GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Implementing Information Technology (IT) Security in the SDLC – A 'How To' Approach (Version 1.1)
Larry G. Wlosinski, CDP, CISSP
October 2002

Contents

Summary/Abstract

The Systems Development Life Cycle (SDLC) is a process that applies to the development of medium to large software applications developed in-house or by contractors. Although there are several published variations of the SDLC, it primarily consists of five phases: initiation, development/acquisition, implementation, operations/maintenance, and disposal. These phases focus on the business process, the functional requirements, and the economic and technical feasibility.

This paper is oriented to federal government agencies, but can be used by commercial organizations to demonstrate how to incorporate security into the SDLC. The sections that follow identify and describe the various IT security activities of the five phases of the SDLC and then suggest possible reporting measures to satisfy new reporting requirements. The information provided is intended for use by system developers, management, and IT Security staff to explain their roles and how they work together, and additionally how progress can be measured. 'Appendix A: Programming Concerns' contains programming advice and can be used as a checklist during system development. 'Appendix B: Responsibilities' is a sample breakdown of IT Security responsibilities for individuals associated with the SDLC and is included to help organizations understand the roles of everyone involved. 'Appendix C: Glossary and Acronyms' contains a definition of terms used in this paper.

Background

The primary objectives of the SDLC are to ensure that the system: is developed in accordance with the stated requirements, works effectively, is cost effective, and is

© 2011 The SANS Institute Author retains full rights.

maintainable. The inclusion of security controls and measures during the process helps to ensure that: safeguards are part of the design, the developmental and/or acquisition costs include security, and progress can be tracked.

The SDLC has been a security concern within the federal government for some time and guidance on many aspects can be found in OMB Circular A-1301[1], Appendix III, Security of Automated Information Resources and the supporting NIST special publications[2] (see 'Appendix D: References' for more information).

For federal government agencies more detailed reporting and accountability of the Information Technology (IT) Security activities in the SDLC is now a more critical part of the security equation as noted in magazine articles such as Federal Computer Week[3] and Government Executive. The GovExec.com article[4] titled "OMB (Office of Management and Budget) orders agencies to report on computer security" and states that *"the total number of security weaknesses identified in programs and information systems, the number of repaired flaws and the number of new weaknesses detected in each quarter"* be reported. This paper supports the OMB reporting requirement because incorporating performance measures into the SDLC saves money by helping to prevent expenditures later in the process that would result from re-work. I.e. it costs more to fix errors and omissions later in the life cycle, because of time and labor that has already been invested and the costs associated with revising the completed work (e.g. programs, testing, procedures, documentation, etc.).

Preparation

Before you can begin with the implementation of any IT Security reporting requirement for an organization, you must understand the organization's structure and application development environment. Meeting and speaking with the people in all the affected departments, divisions, and sections is key to understanding the organization's management environment and structure, and in obtaining the support and cooperation of various department personnel.

When meeting with the staff of each of the 'departments' it is important that information about the application of concern be obtained. Examples of the materials that need to be gathered and used by the systems design and development staff include: the requirements specifications (that describe the purpose of the system), business case studies (that provide an understanding of the organization), and any documentation available about the environment(s) that will be affected by the new system.

Once you have an understanding of the area and people affected you will need to meet with them to explain the security concepts of confidentiality, integrity, and availability so as to provide a common basis of understanding. A few of the topics to be discussed include access controls, system and data integrity, separation of duties, control/balancing totals, and secure programming techniques (refer to programming concerns in Appendix A for more information). Meetings of this type will need to be

© 2011 The SANS Institute Author retains full rights.

conducted with each of the affected departments, especially the systems development staff.

During these meetings ideas and concerns will arise that will need to be addressed and the fruit of the meetings will be a common understanding of how security personnel will work with them. This common understanding will need to be recorded/documented in the form of meeting minutes. The minutes would document the various activities agreed to, the person responsible of each activity, and projected completion dates of each activity. Another important topic for these meetings is performance measures. They need to be discussed, not only because they are important to internal tracking purposes, and they need to be gathered to satisfy periodic government tracking and reporting requirements. The role of IT security in each of the five phases can also be discussed in these meetings. More detail has been provided in the sections that follow.

For larger organizations it is important that someone knowledgeable in systems, networking, and security be assigned to the project. This person should be from the IT security office and could either be in-house staff or a contractor.

Another critical area is upper management support. Upper management must be informed of all government reporting requirements and the importance of the timeliness of the data. If they are not informed, or have other priorities, the ability to track progress and report accurate and timely information will be compromised. They should at least be copied on all correspondence that concerns deadlines and the responsibilities of the people who work for them. Periodic updates/meetings with upper management are recommended.

If the reporting of a performance measure to the government is a new requirement an organizational policy should be developed. The policy would state the government's requirement, identify the performance measures, state when the information is to be reported, and explain areas that may be confusing.

