many security features, that, when utilized correctly, can enhance the security of the client or host and reduce many security risks. These security features must be part of the IS standards that are written to

[2] Tipton, Krause. Fifth Edition. Page 888.
[3] Tipton, Krause. Fourth Edition, Volume 3. Page 353.
[4] Tipton, Krause. Fourth Edition, Volume 3. Page 372
[5] Tipton, Krause. Fourth Edition, Volume 3. Page 374.
[6] http://www.cc.boun.edu.tr/network_security.html



© SANS Institute 2005 Author retains full rights.

support IS policies. According to Special OPS Host and Network Security for Microsoft, UNIX, and Oracle[7], some of the topics that are included are:

- OS Patch Management
- File system security (including registry for Windows)
- User Accounts
- Passwords
- File Sharing
- Active Services
- TCP/IP host filtering
- Logging and auditing
- OS-specific security settings
- Encryption of stored data
- Anti-virus protections
- General Controls (backup, physical security, HVAC, UPS)
- Software / application versions and patches
- Software / application configuration

## Database Security

Data security has three separate, but interrelated objectives:

- *Confidentiality* – "the prevention of improper disclosure of information"[8]
- *Integrity* – "the prevention of improper modification of information or processes" [8]
- *Availability* – "the improper denial of access to information" [8]

Security Controls for databases include access controls, lock controls, integrity controls, and auditing controls. Steps that are more granular include the use of roles to grant access, the use of journals, and controls for Open DataBase Connectivity (ODBC) access.

## Application Security

One of "the primary goals of application security is that it will operate with what senior management has decided is a **reasonable risk to the organization's goals and its strategic business plan**. Second, it will ensure that the application, once placed on the targeted platforms, is **secure**."[9] Many organizations think about application security much after the applications have been completed. Various reasons include the lack of security knowledge. Others think that security is an "add-on feature" and should not be built within the application itself. In addition, there is the idea that security adds overhead to a project. The Defense Information Systems Agency, in their Field Security

[7] Birkholz. Pages 10-11.
[8] Sandhu, Sushil.
[9] Tipton, Krause. Page 1109.



© SANS Institute 2005 Author retains full rights.

Operations Application Security Checklist, describes one of the most important reasons:

> The complexity of most mission critical applications precludes comprehensive security reviews of all possible security functions and vulnerabilities in the time frame allotted for Application Security Reviews. Nonetheless, Application Security Reviews help organizations address the most common application vulnerabilities and identify information assurance issues that pose unacceptable risks to operations.[10]

Organizations need to think about security as a value enhancer, as an enabler in the application development cycle. EnterpriseOne offers a variety of security features that helps IS in creating a security model or framework that enables users to conduct business in a secure environment. These features also help Security Operations in the ease of administration, support, and every-day-operations. Business owners are assisted in applying the proper segregation of duties. The security features boost user-friendliness and the perception of security as being less intrusive and interruptive.

### Physical Security

With the implementation of a new business system, business owners do not think much about physical security. "They are much more interested in what type of application security can be implemented, but implementing a new enterprise plan provides the opportunity to ensure that the best business practices are being used throughout the organization."[11] Business users need to understand the importance of physical security. From a Security Model perspective, this additional layer of security plays a key role and can help minimize the financial impact to the enterprise in preventing physical damage to corporate assets.

## Phase 3: EnterpriseOne Security Considerations

A new EnterpriseOne security model was required. This security model was the result of a collaborative effort between IS, REM Business representatives, IT Engineering (design and development) and Security Operations (administration, support and every-day operations). However, the ultimate responsibility for the security model belonged to the Information Security Office (ISO). Security must be role-based and no security should be assigned outside the security roles. **This posed a difficult challenge, as the EnterpriseOne Xe version does not support role-based access.**

[10] http://csrc.nist.gov/pcig/CHECKLISTS/appsec_checklist2-1-4_25june04.doc Page 4.
[11] Miller. Page 584.



© SANS Institute 2005 Author retains full rights.

The initial project assessment was approved and work began by forming a project team. All the security tasks were assigned to the ISO via a request for service. IS gathered all available information and initiated an engagement process as needed. IS then informed Security Operations and others that a project was at hand, what the project entailed, the project scope, project completion dates, project (security) strategic and tactical views, and project availability of resources.

