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.

A Certification and Accreditation Plan for Information Systems Security Programs (Evaluating the Eff

In order to ensure the confidentiality, integrity and availability of corporate information systems, each organization must implement a comprehensive Information Systems Security Program (ISSP).

Copyright SANS Institute

Author Retains Full Rights

AD

A Certification and Accreditation Plan for Information Systems Security Programs
(Evaluating the Effectiveness of an Information Systems Security Program)

Premise:
In order to ensure the confidentiality, integrity and availability of corporate information systems, each organization must implement a comprehensive Information Systems Security Program (ISSP). Determining the effectiveness of the ISSP requires evaluating each module individually, as well as its relationship to other components. Unilateral analysis, while often necessary due to time and resource constraints, results in a fragmented snapshot of the defenses of the enterprise. Often the non-security community does not fully comprehend the scope, breadth and impact of the ISSP which can result in either a false comfort level or undue concern over the degree to which their corporate resources are protected. To aid in the management of the plan, an annual calendar of major activities, including due dates, dependencies and responsibilities should be compiled, maintained and communicated to all parties with accountability for, or participation in a component of the plan.

As the expertise, ingenuity and persistence of attackers increases (re: NIPC July 2002 article: "*Swarming Attacks: Infrastructure Attacks for Destruction and Disruption"*), it becomes exponentially more important that the ISSP and its assessment utilize a defense in depth approach. This can be accomplished via redundancy or drilled down security. The program and its appraisal should include assurance that multiple layers of protection are present and adequate. Executives must understand the risks associated with operating in today's environment and certify their acknowledgement and acceptance of that environment. The results of the analysis of one component must be considered and mitigated when completing other ISSP components. The CIO should be briefed annually on the overall ISSP, understand the methodology used to develop it, and certify that s/he accepts the risk under which it operates. The CIO then briefs the President or CEO who accredits the ISSP.

Applications:

- *Systems Owners*:

Often, IT personnel become possessive of systems and forget that their purpose is to support business functions. Each application should have a designated System Owner who serves as the primary liaison with the IT community for all IT-related activities including security. The Security Awareness Training Program (SATP) should include a module that briefs Systems Owners on their responsibilities in each of the five system life cycle (SLC) phases. To ensure that System Owners are held accountable for these duties; security-related performance elements should be included in each System Owner's annual performance evaluation. The ISSP should include periodic check-ins with System Owners to verify that they are effectively functioning in their security role. The ISSP should be modified from lessons learned from the periodic check-ins.

- *Security Plans:*

Each application requires a security plan that provides a synopsis of the IT-security considerations. Key information about the system should be documented, stored offsite

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

for disaster recovery purposes, and updated annually to reflect system or operating environment modifications. Checklists for each component should be developed and applied throughout each stage of the SLC. The applications security plan will feed the application risk assessment process. The document should contain a description of the system, the system owner, business process definitions, interrelationships with other applications, rules of behavior with consequences for non-compliance outlined, capital plan for the SLC, and pertinent regulations, policies and guidelines used to design, develop, implement and operate the application.

Data requirements and sensitivity levels should be addressed and tied to access and background investigation requirements. The operating environment and infrastructure including telecommunications and the operating system should be described. Technical, managerial and operational controls should be defined with special attention to physical security, firewalls, IDS, DMZ, or other protection, monitoring and audit procedures. Risk assessment (certification and accreditation) status, backup and disaster recovery procedures/mechanisms for the application should be itemized. Finally, an application SATP for all personnel associated with the application (owner, developer, contractors, system administrators, operators, users, etc.) should be formulated, evaluated and implemented.

Above information was extracted from the USDA, OCIO-Cyber Security guidelines.