Some of the overall performance measures that should be considered during this process are:

- Number and types of applications
- Number of labor hours security staff was involved in each phase of SDLC of application
- Magnitude and duration of system development effort (weeks, months, etc.)
- Number of individuals involved in security review/support activities
- Amount budgeted for security staff involvement of application/system
- Estimated cost of security staff involvement.

For record keeping and organizational purposes it would be beneficial if a database of the information to be acquired is maintained. An on-line database system becomes very useful to those involved in entering the data and for meeting requirements imposed by governing agencies in need of a quick response. System tracking information should

© 2011 The SANS Institute Author retains full rights.

include the office/branch/section/division of concern, name of the director or manager, application name, name(s) of application developer, Independent Verification and Validation (IV&V) team member names, pertinent start and projected completion dates, and if applicable, the name(s) of any independent contractor(s). Other fields included in the database would depend on the decisions that resulted from the meetings on the measures to be used and presented throughout this paper.

A standard form (preferably on-line) should be developed to inform the IT Security office of the completion of security items. It should be submitted to the security office responsible for tracking and reporting. If a paper form is used it should be signed, dated, and include an area for comments.

Phase 1: Initiation

During the initiation phase the need for the system is established and the purpose of the system is documented. Deliverables produced at this time include the funding request, a Project Plan, the Cost/Benefit Analysis, Risk Assessment, and User Requirements.

The IT Security office should be involved in the following activities:

1. Performing a data sensitivity assessment that includes a review of all information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, and organizational policy and guidance. The IT Security office would perform this activity.

2. Developing the initial or preliminary Risk Assessment that identifies weaknesses and recommends safeguards. The Risk Assessment is purely a security office task and the recommendations for improvement should be taken seriously and incorporated into the system requirement documents. If the assessment identifies procedural weaknesses in confidentiality, integrity, or availability they should be addressed immediately. You want to ensure that all the information is secure and that the rights of privacy are maintained. The organization's right to confidentiality is also a concern that must be guarded.

3. The IT Security office should also be involved in reviewing solicitation documents (e.g., Requests for Proposal). The reason for this is that they are familiar with the organization's policies, know what contract language should be included, and have experience with many vendors. One of the reasons they exist is to protect the organization and this is especially important when new and/or un-trained staff is involved in the review and approval process.

Possible security performance measures include the dates the IT Security office has completed the assessments/reviews.

Phase 2: Development/Acquisition

© 2011 The SANS Institute Author retains full rights.

During the development phase the system is designed, programmed, developed, or purchased (if acquired from a software vendor). Key deliverables are the functional and technical requirements, system test plan, and the security test plan. The increasing complexity of systems and the growing number of interconnections with other systems or networks underlines the need for thorough testing to ensure data availability, confidentiality, and integrity.

Functional requirements address the quality assurance requirements, configuration management, and special (possible cyclical or seasonal) events, retention and disposition requirements, and anticipated future enhancements. Technical requirements contain the performance requirements, interfaces, data characteristics, sample screens, failure scenarios, security design concerns, and any special operating and infrastructure needs.

The following security activities occur during the Development/Acquisition phase:

1. Review the technical features of the design. Some areas of concern are: volume projections (system responsiveness is the concern), system capabilities and controls, platform vulnerabilities, programming language constraints and vulnerabilities, and system interface controls. Problems in these areas will cause delays and can likely force compromises in the final product/system.

2. For critical and sensitive systems, conduct background checks on the developers. A review of key staff members (that could include background checks) is mostly likely necessary if the data available to them is of a sensitive, confidential, or mission critical nature. The IT Security office can help determine the requirements here.

3. Review operational practices (e.g., awareness and training). In some organizations the importance of security in operations is only as good as the people who worked there before. Operational support staff must follow strict control and access rules to ensure the data and the system's components are not compromised. The IT Security office and auditors are very aware of what can go wrong and what safeguards are necessary. Periodic external audits and internal risk assessments help to eliminate the weaknesses.

4. Review test plans, scripts, and scenarios. The IT Security office can point out weaknesses that may exist in application programs and can help guide the development of testing scripts and scenarios. Their involvement in the development of the test plans can help minimize program related security problems. Appendix A: Programming Concerns, contains more information on this concern.

5. Work with the development team to incorporate security controls into the specifications. Security controls (i.e. countermeasures, safeguards, etc.) include the review of: personnel, administrative practices, physical security, and technical concerns (e.g. platform issues, vendor). The goals of the controls are to prevent problems and disclosure of sensitive information, detect unauthorized activity/intrusions, minimize potential exposure, and recover from problems quickly.

© 2011 The SANS Institute Author retains full rights.