The challenge was to create a security model that supported role-based access with a product that was not designed to do so. I was the ISO individual assigned to the project and created the prototype Security Model Document for EnterpriseOne. This was accomplished by taking input from the Business side, Security Operations, and others. Network Security (client/server environment), OS/Host Security, Database Security, and Application Security were addressed to ensure a secure system.

For REM, all hardware was housed in the Data Center. All the Data Center and IS policies, procedures, standards, and guidelines for server builds were followed for servers to be brought into a production line. In addition, all the Infrastructure Considerations were dictated by the enterprise IS Policies: Network Security, (client/server environment), OS/Host Security, and Database Security.

One of the Business Requirements was for REM to be setup as a separate scaled-down version of the current production system. Based on that premise, the EnterpriseOne Install, (that is, the Enterprise Server, the Deployment Server, FAT, and Terminal Server clients) was duplicated from the current production system. All the non-essential systems were taken away prior to this duplication. That is, Human Resources (HR) suite and HR data, Payroll suite and payroll data, Customer Support Management System (CSMS) and CSMS data and so on were eliminated, thereby, decreasing the risk for security data exposure for many systems.

| ***Note:*** |
|---|
| The minimum components to run EnterpriseOne are the Enterprise Server, the Deployment Server, a FAT client (a legacy name from Win32 clients), and/or Terminal Server clients. The Enterprise Server serves as a database and logic server. The Deployment Server stores source code for deployment to clients. The FAT client is a workstation that can be used to run enterprise software, perform development, run reports, and perform maintenance. Terminal Server clients are, in general, thin clients used to run reports, and perform basic processing. For additional information, please consult the EnterpriseOne documentation guides. |

## EnterpriseOne "Application Security"

EnterpriseOne security enables users to access objects. These objects can be data or logic items (applications). Data may exist at the granularity of a record, a



© SANS Institute 2005 Author retains full rights.

table, or a set of tables, or via a Data Source. Logic may exist at the granularity of an action, an item on a form, an application form, or an entire interactive or batch application.

"A role-based access control policy bases the access control decisions on the functions that a user is allowed to perform within the organization."[12] To create the Application Security Model, I had to work with the REM Business side and Business Systems Analyst to gather all the objects that pertain to the REM system. The REM Business Unit supported basic business roles: managers, team leaders or super-users, and staff or data entry personnel. I created a model to support the principles of segregation of duties, least privileges access, and the need-to-know basis. I completed research to discover all the actions that were performed by managers, super-users, and staff personnel. I translated that input into the EnterpriseOne objects that were capable of performing such actions. The goal was to couple each basic business roles (mangers, leads, and staff) with EnterpriseOne objects that supported each job function/description. For example, managers were in charge of approvals and able to work with approval actions; however, data entry at that level was not allowed. The staff personnel entered orders that were submitted for approval but were not able to approve such orders.

My main concern with the design of the Security Models roles was "protecting the integrity of the information, essentially who can perform what acts on what information."[13] A basic representation of the REM Roles Application Security Model is depicted below in Figure 1:

| **Group / Role Naming Conventions** | **Functions/Job Descriptions** | **Segregation Of Duties** | **Least privilege or Need-to-know Basis** |
|---|---|---|---|
| REMMGR<br><br>(REM Manager) | Managerial duties, approvals, and approval routs | No data entry and no support functions | Access to managerial data only |
| REMSUP<br><br>(REM Team Lead/Super User) | Support Role, Troubleshooting | No approvals or managerial duties | Access to testing data only |
| REMSTF<br><br>(REM Staff) | Data Entry | No approvals, support or managerial duties | Access to data entry only |

**Figure 1: REM Roles Application Security Model**

Once I created the Application Security Model Prototype Document, Security Operations and the REM Business side reviewed the document. Several iterations took place at this time to ensure a solid foundation for Application Security.

[12] Hansche, Susan et al. Page 202.
[13] Hansche, Susan et al. Page 202.



© SANS Institute 2005 Author retains full rights.

Approval for the prototype model was obtained from the Business and Security Operations before the model could be constructed with the EnterpriseOne security application.

EnterpriseOne offers the advantage of centralized security functions. The Security Workbench application is designed to set permissions for every object in the enterprise. The User Profiles application is used to handle all issues with IDs and User/Group profiles. The User Security application is used to associate users with data sources at the user or group level. For additional information, please consult the EnterpriseOne documentation guides.