- *Risk Assessments:*

The application risk assessment process is closely tied to the SLC process and is a large, vitally important undertaking. The purpose of the application risk assessment is to identify vulnerabilities, threats, impact if the threats are exploited, help identify and implement countermeasures to reduce the identified risk, and have the system owner certify that they understand and accept the remaining residual risk. The equation commonly used to determine risk is: Vulnerabilities x Threat x Impact / Countermeasures = Risk. The ISSP should contain policies and procedures for accomplishing risk assessments throughout the SLC of an application. Best practices dictate performance every three years for implemented systems, or whenever major modifications are implemented. The ISSP should monitor and report on the following risk assessment components:

- Roles and Responsibilities (defined, documented and communicated)
- Needs Assessment (both business and security)
- Data Sensitivity Analysis
- Vulnerability Assessment
- Controls Analysis (managerial, operational and technical)
- Threat Assessment
- Impact Assessment
- Mitigation and Countermeasure Plan (including Cost Benefit Analysis)
- Residual Risk Analysis (report preparation)
- Certification by CIO
- Presentation to System Owner
- System Accreditation.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Above synopsized from Draft USDA, Risk Assessment Methodology, June 5, 2002.

- *Security Considerations in System Life Cycle:*

Historically, many organizations addressed security as the last feature in the SLC process. Luckily, regardless of the age of the system (new or legacy), security considerations can be addressed, evaluated and accommodated. Again, the increased sophistication of the intruder community and the more complicated technologies and operating environments have proportionally affected the attention organizations are devoting to these activities. Each of the five phases in the SLC; initiation, development/acquisition, implementation, operational/maintenance, or disposal/retirement has activities associated with them. Key activities for the various stages include assessing data sensitivity and handling, risk assessments, and operational technical and managerial controls analysis. Each component needs to be defined, assessed and audited via standardized checklists for the appropriate phase and reevaluated when operational systems are modified.

- *Password/USERID Management*:

Basic USERID policies should include the following:

- Be approved by appropriate level of management.
- Key information included on request (background investigation/security clearance status, and tied to position; verified currency.
- Ideally tied systematically to HR and contractor database to verify pertinent information.
- Non-employee database maintained of pertinent information including responsible manager, duration of access, etc.
- Signed statement (preferably digitally) acknowledging completed SATP and understand responsibilities, policies and rules of behavior.
- Exit procedures include ISS signoff and termination of access.
- Periodic report to the responsible manager for review and certification of all access.
- All USERID are assigned to individuals
- Application processes USERIDs assigned to accountable individual
- USERID are not meaningful and access is not determined by the content of the USERID.
- Rules of behavior and consequences for violation are clearly defined.
- Termination after lack of use – criteria defined, exceptions analyzed and documented.
- Failed attempts stopped at three, logged, reviewed and tracked.
- The requirement that documentation (preferably electronically) is required and maintained for the life of the USERID/access.

Basic password policies should include the following:

- Initial password modification requirement
- Password aging and how many time back to check reused password content
- Only encrypted version stored/displayed (strength commensurate with sensitivity of data being accessed.
- Shared secret when processing USERID or password reset

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Length/content considerations
- Run cracking processes to identify and correct weaknesses
- Use of shadow password file to protect encrypted password files
- Ultra secure – smart cards; challenge/response, SKey (password list – different each time)

Exceptions to any policies/procedures need to be documented and approved by appropriate individuals commensurate with risk assigned to exception.

Above summarized from SANS: Password Assessment and Management v1.9 2/02

- *Access Verification Reports*:

USERID creation procedures while important are only half of the USERID management program. Periodic (ideally monthly) reports itemizing all access associated with users should be sent (preferably electronically) to managers and contracting officers to verify the accuracy and appropriateness of the access. Non-employee access should be reported to either the manager directly responsible for the activities of the non-employee, the contracting officer, or in special circumstances, the CIO or CEO. A process should be established to allow managers to easily communicate necessary modifications. Access is then monitored from a business perspective to ensure changes in user job responsibilities (transfers, separations, reorganization, or contract termination), application modifications or other circumstances result in commensurate changes in user access. The ISSP should include assurance that managers are trained on these responsibilities in the SATP and that the process is reviewed for effectiveness.