6. For systems developed in-house, the IT Security office would: define security features, monitor the development process for security problems, respond to changes, and monitor threats and vulnerabilities such as accidents, acts of nature, design limitations, Trojan horses, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.

7. For Commercial Off The Shelf (COTS) systems, the IT Security office can help in system assessment by reviewing: market surveys to ensure security is covered, contract solicitation documents, and evaluate proposed systems. This support function differs from in-house systems in that COTS systems come predetermined and the recipient/buyer has little control in their design, features, and controls. Should the features and controls fall short in security the IT Security office can help determine what and where internal changes are needed.

8. Development of secure operational practices is the last concern and can be found in the System Security Plan (SSP), the Contingency Plan (CP), awareness and training material, and various types of documentation (e.g., user manual, operations and administrative manuals). These documents provide varying degrees of security support in the areas of preparation, training, and execution of the system. When problems arise thorough documentation will help ensure that the system and data are accurate and available when needed.

One of the most critical and important areas of concern during the SDLC is programming. Programmers perform the critical task of developing the source code for the application but are primarily focused on developing a usable and error free system. As a result programmers often assume that the programming language is flawless and are consequently unaware of how this assumption can jeopardize data and system security. It is important that the programmers be aware of unknown language flaws, system errors, and poorly coded routines. The information provided in Appendix A can be used as a preliminary checklist for the application development staff.

The performance measures that can be gathered/acquired during system development and/or acquisition are:

- Cost associated with background checks
- Number of vulnerabilities found
- Number of solicitations evaluated
- Cost of developing the Contingency Plan
- Cost and number of manuals, plans, documentation, etc. developed and distributed.

Phase 3: Implementation

During the implementation phase the system moves/transitions to production. If this is not done correctly, it can cause unnecessary delays, cause additional expenditures and

© 2011 The SANS Institute Author retains full rights.

possibly embarrass the organization, management, and the developers. Critical activities of the implementation phase include: final testing, system certifying, and system installation. Key deliverables include the security certification package, user documentation, training material, trusted facilities manual, contingency plan, and disaster recovery plan.

The following security activities occur during testing and system certification:

1. Develop test data. The IT Security office can help ensure that the test data created covers known vulnerabilities. Vulnerabilities may exist in the operating system, the programming language, the utilities used, COTS software, and in the programmer's code.

2. Test unit, subsystem, and entire system. All three levels of testing can uncover bugs and security vulnerabilities. This is especially important for large and/or complex systems. The IT Security office is more aware and knowledgeable about these types of tests than the application developers may realize so their participation in the testing is important to the system's development.

3. Ensuring that the system undergoes technical evaluation in keeping with federal laws [i.e. Sec. 508], regulations, policies, guidelines, and standards. The IT Security office should be familiar with the requirements and can make sure they are considered in any new or existing applications.

During implementation installation security features are enabled or configured, and data field sensitivity and control are also evaluated. It is important to recognize that the scope of the IT security related work of the SDLC is extensive because all related or associated components (including the environment) of the application and tangential security concerns affect the process and the final product. Additional IT security tasks performed at this time include reviews of the following.

- Security management (administrative controls, safeguards)
- Physical facilities
- Personnel, responsibilities, job functions, and interfaces
- Procedures (e.g., backup, labeling)
- Use of commercial or in-house services (e.g., networking)
- Contingency Plans
- Disaster Recovery plans
- COTS products (they may not have had all security patches installed)
- Removal of all installing programs (they may become a mechanism for a compromise)
- Machine content (Machines containing system programs that should only reside be on servers)
- File and program overlay settings and privileges
- Backup, restore, and restart instructions and procedures
- Implementation backups (they could serve as a benchmark)

© 2011 The SANS Institute Author retains full rights.

- Ensuring the implementation of only approved/accredited systems.

Performance measures that can be obtained upon completion of the implementation phase are:

- Number of test plans developed
- Number of tests performed
- Number of interfaces with the system
- Labor hours involved in testing
- If testing was contracted out, the cost of the testing
- Number of locations (buildings/cities) involved
- Number of desktops involved
- Number of support staff involved
- Percentage of tests performed that were successful
- Number and type of security deficiencies found.

Phase 4: Operations/Maintenance

During the operational phase the system performs its work, enhancements are programmed and tested, and hardware and/or software is added or replaced. The primary concern is system availability. On-going activities include performance monitoring and management feedback, managing system problems, recovering from system problems, and implementing system changes.

Operational and administrative activities where security staff may be involved follow. They may be in the form of an audit or risk assessment, or simply part of an accreditation checklist.

1. Reviewing backup and restore parameters. The concerns are equipment failure, media failure, incorrect programming of the backup scripts and configuration settings, and utility program (backup/restore) errors.

2. Performing backups. Storage media location and frequency of backups are the concern of every computer system.

3. Conducting training classes. Training of the users about the reason for and usage of security controls is critical to protecting data confidentiality and (depending on the system) a person's privacy.