***Note:***

The Security Workbench provides development and implementation of granular security controls based on: (Miller et al 561-591)

- Application Security
- Action Security
- Row Security
- Column Security
- Processing Options Security
- Tab Security
- Exit Security
- Exclusive Application Security
- External Calls Security
- Solution Explorer Security
- Portal Security

For the REM implementation, only the following types of security were used:

- *Applications Security* – Enables users to use applications and forms. This is highest level of security.
- *Action Security* – Enables users to perform certain actions when in applications or forms. Security can be set on OK, Select, Add, Change, Copy, Delete, etc.
- *Row Security* – Enables users to perform certain actions on specific records in a table. It can secure a user from seeing records belonging to other users.
- *Column Security* – Enables users to perform certain actions on specific columns in tables, applications, or forms. For example, it can secure a user from viewing all salary-related fields in a table.
- *Processing Options Security* – Enables users to view or modify values on Processing Options for applications.

EnterpriseOne security was designed to function based upon access levels, those being User, Group, and *PUBLIC levels. A security check by User ID is first



© SANS Institute 2005 Author retains full rights.

performed. If security for the User ID is not set up, then Group ID will be checked next. If security for the Group ID is not found, then all records assigned to *PUBLIC will be checked. If there are no security records found in the Security Workbench, then the user has access to the object/objects in question.

| ***Note:*** |
|---|
| The install default setting for EnterpriseOne is based on an Open/Restrict model; that is, all access is allowed, unless the access is specifically denied. |

**By original design, EnterpriseOne Xe version does not support Role-Based-Access.** Gordee has advocated using logical role-based access using the group level. His approach identified the difficulty in managing this type of security model. "The main problem stems from the rule that a user may have only one group."[14] Therefore, the strategy that I utilized to overcome this challenge was to construct *PUBLIC, Group and User level security records in a comprehensive way to include all the access that would support a role or job function/description.

The system that I developed was based on levels that would support a job description and the access or security needed to support each level. *PUBLIC was the lowest of all the levels and all users had access to security that was set up at this level. A user or multiple users were assigned to the Group security level. Only the users in that group had access to the security that was set at that level. It was the "middle of the road" access level. Security at the user level was the highest level and superseded the Group and *PUBLIC levels. **The sum of all levels depicted the security or access for a specific user or group.** For example, the REM Application Security Model was based on a Restrict/Open model; that is, all access was denied, unless the access was specifically allowed. To accomplish this goal, the security model incorporated a couple of records in the Security Workbench that denied all Application Security access at the *PUBLIC level. The same was done for Action Code Security and Processing Options Security.

**A note of caution:** I made sure that the Security Operations group had corresponding records at the group level (one level higher than *PUBLIC) to counteract all the *PUBLIC actions. Otherwise, no user would be able to access the system. If this happened, the only solution would be to access the database and make changes to the Security Workbench table directly. *PUBLIC was the base for all security sets in EnterpriseOne, and was like a container that I used to group the minimum, most basic and common access that users needed to access the system.

From the REM Business side, I knew all the objects that comprised the REM system. Those objects or applications that were common to all groups and users and did not represent security risks were assigned to *PUBLIC. That meant that

[14] Gordee. Page 1.



© SANS Institute 2005 Author retains full rights.

each user in the system would have access to the applications. Those applications were the base for REM access. Security at the Group level was a step higher, and was set up based on the particular job description for that group. For example, REM managers had access to all the managerial duties, approvals, and approval routs on a need-to-know basis and that was reflected at the group level.

Application Security records and Action Code security records work with each other in a precise relationship. Application Security will allow unrestricted access to the application. Action Code Security records dictate the actions that can be taken by the user for that application. It is at this point that the security set up becomes confusing. A user may have Application Security access to an application via *PUBLIC; however, if *PUBLIC does not contain an Action Code Security record that restricts the user to add, change, delete or copy data, the user will have unrestricted access to the application. At the group level, an Action Code Security record can be entered to grant/restrict access to the group for add, change, delete, or copy data for the same object. Furthermore, actions can be restricted for all the users in a particular group and access granted to add, change, delete, or copy data at the user level, the highest possible level. This is the EnterpriseOne foundation for segregation of duties - the Security Workbench's ability to be extremely granular at the record level.