Auditing:

An effective security professional welcomes the auditing of their ISSP as a useful hardening mechanism. Better to discover and mitigate weaknesses in the armor prior to exploitation. Optimal configurations utilize an internal team that is responsible for evaluating the various ISSP components on a rotational basis so vulnerabilities can be identified and rectified prior to exploitation by intruders or exposure by external auditors. An auditing plan should be included in the overall ISSP, periodically targeting each module. The plan should integrate internal and external audits to optimize the evaluation of corrective actions, and aggressive scanning and penetration attempts. This will ensure the continual evaluation of a program's effectiveness. It is imperative that knowledge of the timing, focus and procedures for internal audits be limited to the immediate auditing team and their managers to closely mimic the intruder experience as much as possible. Because people are the determining factor in the success of any undertaking, social engineering should be a targeted auditing function and the SATP updated to mitigate the results of the audit.

Two keys to a worthwhile audit program are the atmosphere in which they are conducted, and the competence of the auditing personnel. The attention given to investigating the systemic, procedural, or other problem causes and/or weaknesses identified, tracked through resolution, and prioritization and timing of corrective actions all contribute to this atmosphere. Verification mechanisms should ensure that auditors

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

have the appropriate skills to match the complexity of the component being audited (i.e., individuals without systems administration or network administration experience or training cannot perform an effective audit of that function. Subsequent audits should verify that previous findings have truly been fixed and outstanding audit findings and recommendations should be considered when performing standard security assessment functions such as security plans and risk management.

Background Investigations/Security Clearances:
Prudent security programs include screening all personnel for suitability of employment. This is especially true for individuals who will be interfacing with an organization's IT resources. The level of the background investigation should be tied to the position. Position changes dictate investigation requirements. Consideration should be given to investigations for temporary, intermittent, or seasonal employees. The results of investigations should be assessed in relation to its relevance to the position's duties and an employee's performance of those duties. An example would be an accountant whose investigation comes back with notice that they are currently being investigated for embezzlement of church funds where she functioned as a treasurer. This would impact her suitability even though she was performing her accountant functions adequately with no concerns presented.

A timeframe should be established for reevaluation. A rule of thumb is lowest level investigation every 3-5 years for all employees, with a higher investigation level every 10-15 years. The seriousness, fre-quency (whether multiple infractions within the same category or in combination with other infractions), age of infraction, as well as the age of the individual when the infraction occurred, are all considerations when determining suitability or continuation of employment/access. The Office of Personnel Manage-ment (OPM), the Human Resource arm of the federal government provides the following guidelines:

Rank	**Seriousness**	**Potential Disqualification** (if conduct or issue stands alone)
A	Minor	Not Disqualified
B	Moderate	Probably Not Disqualified
C	Substantial	Might be Disqualified
D	Major	Would be Disqualified
Frequency Upgrade		
2 Issues in 0-36 months		Raise both issues once (e.g. "A" to "B")
3 or more issues in 0-36 months		Raise all issues twice (e.g. "A" to "C")

Timeliness Downgrade			
Issues	0-36 Months	32-72 Months	73-108 Months
B	B	A	Non-Issue
C	C	B	A
D	D	C	B
Note: Anything >108 months is non-issue.			

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Other considerations are: kind of position, nature of seriousness, circumstances, recency, societal conditions, absence or presence of rehabilitation.

Special thanks to Pat Hess, USDA/Human Resources, for her assistance with summarizing OPMs Suitability Training, Federal Investigation Process.

Cyber Incident Response Plan:
An effective cyber incident response policy identifies internal and legal authority reporting requirements and clearly defines roles and responsibilities for all individuals involved in the process. Executive managers need to be briefed on the process before they get presented with an incident and are blindsided by the methodology, techniques, impact, requirements, etc. Any unauthorized activity that has infiltrated the security defenses and affect the confidentiality, integrity, or availability of corporate IT resources can be considered an incident and should be researched, tracked, and rectified. The policy should begin with a definition of what constitutes an incident (e.g., will suspicious activity be included), what the various categories are (scanning results, audit findings, log reviews, etc.), and include threat and consequences of exploitation.

The sensitive nature of the incident response function and confidentiality requirements must be stressed. Timeframes and conditions for reporting should be outlined. Incident response procedures include identification of detection mechanisms, acknowledgement of the occurrence, and internal notification procedures (when to notify/involve management chain, Human Resources, and legal authorities of suspicion/confirmation of incident). Documentation requirements should be defined for recording the assessment of how infiltration or infraction occurred, historical requirements for research, the factors for determining the impact of exploitation, quarantine and recovery activities, and how lessons learned should be incorporated into hardening environment to avoid recurrence. Proactive monitoring procedures will help to reduce the amount and severity of incidents and invocation of incident response procedures.