4. Managing cryptographic keys. The duration of a system may be many years and if it is an enterprise system, and if the data is stored encrypted, data storage and retrieval could become a problem. The areas of concern are archiving of obsolete or historical data and the ability to retrieve it. If the encryption keys change during that time three options must be weighed: (1) keep the data encrypted, store the key, and maintain the ability to retrieve it, (2) convert the old data to the new format, or (3) not

© 2011 The SANS Institute Author retains full rights.

do anything in the hope that no one needs it. Note that the latter may be a moot point if no funds have been made available for the first two options.

5. Maintaining user administration and access privileges. The term used to describe this is Access Control List (ACL). This activity involves the review of who should be allowed access to the system and what data should they be permitted to see, update, and/or delete. Personnel should only have the minimum access rights for what they need to perform their job. The security concern of separation of duties is critical for systems that control purchases and payments.

6. Ensuring that audit logs are available. The content of, or lack of, audit logs is a critical concern when it is suspected that a machine that can access the applications data has been compromised. Hacker tools can delete the content of the logs to hide the tracks of hackers, or in-house staff may change the data directly. Protected system logs provide a means to identify the actions performed and the person(s) responsible, the date(s) and time(s) of occurrence, how they did it, and possibly what they did. Log files can be configured to record considerable information, but a decision must be made about how much data (i.e. number and types of fields and activities) to store. The IT Security office can recommend the appropriate settings.

7. Training administrators on log file analysis. For large organizations and especially those that have multiple locations there may be many security officers. Their understanding and interpretation of the logs is critical to determining if a compromise occurred, the extent of the intruder's activity, how to recover, and how management should react. The IT Security office can provide classes, individual training, and/or funding. The function of checking system logs should be performed by a Security Officer because, as with any system, there is a risk of unauthorized activity by System Administrators.

8. Updating security software. During the life cycle of the system the security software used to monitor and audit activity may change. The security officer should be involved in updates to any security software associated with the application. There is a risk of nonperformance, incompatible run scripts, and erroneous software patches. The types of software include firewalls, intrusion detection, anti-virus, vulnerability and penetration testing, test data development software, and audit tools.

9. Reviewing the physical protection. This activity may appear to not be related to the SDLC but it is always a concern. It is especially important if the system is moved, or developed for a new location, or there is building renovation. Anyone who has access is capable of unauthorized, destructive, or compromising activity.

10. Reviewing off-site storage usage, services, and availability. System Security Plans, Contingency Plans, and Disaster Recovery Plans all specify the system storage requirements. The involvement of the IT Security office when the system is under development helps ensure proper implementation.

© 2011 The SANS Institute Author retains full rights.

11. Reviewing the output distribution process. The process of distributing hardcopy reports, forms (especially purchasing and billing), checks, etc. is critical to all organizations. Unscrupulous people look for opportunities to exploit weaknesses in security and the IT Security office can recommend proper procedures and controls.

12. Reviewing software and hardware warranties. One of the most embarrassing events when developing a system is to find that the software and/or hardware for the system is no longer supported. This affects not only the organization's posture in the community, but also the ability to grow and survive. The IT Security office and the contracts office can perform the necessary research to help prevent this from occurring. No organization wants to start over especially when funds have already been invested.

IT Security staff perform the following operation assurance activities:

- Review the action of people who operate/run system (e.g., change control procedures, backup routine, log review procedures, etc.)
- Review technical controls (e.g. scripts and batch programs)
- Ensure that access control permissions are documented
- Review system interdependencies
- Compare documentation to current system
- Ensure that deregistration procedures are in place and followed
- Monitor the accuracy of operational, system, user, and programmer documentation.

Self-administered or independent security audits (Risk Assessments) should be periodically performed to ensure compliance. The types of audits that can be conducted vary from the use of automated tools, to performing an internal control audit, to reviewing security checklists, and performing penetration tests.

The security office may also monitor the system and/or its users. Monitoring methods may include any or all of the following: review system logs and reports, use automated tools, review change management, monitor external sources (trade literature, publications, electronic news, etc.), and perform periodic re-accreditation. Before monitoring is implemented, users should be advised through a warning banner or some other means that usage monitoring is in place.

Performance measures that can be obtained upon completion of this phase of the SDLC are:

- Number of users involved/affected
- Number of training classes held
- Number who took training classes: users, LAN/System Administrators, managers, etc.
- Cost of developing and conducting training class (binders, copies, disks, etc.)

© 2011 The SANS Institute Author retains full rights.

- Number of staff reviewed for security concerns
- Cost of independent audit
- Cost of penetration testing
- Cost of purchasing automated tool(s)
- Frequency and number of accreditations.

Phase 5: Disposal

The disposal phase is concerned with resolving the disposition (move, sanitize, dispose, archive, etc.) of the information, software, and hardware. Security is a concern not only prior to and during the system's life but also when disaster occurs and during disposal. If this phase is not done correctly confidentiality can be compromised and the ability to retrieve/recover archived data may be lost.

Security related activities include:

1. For encrypted data, ensure long-term storage of cryptographic keys. As technology improves encryption techniques are improving and consequently changing as well. This provides a challenge to those who need to recover archived and encrypted data. Those responsible for archiving data will need to ensure that the ability to decrypt the data accompanies it. The Records Management section of your organization should be able to provide guidance in this area. In some cases it may be required that the hardware (i.e. computer, media reader, and display device) accompany the system to ensure the technology exists at the time of retrieval. Future availability is the security concern here.

2. Review the legal requirements for records retention. The Freedom of Information Act (FOIA) provides the public a vehicle with which to request information on varying aspects and parts of the federal government. You should consult with the FOIA office for the particulars.

3. Consult with the organization's office regarding retaining and archiving hardcopies of federal information. Prior to moving the documents to an archive facility it may be necessary to stamp them with the appropriate sensitivity, or alternatively it may be appropriate to destroy (i.e. shred or burn) them. Confidentiality is a primary concern.

4. A final disposal phase concern is sanitizing the media. Sanitizing can be done by overwriting, degaussing, or destroying the data on the storage media. Privacy and confidentiality are the concern of sensitive and/or personal data. Each organization should have a policy on proper disposal techniques and services.

Performance measures that apply to the disposal phase are:

- Cost of long-term storage of cryptographic keys
- Number of files to be retained
- Number of disks, desktops/staff affected

© 2011 The SANS Institute Author retains full rights.

- Length of time to complete sanitization.

Conclusion

This 'How To' paper presented a lot of information about how to incorporate information security into the application system development life cycle, but it only provides a basic outline of activities. Appendix B is a suggested outline of individual responsibilities that can be used in the preliminary meetings to provide a common level of understanding.

The URLs in Appendix D provide information and guidance as supplied by the National Institutes of Standards (NIST) and other government agencies. Guidance on how to incorporate security into programming can be found in the links that focus on Java, web security, and Microsoft. They can provide programmers with important insight into security and system availability concerns. The reference books listed in Appendix D provide additional guidance for managers interested in more information.

Not everyone understands every aspect of security and because of this the importance of using the knowledge and skills of others is crucial to success. This paper has provided a foundation for that understanding, but readers must be aware that because of ongoing technology and personnel changes, keeping up with the vulnerabilities is a never-ending responsibility.

Appendix A: Programming Concerns

This appendix is a compilation of material extracted from web sites[5] that provide programming advice. It can be used to develop an IT Security Application Development Checklist and/or as the basis for another paper. The links are included in the references section (Appendix D).

Areas where programmers should be concerned include:

A. Access Control Requirements:
   - Requiring a user identification and password to restrict system and data access
   - Developing applications that will not be overridden by SQL commands
   - Programming with valid accounts (i.e. not 'Anonymous)
   - Encrypting passwords
   - Using difficult to crack passwords
   - Removing disks from machines immediately after use
   - Not programming with administrator privileges.

B. System and Data Integrity Concerns:
   - Disks supplied and used by contractors (possible viruses)
   - Software upgrades and patches
   - Program versatility (i.e. accessible to all terminals and/or desktops)
   - Only allow/program acceptable/pre-defined parameters

© 2011 The SANS Institute Author retains full rights.

- Restricted use of configuration files
- Pass parameters instead of storing them in system registers
- Edit entered data for size and value to prevent buffer overflow
- Avoid the use of path names in programs
- Allow only acceptable error codes
- Not retrieving data from publicly writable files/directories
- Use of undocumented, seldom used, and unusual functions or commands
- Excessive number of files and/or very large files (they could test the limits of the system)
- The number of processes running at one time (too many can tax/overwhelm the user machine)
- For web applications, cookie data updated via on-line access
- Data encryption for sensitive or critical data.

C. Unauthorized Access. Preventative erroneous programming practices including:
- Avoiding the retrieval commands that log data that hackers can find
- Avoiding hidden fields (hackers can compromise them)
- Not storing sensitive information on web control pages
- Avoiding the use of cookies (they could be compromised)
- Using compiled instead of interpreted code
- Boundary checking of test and data areas
- End checking for the completion of received or transmitted files
- Developing the application so it doesn't require root access
- Depending on security needs you might need to log all transactions
- Programming control totals to ensure only applicable records exist and they haven't been altered
- When practical, have a third party perform the testing
- Write protecting all installation disks
- Separate reporting of financial transaction involving receipts and payments.

D. Privacy and Confidentiality. Safeguards include:
- Having 'Sensitive Information' programmed to print on appropriate reports
- Not storing personal information into cookies
- Not using persistent cookies (i.e. cookies that remain on the system/machine after the application has terminated).

E. Production Implementation.
- Check the development environment to ensure that all COTS products have had their security patches installed.
- Remove installation programs (they could be used as a mechanism for compromise)
- Remove non-essential programs from user machines
- Verify that the operating system and relevant COTS products have the latest upgrades and patches.
- Check the runtime privileges.

© 2011 The SANS Institute Author retains full rights.

- Review backup and restore procedure as well as checkpoint restart procedures.
- Have a backup of the system made immediately after initial installation.
- Only implement systems that have had IV&V and been certified and accredited.

F. Documentation.
- Document access privileges
- Implement procedures that require immediate notification when users leave for other employment (i.e. deregistration procedures).
- Check that operations, system, user, and programming documentation are kept up-to-date.

Appendix B: Responsibilities

The responsibilities for IT Security fall on many individuals. For organizations not very familiar with how information security relates to system development efforts the following suggested list of responsibilities is provided.

Manager/Director

- Have a Business Case developed (I.e. require a Cost/Benefit Analysis)
- Review cost of project and gain financing (budget for it) if approved
- If mission critical or sensitive application, have staff reviewed/investigated
- Contact the IT security office to perform risk assessment if it is a mission critical system
- Monitor/approve releases of system into production (configuration management)
- Have Contingency Plans developed
- Consult with agency office regarding retaining and archiving federal records

Contract Officer

- Review Request for Proposal for IT Security concerns/wording
- Review hardware and software warrantees
- Consult on legal requirements for records retention

Project Officer

- Prepare project plan (includes security support estimates: labor hours, project duration, staffing, cost, developer advice, etc.)
- Review/access statement(s) of work
- Monitor/approve project costs on monthly basis
- Develop implementation plan
- Work with Manager/Director to create contingency plans
- Contact the IT Security office to obtain their involvement

© 2011 The SANS Institute Author retains full rights.

- Monitor application and production environment enhancements
- Perform self-administered or independent security audits (risk assessments) periodically

Budget Specialist

- Track labor usage of all personnel
- Track expenses (binders, copies, supplies, other material, etc.)

Security Officer

- Periodically/regularly review operating system logs
- Work with developers and LAN support staff to maintain secure environment
- Monitor disposal activity
- Review operational environment for vulnerabilities and threats
- Ensure that threats are reduced or eliminated
- Develop System Security Plan
- Participate in LAN risk assessments

Application Developer/Programmers

- Review design taking into account the network architecture and security controls
- Design application taking into consideration intruder methods of compromise
- Incorporate security requirements into system specifications (deliverable)

Database Managers

- Input/maintain application access controls
- Review database/audit/access logs
- Backup data files daily
- Support data restoration and recovery operations

LAN Administrators (Operations)

- Configure production environment (operating system, COTS software)
- Ensure the data files and transactions are encrypted
- Program access restrictions (directory, file, user accounts)
- Implement operating system and software upgrades and patches
- Provide system, environment, and data recovery support
- Monitor system and/or users. Methods: review system logs and reports, use automated tools, review change management, monitor external sources (trade literature, publications, electronic news, etc.), and periodic re-accreditation.
- During disposal phase assist with or perform media sanitization.

© 2011 The SANS Institute Author retains full rights.

Trainers/Instructors

- Develop manual, brochures, and documentation to include security concerns
- Train users, LAN administrators, etc. on security concerns of application.

IV&V/Test Team (preferably an independent contractor)

- Develop test plans and scripts
- Develop test data in concert with IT Security office efforts
- Test application from a security perspective (stability, availability, confidentiality, integrity, etc.)
- Test operating environment (operating system, COTS software, etc.) for vulnerabilities
- Coordinate and test interfaces
- Review application controls (transaction, input, output, access, database, etc.)
- Document results of testing (vulnerabilities, problems, successes).

IT Security Section Staff

- Conduct sensitivity assessment (information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, organization policy and guidance)
- Perform initial or preliminary Risk Assessment
- Review solicitation documents (e.g., Requests for Proposal)
- Develop security requirements: technical features (e.g., access controls), assurances (e.g., background checks for developers), operational practices (e.g., awareness and training), and test plans/script/scenarios
- Evaluate proposed systems
- Participate in security awareness and training
- Participate in development of test data
- Contract for IV&V and penetration testing if mission critical system
- Ensure it undergoes technical evaluation (federal laws [Sec. 508], regulations, policies, guidelines, and standards)
- Review production, test, and support environment security features, configurations, and controls
- Review off-site storage usage, services, and availability
- Review output distribution process
- Monitor threats - Threats and vulnerabilities include Trojan horses, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.
- For encrypted data ensure long-term storage of cryptographic keys
- Review System Security Plan - A formal security plan is required by the Computer Security Act of 1987 for all systems containing sensitive information.
- Review Contingency Plan
- Review Disaster Recovery plans

© 2011 The SANS Institute Author retains full rights.

- Periodically perform risk assessment
- Certify/approve application
- Maintain/keep security history and records.

Appendix C: Glossary and Acronyms

Access Control List (ACL) – SANS Security Essentials Glossary of Terms defines the ACL as *"a mechanism that implements access control for a system resource by listing the identities of the system entities that are permitted to access the resource."*

Contingency Plan (CP) - The SDLC Handbook, HB 5500-07[6] (page II-15-46) states that *"a Contingency Plan is an action plan for ensuring IT processing continuity despite catastrophic events. Contingency Plans cover three types of actions:*

- *Emergency procedures for initially responding to disruptions at primary locations,*
- *Backup procedures for conducting operations at alternate locations, when necessary, and*
- *Recovery procedures for restoring normal operations back at the primary locations."*

Cost Benefit Analysis (CBA) - The SDLC Handbook, HB 5500-07[6] (page II-15-46) defines the CBA as *"a study that projects the costs and benefits of an information system. Costs include all resources required for development as well as operating the system. Benefits are tangible and intangible."*

Disaster Recovery Plan (DRP) – NIST SP 800-34 'Contingency Planning Guide for Information Technology Systems'[7] (page D-1) defines the DRP *"as a written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities."*

Freedom of Information Act (FOIA) - http://www.nist.gov/admin/foia/foia.htm states that *"The Freedom of Information Act, enacted in 1966, provides that any person has a right, enforceable in court, of access to federal agency records, except to the extent that such records are protected from disclosure by one of nine exemptions or by one of three special law enforcement records exclusions."*

Independent Verification and Validation (IV&V) – IV&V is the independent testing and validation of the results by a third party.

National Institute of Standards and Technology (NIST) - SANS Security Essentials Glossary of Terms defines NIST as *"a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards."*

© 2011 The SANS Institute Author retains full rights.

Office of Management and Budget (OMB) - http://www.whitehouse.gov/omb/organization/role.html states that *"OMB's predominant mission is to assist the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies. In helping to formulate the President's spending plans, OMB evaluates the effectiveness of agency programs, policies, and procedures, assesses competing funding demands among agencies, and sets funding priorities. OMB ensures that agency reports, rules, testimony, and proposed legislation are consistent with the President's Budget and with Administration policies. In addition, OMB oversees and coordinates the Administration's procurement, financial management, information, and regulatory policies. In each of these areas, OMB's role is to help improve administrative management, to develop better performance measures and coordinating mechanisms, and to reduce any unnecessary burdens on the public."*

Risk Assessment (RA) - The SDLC Handbook, HB 5500-07[6] (page II-15-5) states that *"the risk assessment process includes defining and valuing the assets, defining the threats to those assets, determining the system's vulnerabilities, and recommending reasonable safeguards to bring the risks down to acceptable levels."*

Security Accreditation - The SDLC Handbook, HB 5500-07[6] (page II-15-54) states that *"the Security Accreditation Statement is senior management's formal acceptance of all residual security risks. In effect, it is senior management's 'buy-off' on the Security Certification Statement."*

Security Plan (SP) – The SDLC Handbook, HB 5500-07[6] (page II-15-5) states that *"the Security Plan documents all security-related activities. In the pre-operation phases of the SDLC, the Security Plan lists actions needed to ensure that the system is developed in a reasonably secure environment and that it contains the sufficient and appropriate security features. It defines the security requirements and provides the step-by-step management plan to meet those requirements. During the system's operation phase, the Security Plan becomes the document for responding to new vulnerabilities and threats as well as serving as the primary basis for management reports. It must be updated at least annually, but may be updated more often prior to the system's operation phase."*

System Development Life Cycle (SDLC) - NIST SP 800-34 'Contingency Planning Guide for Information Technology Systems'[7] (page D-2) defines the SDLC as *"the scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation."*

Trusted Facilities Manual (TFM) - The SDLC Handbook, HB 5500-07[6] (page I-A-49) states that the TFM *"cautions about functions/privileges that should be controlled when running a secure facility and procedures for examining and maintaining audit trails (including the audit trail record structure)."*

© 2011 The SANS Institute Author retains full rights.

Unit Testing - The SDLC Handbook, HB 5500-07[6] (page I-A-49) states that they *"are procedures used to verify the code or changes to the code within a particular module or subroutine."* They are *"the lowest level of testing that can be done on a code module or unit."*

Validation - The SDLC Handbook, HB 5500-07[6] (page I-A-49) defines validation as *"the process of evaluating software at the end of the software development process to ensure compliance with software requirements."*

Verification - The SDLC Handbook, HB 5500-07[6] (page I-A-50) defines verification as *"the process of determining whether or not the products of a given phase of the software development cycle fulfill the requirements. The act of reviewing, inspecting, testing, checking, auditing or documenting whether or not items, processes, or documents conform to specified requirements."*

Appendix D: References

Government provided information on IT Security and the SDLC:

[1] Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources".
URL: http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html.

[2] URL for NIST Special Publications:
http://csrc.nist.gov/publications/nistpubs/index.html.

- [7] SP 800-34, Contingency Planning for Information Technology Systems, June 2002
- SP 800-28, Guidelines on Active Content and Mobile Code, October 2001.
  SP 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), June 2001.
- SP 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001.
- SP 800-18, Guide for Developing Security Plans for Information Technology Systems, December 1998.
- SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
- SP 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, April 1988

[2] Federal Information Processing Standards Publication 73 (FIPS PUB 73) Guidelines for Security of Computer Applications, Washington, DC GPO, June 1980. URL: http://csrc.nist.gov/publications/fips/index.html.

[6] U.S Customs Service, System Development Life Cycle (SDLC) Handbook, HB 5500-07, October 1998. URL: http://www.customs.ustreas.gov/contract/modern/sdlcpdfs/.
[This handbook contains detail information about the System Development Life Cycle.]

© 2011 The SANS Institute Author retains full rights.

Carnegie Mellon Software Engineering Institute (SEI) Capability Maturity Model 2002.
URL: http://www.sei.cmu.edu/cmm/

Articles on government IT Security reporting concerns:

3 Frank, Diane, "Agencies Seek Security Metrics." Federal Computer Week, 19 June 2000. URL: http://www.fcw.com/fcw/articles/2000/0619/pol-metrics-06-19-00.asp

4 Sirhal, Maureen, "OMB orders agencies to report on computer security", 11 July 2002.
URL: http://www.govexec.com/dailyfed/0702/071102td2.htm

Burris, Peter, and Chris King. "A Few Good Security Metrics." METAGroup, Inc. 11 October 2000. URL: http://www.metagroup.com/metaview/mv0314/mv0314.html

***5*Web Sites with information on programming more securely:**
[These ten URLs/links were used to develop Appendix A: Programming Concerns]

5 "Best Practices for Secure Web Development"
URL: http://www.securitymap.net/sdm/docs/secure-programming/Secure-Web-Development.pdf

5 W3C, "The World Wide Web Security FAQ", 4 February 2002.
URL: http://www.w3.org/Security/faq/www-security-faq.html

5 Carnegie Mellon Software Engineering Institute CERT Coordination Center, "Understanding Malicious Content Mitigation for Web Developers", 2 February 2000.
URL: http://www.cert.org/tech_tips/malicious_code_mitigation.html

5 Netscape Communications Corporation, "JavaScript Security", 27 May 1999.
URL: http://developer.netscape.com/docs/manuals/js/client/jsguide/sec.htm

5 Sun Microsystems, "Java Web Server Security Problems", 15 February 2000.
URL http://www.sun.com/software/jwebserver/faq/jwsca-2000-02.html

5 Apache Software Foundation, "Apache Cross Site Scripting Info", 2 February 2000.
URL: http://www.apache.org/info/css-security

5 Microsoft Corporation, "HOWTO: Prevent Cross-Site Scripting Security Issues", 1 February 2000.
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q252985

5 Microsoft Corporation, "Q253119 HOWTO: Review ASP Code for CSSI Vulnerability", 2 February 2002.
URL: http://support.microsoft.com/support/kb/articles/Q253/1/19.ASP

© 2011 The SANS Institute Author retains full rights.

5 Microsoft Corporation, "Q253120 HOWTO: Review Visual InterDev Generated Code for CSSI Vulnerability", 2 February 2002.
URL: http://support.microsoft.com/support/kb/articles/Q253/1/20.ASP

5 Microsoft Corporation, "Q253121 HOWTO: Review MTS/ASP Code for CSSI Vulnerability", 2 February 2002.
URL: http://support.microsoft.com/support/kb/articles/Q253/1/21.ASP

Management Reference Books on IT Security and the SDLC:

Braithwaite, Timothy. Securing E-Business Systems – A Guide for Managers and Executives 2002

Stackpole, Bill. Information Security Management Handbook, 4th Edition, Tipton, Harold F., and Krause, Micki, Copyright 2000 by CRC Press LLC.

McBride, Patrick; Patilla, Jody; Robinson, Craig; Thermos, Peter; Moser, Edward P. Secure Internet Practices – Best Practices for Securing Systems in the Internet and e-Business Age. METASeS 2002

© 2011 SANS Institute, Author retains full rights.

© 2011 The SANS Institute Author retains full rights.