The REM Role-Based security equation depicts the use of EnterpriseOne's multiple security levels:

***PUBLIC Level + Group Level + User Level = Security for the Role/User**

**Figure 2: REM Role-Based Security Equation**

The above equation can balanced in a multitude of ways. For REM, I established the base of all the access using *PUBLIC. Then for each REM group, all the objects/applications that supported their job description were added. The result was a system that was balanced, fully restricted, and that supported role-based-access, segregation of duties, least privilege access, and data access on a need-to-know basis when data was accessed via the REM applications.

***Note:***

I created each REM Application Security record with a corresponding Action Code Security record. The main reason for this approach was to avoid confusion when access needed to be determined for *PUBLIC, Group or User Level. When looking at the Security Workbench, it was easier to see records for objects in pairs. For each Application Security record, there was an Action Code Security record and so on. This helped Security Operations to administer and maintain the security for the system.



© SANS Institute 2005 Author retains full rights.

**Process Flows and Checklists** - I have used the same strategy for creating EnterpriseOne security models for the last four and a half years with no measurable issues. My recommendation is to take what works for you and your enterprise and create process flows, procedures, and checklists that comply with the Cobit Framework DS5 - Ensure Systems Security. The process needs to be repeatable and verifiable in the eyes of any audit and/or auditor that may evaluate your enterprise.

**What is next?** Once the REM business owners and management approved the prototype security model, Security Operations built the actual model using the EnterpriseOne Security Workbench application. The model was created in the EnterpriseOne's Development Environment. At this point, process flows were very beneficial.

A prepared checklist with tasks such as the ones listed below is helpful when the project is limited by time and helps decrease human errors:

- Create user and group profiles using the User Profiles application
- Populate the Security Workbench with *PUBLIC, Group/Roles and User Level security
- Create Testing IDs for Development and Prototype Environments
- Create User Security association with data sources
- Add Environments to User IDs and groups
- Run Security Operations Internal Quality Assurance (error detecting routines)
- Email testing users of available access (Development and Prototype Environments only)

A security-functionality-testing phase was set in motion to ensure that all the security depicted in the security model was working as designed. Several iterations took place to ensure a solid security and project QA. Approval after the testing phase was obtained from the *Business side, Data Owner,* and Security Operations. Before the security model could move forward, a sign-off from all parties took place. The main supporting argument to have the Business or Information owner's involvement every step of the process is because they "are responsible to assure the accessibility and availability of information and business functions critical to the effective operation of the company."[15]

The next question was, "Are we ready to 'go live' with the project?" A pre-"go-live" project status meeting took place to ascertain the feasibility of going-live with the project. Once all the parties agreed, a series of tasks were set in motion. Again, process flows and checklists were perfect for this stage of the project. The tasks include:

[15] Peltier. Page 291.



© SANS Institute 2005 Author retains full rights.

- Disable and/or remove testing IDs – per project plan
- Add Production environments to production IDs – per project plan
- Move Production users into production groups – per project plan
- Notify users of access – per project plan
- Communicate that the project is "Live" – per project plan
- Start post go-live tasks – per project plan
- Update all the Security Model documentation
- Turn security access approval process to data and process owners
- Request all support documentation and move to project repository
- Update all EnterpriseOne security related documentation
- Establish a "clean up" process
- Establish a "grace period" to troubleshoot issues
- Turn all first level support to Security Operations

A post-mortem meeting took place to evaluate success or failure for the project. Normally, within the post-mortem, a section is assigned to security and all the security issues are reviewed and evaluated at that time. Prior to the meeting, it is advisable to take time and evaluate issues, talk to users, project team members and others to get feedback and see how the security for the project is working. **Always be prepared** to answer any questions and to have supporting evidence and documentation for any security decisions or issues that you may encounter. It speaks well of your reputation and the reputation of your Security Organization.

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005 Author retains full rights.

## Conclusion

The main goal for the REM system was to create a security model or framework that would enable REM users to conduct business in a secure environment maintaining confidentiality, integrity, and availability. To create such framework the collective strength, knowledge, and experience of Information Security needed to come into play. A significant challenge was to use role-based access with a product that was not designed to support that approach.

In order to meet that challenge, I established a collaborative partnership between IS, IT Engineering, Security Operations and the REM Business users. However, the ultimate responsibility for creating the security model was the Information Security Office. Information Security policies, standards, and procedures are the foundation, and play a key role in creating security requirements and how these apply to today's business environments. Network Security (client/server environment), OS/Host Security, Database Security, and Application Security, were addressed to ensure a secure system. To create a more comprehensive EnterpriseOne security solution, all three levels of security must be used, that is *PUBLIC, Group, and User level.