Tiger teams ready to investigate, quarantine if necessary, resolve and document incidents should be compiled, trained and funded. Tools of the trade include well stocked "jump bags" containing: boot disks, CDs or diskettes with application software, IDS software, ghosted images of standard software loads, a variety of cables, phone and email contact lists, ISSP freebie diskettes and spare blank CDs and diskettes.

Desktop Security:
Desktop policies, baseline standards, and procedures should be clear, communicated, enforceable, and audited periodically for effectiveness. In his paper titled "*Managing Desktop Security*", Amran Bin Munir, dated 9/23/01, defines baselines as:

> *"Baselines are the minimum security standard applied to any system configuration. Baselines can be categorized into two groups. General baselines specify general standard which cover overall systems in a company while technical baselines is more specific toward a particular system platform or application."*

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Checklists of specific configuration settings should be prepared for each operating system (OS) and completed as part of the annual risk assessment process. Access requirements for desktop applications and resources should be defined, tied to background investigations/security clearances, and reported to appropriate managers for verification and certification.

Desktop configurations should be managed and optimized for each OS to take full advantage of security defenses. A configuration image library, including up-to-date and applied anti-virus and OS patches/fixes, should be maintained, backed up and stored offsite for disaster recovery purposes.

A key element to desktop security is an effective SATP. Its focus should be for all users to increase awareness of the environment and their role and responsibility in ensuring the confidentiality, integrity, and availability of corporate resources. Another important SATP component for users, developers and administrators of desktop applications are application-specific security/risk considerations. All need to understand the risk concept that Risk=(Vulnerabilities x Threat x Impact / Countermeasures), and the interrelationship of this application with other applications on the system/network. Finally, all personnel associated with desktop applications need to be educated on the identification, initial containment and reporting procedure for security defense violations, intrusions or other incidents.

Disaster Recovery/Contingency Planning:
The events of September 11, 2001, emphasized the need for organizations to plan, develop, train, test, incorporate lessons learned, implement, and most importantly maintain disaster recovery and contingency planning. The National Institute of Standards and Technology published NIST SP 800-34, Contingency Planning Guide for Information Technology Systems, dated June 2002, http://csrc.nist.gov/publications/nistpubs/800-34/800-34.pdf. This document itemizes the various plans, their purpose and scope, assigns responsibility for each component, and explores the interrelationship among the plans. If this component is neglected, the time, money, effort, and resources put into the other ISSP components is for naught. In extreme cases, the organization itself could cease to exist. NIST defines the plans as:

- *Business Contingency Plan (BCP):* Provides procedures for sustaining essential business operations while recovering from a significant disruption. Addresses business processes; IT addressed based only on its support for business process. A DRP, BRP and OEP may be appended to the BCP. BCP responsibilities and priorities should be coordinated with those in the COOP to eliminate conflicts.
- *Business Recovery (or Resumption) Plan (BRP):* Provides procedures for recovering business operations immediately following a disaster. Addresses business processes; not IT-focused; IT addressed based only on its support for business process. Development of the BRP should be coordinated with the DRP and the BCP. The BRP may be appended to the BCP.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- *Continuity of Operations Plan (COOP):* Provides procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site for up to 30 days. Addresses subset of an organization's missions deemed most critical; usually written at headquarters level; not IT-focused. The COOP may include the BCP, BRP, and DRP as appendices.
- *Continuity of Support Plan/IT Contingency Plan:* Provides procedures and capabilities for recovering major application or general support system. Same as IT CP; addresses IT system disruptions; not business process focused. Because an IT CP should be developed for each major application and GSS, multiple CPs may be maintained within the organization's BCP.
- *Crisis Communications Plan:* Provides procedures for disseminating status reports to personnel and the public. Not IT-focused. Plan procedures should be included as an appendix to the BCP.
- *Cyber Incident Response Plan:* Provides strategies to detect, respond to, and limit consequences of malicious cyber incident. Focuses on information security responses to incidents affecting systems and/or networks. This plan may be included among the appendices of the BCP.
- *Disaster Recovery Plan (DRP):* Provides detailed procedures to facilitate recovery of capabilities at an alternate site. Often IT-focused; limited to major disruptions with long-term effects. The DRP scope may overlap the IT CP; the DRP is narrower in scope and doesn't address minor disruptions that don't require relocation. Dependent on organization's needs; several DRPs may be appended to the BCP.
- *Occupant Emergency Plan (OEP):* Provides coordinated procedures for minimizing loss of life or injury and protecting property damage in response to a physical threat. Focuses on personnel and property particular to specific facility; not business process or IT system functionality based. The facility OEP may be appended to the BCP, but is executed separately.

NIST stresses the need for DR/CP activities to be enterprise-wide. Because both minor outages and major natural or man-made disasters can affect the confidentiality, availability and/or integrity of corporate information both should be accommodated in the plans. A prudent ISSP ensures that each of the plans: exist, has its own checklist to ensure key pieces are accounted for and adequately addressed, documented, tested, trained, and procedures that include incorporating lessons learned from audits or actual execution and implemented. As with all ISSP components, the DR/CP is useless if a well thought out plan sits on the shelf.

E-Mail:

Due to the convenience, volume and acceptability of e-mail exchange in today's society, e-mail is one of the most fertile grounds for penetrating corporate defenses to either spread havoc or harvest data. Therefore, multiple methods of identifying and isolating intrusion should be employed. Strong e-mail security includes attachment checking, scanning and possibly filtering (especially targeting HTML, scripts and .exe files) to prevent dangerous or malicious code from penetrating corporate defenses. Strong password format, content, and aging policies need to be enforced. Anti-virus software

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

patches should be current and a tracking system established to ensure distribution throughout the enterprise. Encryption mechanism should be commensurate with sensitivity of data. Publication of e-mail distribution lists should be limited to those with a need to know.

Consideration should be given to location of the mail server in relation to the DMZ, firewall and other perimeter defenses. Because e-mail is often a mission-critical application, due diligence should be afforded the disaster recovery procedures. Remote administration and user access should be addressed to ensure compliance with security procedures.

The e-mail SATP program should advise employees of the inherent insecure nature of many e-mail systems. It should also make clear to employees that they forfeit their right to privacy when utilizing corporate e-mail accounts and that all traffic (incoming and outgoing) become corporate property. Typical policies include a limited personal use clause. E-mail is also ripe territory for social engineers to work their magic, so employees need to be aware of methods, practices, and implications of succumbing. Finally, users should be kept apprised of the latest viruses, hoaxes, scams, worms, spamming, and other malicious code and ways to avoid them or report to proper authorities when infected.

Network/System Administration:
Cisco Best Practices – Security Management defines the purpose of network security as *"control access to network resources according to local guidelines so that the network cannot be sabotaged (intentionally or unintentionally)."* Network and systems administrators play an integral role in the success of this component of the ISSP. Security clearance requirements for these and other privileged users should be stringent and reviewed more often then regular users. It is important that they integrate the network security program into the other International Organization for Standardization (ISO) defined network management model functional areas: fault, configuration, performance, and accounting management. Risk assessments should be performed prior to implementing new or modified software or hardware on the network.

Network sign-on requirements should be documented and communicated to the user community. These requirements should include signed acknowledgement of SATP completion and a review of the network access policy. The sign-on screen should include a message advising of corporate security policy, advise users that they are subject to monitoring and tracking, and consequences for violations of corporate security policies.

User identity must be authenticated and procedures developed to handle validation failures. Unsuccessful attempts to log onto the system should be logged, reviewed, investigated and resolved. The level of sign-on and access tracking to be logged, reviewed and monitored should be defined and followed. Once the user's identity is substantiated, access privileges and restrictions should be checked and failed attempts

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

logged as well. As with other applications, network USERIDs and access should be reported and validated by appropriate managers on a periodic basis.

A strong IP management plan will identify the organizational and physical location of equipment (gateways, routers, switches, servers, printers, as well as PCs and other peripherals), uniquely distinguish specific machines and assist in the identification of individuals. Special attention should be given to remote devices like laptops, home users, PDAs and other wireless devices. This will assist in incident research and resolution activities.

A strong network policy should include an outline of the rules of behavior and consequences for violation, a limited personal use clause, and backup and recovery requirements. Anti-virus use and currency should be governed by both policies and procedures, and included in the periodic audit calendar.

Finally, when incidents or violations occur, procedures for identification, isolation, historical research and recording, impact analysis, irradication, restoration and lessons learned utilization should be defined and implemented.

Organization:
The strongest ISSP is substantially weakened without a sufficient quantity of trained (certified), empowered staff, executive management support and a budget commensurate with the security task. To address accountability and ensure compliance, executive managers, supervisors and users should have security-related performance elements in their annual reviews which reflect upon their individual work evaluation.

Where the Information Systems Security Staff (ISSS) is located within the organizational hierarchy has a direct correlation to the success of the ISSP. The staff must be organizationally situated within the corporate hierarchy with sufficient authority to implement the ISSP across the enterprise. Many ISSSs report to the Chief Information Officer (CIO) due to the technical nature of the work and its intimate relation to the information technology function. However, ISSP tasks span the enterprise:

- Human Resources is responsible for the hiring of personnel; position classification; processing of security clearances; notification of garnishment of wages, bankruptcies or other worrisome investigations; and termination or other separations.
- Labor Relations can assist with the interpretation of labor-management agreements and provide advice on negotiable items.
- Compliance Office provides expertise in corporate compliance with Federal, state, industry, corporate laws, standards and policies.
- Facilities/Space Management administers physical access controls and monitoring technologies.
- Contracting Staff handles outsourcing and procurement of all IT-related resources (hardware, software, telecommunications, and support services).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Each IT organization exists to support a production entity. This organization not only has a vested interest in the success of the Security Program, it plays an intimate role in carrying out the ISSP.
- Often, telecommunications professionals, and network and system administrators are not organizationally situated with the appropriate relationship to the ISSS. These critical functions play a pivotal role in the success of the ISSP. Special consideration should be given to analyzing the structure, communication mechanism, and interplay between the entities to ensure consistent and effective implementation of the ISS policies and procedures.

Especially in large or highly structured organizations, placement of the ISSS at a level below or equal to other entities with security-related responsibilities will diminish their authority, ability to perform critical tasks, and weaken the ISSP, possibly to the point of failure.

Perimeter:
Each organization maintains what is commonly referred to as a DMZ between corporate resources (networks, Intranets, and applications), and the Internet. The DMZ serves as the first in multiple levels of the defense-in-depth protection of IT resources. Components and evaluation considerations for an organization's perimeter are itemized below and should be tied closing to the incident response policy/procedures:

- Analysis and determination of data sensitivity and relation to encryption level requirements
- Threat vectors (who, where, how intruders can attack-both internally and externally), and mitigation strategies deployed
- Internally assessable and public-access boxes situated properly and limited, secured paths between
- Failover, load balancing and backup and recovery procedures are outlined, tested and maintained
- Qualification and currency of training for telecommunications, network administrators, WebFarm and ISSS personnel
- Physical considerations, access (including log retention and auditing requirements), location, signage are addressed
- Firewalls, gateways, routers and switches properly configured, logs analyzed, and follow up activities performed on an appropriate recurring basis
- Analysis of both in and outbound traffic
- Protocol allowances checked and hardened
- Dial-up connection restrictions and auditing
- Quarantine and recovery procedures and strategy reviewed, tested and lessons learned utilized
- IDS policy and procedures (including log retention, auditing requirements, follow up activities and hardening activities),
- Procedures are in place to ensure risk assessments are performed before modifications are implemented
- Infrastructure diagrams and documentation maintained and accessible by those with need-to-know, but adequately protected from outside access

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Virus, spoofs and worm identification, inoculation and irradication strategy
- Independent auditing strategy including rigorous attack plan and social engineering strategies tested.

Physical Security:
The ISSP should include a Physical Security Plan even though many ISSSs don't maintain direct responsibility for the physical security function. Items to be addressed include:

- Access to building and room restrictions (including parking lots and proximity parking if applicable); special consideration for key IT resources: computer rooms, web farms, servers and the telecommunications cabinets. Periodic checks on cleaning, maintenance and other personnel with unfettered access to office (again, special attention to key IT resources) areas should be included in the plan.
- Employee identification: badges, guard notification of separated/removed employees or contractors.
- Policies and procedures itemized for non-employees access to building and key IT resources; visitor logs maintained.
- Maintenance of master keys, key-cards and cipher lock numbers.
- Emergency preparedness materials identified, maintained and accessible.
- Response and removal procedures for violent, disruptive or otherwise threatening personnel.
- Property (PCs, laptops, hard drives, diskettes, CDs, etc.) tracking. In: verification material is safe and appropriate. Out: authorized via property pass and logged.
- Backups and offsite storage appropriate and according to established policy/procedures.
- Occupant Emergency Plans in place, tested and maintained.

Additional physical security guidance and how to conduct a Crime Prevention Assessment can be obtained from:
http://www.gsa.gov/Portal/content/pubs_content.jsp?contentOID=115872&contentType=1008&cid=null.

Policies/Procedures:
The ISSP should include the definition and effective communication of the full range of program-level and issue-specific security policies and procedures. Each ISSP component should have an associated security policy and procedure.

Policies must be clear, concise, non-conflicting, acknowledged (for accountability), measurable (to ensure enforceability), and non-compliance consequences explicitly outlined. Corporate policies need to be consolidated in a logical collection and communicated to new employees or non-employees accessing corporate resources via the SATP. They should be reviewed to ensure validity and updated when audits,

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

procedures, or other circumstances dictate. The entire ISSP suffers when policies are ineffective.

Procedures standardize the ISSP, ensuring equitable application of the policies. When implementing procedures without associated policies, problems ensue with accountability, developing or utilizing automated evaluation tools, and aggregating results of the analysis, and understanding, interpretation and enforcement of the policies.

Security Awareness Training Program (SATP):
The ISSP should contain a robust SATP customized to addresses the unique security responsibilities for a diverse group of individuals. Key groups include: basic end users (typically COTS training can address this group), developers, managers (with special attention for the ISSP Manager, CIO and CEO), system owners, network and system administrators and non-employees. The SATP should contain components covering: security policies and procedures; an overview of the telecommunications infrastructure so the individual understands their place in the overall corporate structure and that a risk assumed by one is assumed by all; application-specific security requirements; infowar concept; email considerations; social engineering concerns; an overview of viruses, scams, hoaxes, spamming and spoofing; and physical security matters.

The SATP needs to be included as an integral part of employee and non-employee orientation. It must be tracked, acknowledged in writing, and a prerequisite for USERID or application access. Finally, each component of the SATP should be included in the audit schedule and lessons learned recycled.

Web Applications:
The placement of application servers in relation to DMZ, firewalls, gateways, etc., plays an integral role in the effectiveness of web application security. Once implemented, another important factor is strong configuration management policies and procedures to ensure continued defense integrity as modifications or enhancements are moved to the production environment. Software patches and fixes should be checked to ensure currency. Checklists should include analysis of permissions and services to ensure minimally enabled.

Applications should be reviewed to ensure that sensitive corporate information (including USERIDs; passwords, application, links and server names) has been adequately sanitized from public (or inappropriate internal viewing) either openly or hidden in source code. Data input to forms should be validated for correctness (type, length and expectation) and transmission paths tested for vulnerabilities. Encryption of data should be commensurate with the sensitivity of the data. The use, transmission and storage or cookie information should be included in the policies, procedures, and audit activity.

As with all access, user authentication is integral to the success of web security. Strong USERID and password requirements should be instituted to thwart harvesting attempts.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Consideration should be given to utilizing URLs, hidden form elements and cookies to establish state and track/log user activity. Backup and recovery procedures should be included in documentation, tested and lessons learned incorporated. Auditing should be outlined in policies and procedures and performed on a frequent basis, including scanning, IDS, penetration attempts, information harvesting attempts, and other vulnerability assessment tools.

Portions of the above synopsized from: "Web Application and Databases Security", Darrell E. Landrum, 4/2/01, http://rr.sans.org/security.basics/web_app.php.

Wireless:
One of the newer components of many ISSPs is the Wireless Security Plan. Included in the wireless family are pagers, cell phones, PDAs, laptops and palmtops. These devices bring a whole new level of access, flexibility and portability to the IT-environment and present increased challenges for the ISS professional and the ISSP. The quantity of devices/users and the temporary nature of the connection set hurdles for the logging, tracking and auditing function. GSA, Federal Technology Service, compiled a presentation titled "Hello? Who's Listening In?" available at http://fts.gsa.gov/webcast/3-7_wireless_security/sld001.htm, which outlines Wireless Security Basics. The article provides a framework for security issues/countermeasures which should be addressed in the Wireless Security Plan, including:

- Protective measures for Access Points (AP), including:
  - Antenna signals (vertical as well as horizontal distance considerations),
  - Ensure layer filtering of Media Access Control (MAC) Access Control Lists (ACLs) not only level of protection,
  - Corporate policy addresses AP placement, environmental considerations as well as its relation to firewalls and DMZs
  - Single AP doesn't access multiple segments of network unless via VPN.
- Disable (if possible) broadcasting and sanitize the Service Set Identifier (SSID), the shared secret manually entered in the AP and the client.
- Use IDS and "arpwatch" to monitor unauthorized MACs.
- Use VPN-type (SSH or SSL) instead of Wired Equivalent Privacy (WEP) link-layer encryption.
- Centralized authentication and dynamic key distribution via EAP/802.1X, Extensible Authentication Protocol.
- Perimeter of building is shielded to reduce risk of outside RF interference, assist in protecting AP, and reduce the possibility of Denial of Service (DoS) attacks via drive-by or other means.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

1) "Cisco – Network Management System: Best Practices White Paper", http://www.cisco.com/warp/public/126/NMS_bestpractice.html.

2) "Cisco – Network Security Policy: Best Practices White Paper", http://www.cisco.com/warp/public/126/secpol.html.

3) "Computer and Information Security Policy", http://secinf.net/info/policy/hk_polic.html.

4) "Draft USDA, Risk Assessment Methodology dated 6/5/02".

5) "Email in the New Era (Version 1), Guang Chen, July 21, 2001, http://rr.sans.org/email/new_era.php.

6) "Hello? Who's Listening In?", http://fts.gsa.gov/webcast/3-7_wireless_security/sld001.htm.

7) "IT Security Cookbook – 8 Physical Security", Last Update 08 Jun 2000, http://boran.linuxsecurity.com/security/IT1x-8.htm.

8) "Managing Desktop Security", Amran Bin Munir, September 23, 2001, http://rr.sans.org/securitybasics/desktop.php.

9) "NIH Application/System Security Plan Template for Major Applications and General Support Systems", May 4, 1999, http://irm.cit.nih.gov/security/secplantemp.html.

10) "NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems", dated June 2002, http://csrc.nist.gov/publications/nistpubs/800-34/800-34.pdf.

11) Pat Hess, USDA/Human Resources, summarization of OPMs Suitability Training, Federal Investigation Process, 2001.

12) SANS: Password Assessment and Management v1.9 2/02.

13) SANS: Web Security, v1.4, 11/01.

14) "Secure This: Organizational Buy-in (A communications approach), Sean Heare, December 1, 2001, http://rr.sans.org/aware/data_center.php.

15) "Securing E-mail", Sharipah Setapa, 09/13/01, http://rr.sans.org/email/sec_email.php.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

16) "Security in the Workplace – Informational Material: Conduct a Crime Prevention Assessment" http://www.gsa.gov/Portal/contents/pubs_content.jsp?contentOID=115872&contentType=1008.

17) "Swarming Attacks: Infrastructure Attacks for Destruction and Disruption", National Infrastructure Protection Center article dated July 2002.

18) USDA, OCIO-Cyber Security, Security Plans guidelines, 2001.

19) "Web Application and Databases Security", Darrell E. Landrum, 4/2/01, http://rr.sans.org/security.basics/web_app.php.

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**