Mission critical applications should not prevent comprehensive security reviews of security functions and vulnerabilities. Using predefined process flows and checklists, which comply with the Cobit framework DS5 documentation, is a way to expedite security models for mission critical applications.

EnterpriseOne security is flexible and granular enough to be able to enforce and support security principles. That flexibility allowed me to create a security model that was balanced and fully restricted. It also supported role-based-access, segregation of duties, least privilege access, and data access on a need-to-know basis when data was accessed via the REM applications.



© SANS Institute 2005 Author retains full rights.

# References

## Cited Internet Sources/URLs

Bogazici University Computer Center (bim@boun.edu.tr). "What Is Network Security?" (No date listed).

URL: <http://www.cc.boun.edu.tr/network_security.html>

Gordee, Scott. "J. D. Edwards OneWorld Security Using RBAC". 2003.

URL: < http://www.giac.org/practical/GSEC/Scott_Gordee_GSEC.pdf >

National Institute of Standards and Technology - Security Technical Implementation Guides (stigs) and Checklists. "Application Security Checklist." Version 2, Release 1.4. 2004.

URL: < http://csrc.nist.gov/pcig/CHECKLISTS/appsec_checklist2-1-4_25june04.doc>

PeopleSoft. "Product and Industries - EnterpriseOne Product Lines". 2004.

URL: <http://www.peoplesoft.com/corp/en/products/ent_one/index.jsp>

## Other Internet Sources/URLs

Chan, Eddy. Computer Security Models. (No date listed)

URL: <http://infoeng.ee.ic.ac.uk/~malikz/surprise2001/spc99e/article1/>

IT Governance Institute. IT Control Objectives for Sarbanes-Oxley. 2003.

URL: < http://www.isaca.de/Dokumente/Sarbanes-Oxley_110303.pdf>

National Institute of Standards and Technology - Computer Security Resource Center – CSD. Information Technology Security. 2004.

URL: <http://csrc.nist.gov/pcig/cig.html>

SANS. SANS Information Security Reading Room. 2004.

URL: <http://www.sans.org/rr/>



© SANS Institute 2005 Author retains full rights.

## Cited Printed Works (Books)

Birkholz, Erik Pace. Special OPS Host and Network Security for Microsoft, UNIX, and Oracle. Rockland, MA: Syngress Publishing, Inc., 2003. Chapter 1, Assessing Internal Network Security page 10-11.

Hansche, Susan et al. Official (ISC2) Guide to the CISSP Exam. Boca Raton, Fl: Auerbach Publications, 2004.

Miller, Joe, et al. J. D. Edwards OneWorld: The Complete Reference. Berkeley, CA: Osborne/McGraw-Hill, 2001.

Sandhu, Ravi S. and Jajodia, Sushil. "RELATIONAL DATABASE SECURITY: AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY." Information Security Management Hand Book on CD-ROM. Boca Raton, Fl: Auerbach Publications, 2002.

Peltier, Thomas R. Information Security Policies and Procedures: A Practitioner's Reference. Boca Raton, Fl: Auerbach Publications, 2004.

Tipton, Harold F. and Krouse, Micki. Information Security Management Handbook 4th Edition Volume 3. Boca Raton, Fl: Auerbach Publications, 2002. Chapter 20, Pages 353, 372, and 374.

- - -. Information Security Management Handbook 5th Edition. Boca Raton, Fl: Auerbach Publications, 2004. Chapter 94, Application Security page 1109.

## Other Reference Material (Books)

Bragg, Roberta. Windows 2000 Security. Indianapolis, In: New Riders, 2001.

Cole, Eric, et al. SANS Security Essentials and CISSP 10 Domains Track 1-6. Printed in the United States of America: The SANS Institute, January 2004.

Gibaldi, Joseph. MLA Style Manual and Guide to Scholarly Publishing. New York: The Modern Language Association of America, 1998.

Jacot, Allen, et al. J. D. Edwards OneWorld Xe: Object Management Workbench. Berkeley, CA: Osborne/McGraw-Hill, 2002.

Maiwald, Eric. Network Security: A Beginner's Guide. Berkeley, CA: McGraw-Hill, 2001.



© SANS Institute 2005 Author retains full rights.

Last Updated: September 1st, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |