Security Operations

Table of Contents

Getting Started

Operations security involves planning and sustaining the day-to-day “rubber meets the road” processes that are critical to maintaining the security of institutions’ information environments. The extent and complexity of security operations will vary between institutions based on institutional risk tolerances and resource levels. However, each of the control areas in this chapter must be addressed in some manner to help mitigate common ubiquitous risks. **The most important aspect of operations security is that the operations themselves need to be repeatable, reliable, and consistently performed.**

If you are just starting an information security program or looking to evaluate and improve operations security then the following approach can be very helpful:

1. **Review** the following areas to assess the confidentiality, integrity, and availability of operations center controls:
    a. Operational procedures and responsibilities
        i. Review documentation and evaluate guidance in regards to change management, capacity management, and separation of development, test, and production environments
    b. Malware detection and prevention controls
        i. Evaluate their level of effectiveness
    c. Data center backup strategy
        i. Evaluate whether backup procedures and methods (e.g., encryption) are effective both for on- and off-premises backup management
    d. Audit trails and logging
        i. Review whether they are implemented effectively so that security reviews can be conducted to detect tampering, unauthorized access, and record user activities
    e. Installation of software on operational systems
        i. Ensure licensing requirements are met
2. **Implement** a formal vulnerability management program to proactively test IT infrastructure for vulnerabilities that can be exploited and ensure that there is an effective process in place to manage corrective actions in collaboration with stakeholders.
3. **Prepare** in advance for IT controls audits to avoid service disruptions.

Top of page

Overview

To be effective in reducing information security risk and ensuring correct computing, the security program needs to include operational procedures, controls, and well-defined responsibilities. These are complemented and often necessitated by formal policies, procedures, and controls which are necessary to protect exchange of data and information through any type of communication media or technology.

We will briefly examine 7 key effective security control areas in this chapter:

- Operational Procedures and Responsibilities (important operational processes include: Change Management; Capacity Management; Separation of Development, Test, and Operations Environments)
- Protection from Malware
- Backups
- Logging and Monitoring
- Control of Operational Software
- Technical Vulnerability Management
- Information System Audit Considerations

Top of page

Operational Procedures and Responsibilities

Objective: To ensure the effective operation and security of information processing facilities.

Documented Operating Procedures

Key Question: Do we have a procedures that are readily available, periodically updated, and consistently executed?

Operating procedures must be documented and readily available to the teams for which they have relevance. These procedures should cover methods that reduce the likelihood of introducing or enhancing risks due to accidental or ill-advised changes. Before authoring documentation, it is often very important to identify up-front who the intended audience is. For instance, documentation that is intended to to have value for new hires (continuity) often requires a greater degree of detail than steps for staff who regularly perform operations tasks.

It is very important that operating procedures be treated as formal documents that are maintained and managed with version and approval processes and controls in place. As technology and our systems infrastructure changes, it is an absolute certainty that operational procedures will become out of date or inaccurate. By adopting formal documentation and review processes, we can help reduce the likelihood of outdated procedures that bring forth their own risks -- loss of availability, failure of data integrity, and breaches of confidentiality.

What should we document?

As mentioned before, the decision on what areas deserve documentation must be informed by an understanding of organizational risks including issues that have previously been observed. However a good list of items to consider include the following items:

- Configuration and build procedures for servers, networking equipment, and desktops.
- Automated and Manual Information Processing
- Backup procedures
- System scheduling dependencies
- Error handling
- Change Management Processes
- Capacity Management & Planning Processes
- Support and escalation procedures
- System Restart and Recovery
- Special Output
- Logging & Monitoring Procedures

Common Challenges

"Not enough time." Very often operations teams already have considerable responsibility and may indicate that there is simply not enough time for documenting processes. The allocation of time for documentation efforts is a management issue and for this reason it is important that IT leadership have an understanding of risks associated with outdated or informal operational procedures. In addition, defining a mandatory requirement that documentation efforts be completed before closing a project or significant change can help.

Notes/ Ideas

- Wiki Software + Process Documentation - Wiki software can sometimes help establish a system of documenting and centrally maintaining operating procedures. This software often usually supports change tracking and can also easily help identify procedure documents that may not have been updated in some time.
- IT Operations Manuals - Many IT organizations have found benefit in collating operational procedures into IT Operations Manuals that is available to relevant staff. This approach also has significant benefits and tie-in when considering Disaster Recovery.

Useful Resources

- University of Texas Network Operations Manual (PDF)
- University of Houston Information Security Resources and Operations Manual
- EDUCAUSE: Shared Data Centers: Something Old and Something New
- EDUCAUSE: The EITS Analysis Committee: A Grassroots Effort at Standardized Documentation and Diagramming Templates
- EDUCAUSE: Business Continuity Management Discussion

Change Management Procedures

Key Question: Do we have a formal method for classifying, evaluating, and approving changes?

Change management processes are essential for ensuring that risks associated with significant revisions to software, systems, and key processes are identified, assessed, and weighed in the context an approval process. It is critical that information security considerations be included as part of a change review and approval process alongside other objectives such as support and service level management.

What change should we evaluate and how to get started?

Change management is a broad subject matter (see resource below for additional reading) , however some important considerations from an information security perspective include:

- Helping to ensure that changes are identified and recorded.
- Assessing and reporting on information security risks relevant to proposed changes.
- Helping classify changes according to the overall significance of the change in terms of risk.
- Helping establish or evaluate planning, testing, and "back out" steps for significant changes.
- Helping ensure that change communications is handled in structured manner (see RACI matrix below).
- Ensure that emergency change processes are well defined, communicated, and that security evaluation of these changes is also performed post-change.

Common Challenges

“Change Management Takes Too Much Time.” Change management processes are notoriously susceptible to becoming overly complex. Staff who conduct changes are more likely to attempt to bypass change management processes they feel are too burdensome by intentionally classifying their changes at low levels or even not reporting them. If you are starting a Change Management program it is often helpful to first focus on modeling large scale changes and then working to find the right change level definitions which helps balance risk reduction with operational agility and efficiency.

Notes/Ideas

- Business Impact Analysis - Undertaking a Business Impact Analysis can often help strengthen change management operations by developing an understanding of both system and process level dependencies. This can help to evaluate and plan for less ostensible issues that emerge due to changes that impact system interactions (e.g. cascade failures).

Useful Resources

- Clemson CCIT Change Management Page
- Indiana University UITS Change Management
- Stanford Change Management System
- Oregon State Change Management Policy
- EDUCAUSE Presentation: Inform, Engage, and Educate: How to Communicate Major Service and System Updates and Changes to the Campus
- The Visible Ops Handbook

Capacity Management Procedures

Key Question: Do we monitor resource utilization and establish projections of capacity requirements to ensure that we maintain service performance levels?

Formal capacity management processes involves conducting system tuning, monitoring the use of present resources and, with the support of user planning input, projecting future requirements. Controls in place to detect and respond to capacity problems can help lead to a timely reaction. This is often especially important for communications networks and shared resource environments (virtual infrastructure) where sudden changes in utilization can in poor performance and dissatisfied users.

To address this, regular monitoring processes should be employed to collect, measure, analyse, and predict capacity metrics including disk capacity, transmission throughput, service/application utilization.

Also, periodic testing of capacity management plans and assumptions (whether tabletop exercises or direct simulations) can help proactively identify issues that may need to be address to preserve a high level of availability of services for critical services.

Notes/Ideas

- Emergency Operations - Many campuses who have experienced a crisis have seen dramatic surges of requests for information from institutional websites. If there are units at your institution who plan and manage emergency operations then partnering to evaluate the capacity management implications of varied emergency response scenarios can often be helpful.
- Cloud Service Models + Resource Elasticity - Enterprise Cloud service models including PAAS, IAAS, and SAAS often offer attractive resource elasticity features (in some cases to automatically scale rapidly in response to demand). When considering these benefits and risk reduction capabilities, it is also important to understand and review other security considerations relevant to Cloud Computer (see Cloud Computing Security Hot Topic).

Useful Resources

- Apache JMeter _load testing tool for web services and a variety of other protocols)
- IBM partnership with North Carolina Central University (NCCU) and NC State University to create the "greenest" cloud computing Data Center (Capacity Management emphasis)

Top of page

Protection from Malware

Objective: To protect the confidentiality, integrity, and availability (CIA) of information technology resources and data.

Key Question: Do we have effective security controls to prevent, detect, and recover from malware threats?

While malware prevention efforts can only be as effective as the level of protection offered by current anti-malware solutions in place---proactive measures to assess the effectiveness of anti-malware controls in place are both appropriate and necessary, as well as user awareness training. The ability to maintain centrally-managed and current protection updates is important, as is ensuring that users understand the importance of properly installed and utilized anti-malware solutions that they are provided. Malicious mobile code that is obtained from remote servers, transferred across networks and downloaded to computers (ActiveX controls, JavaScript, Flash animations) is a continuing area of concern as well. If identified as pertinent, technical provisions can be made to comply with guidelines and procedures that distinguish between authorized and unauthorized mobile code.

- Managing Malware
- Tools and Methods for Managing SNORT Sensors in Distributed Environments
- DNS Sinkholing to Reduce Network Compromises
- Symantec Corporation and Temple University - Securing a Free and Open University Environment
- FireEye, Inc. and University of California, Berkeley - Combating Stealth Malware and Botnets in Higher Education
- Using OSSEC Open-Source, Host-Based Intrusion Detection
- Web Application Firewalls at SCSU: Why and How
- University of Albany's IP Blocker: Elevating IDS to IPS

- Malware Detection and Mitigation with Passive DNS and Blackhole DNS (seminar)
- A Gentle Introduction to Bro
- VirusTotal (Free Scanning Tool That Uses Multiple AV Engines)

Top of page

Backups

Objective: To ensure the integrity and availability of information processed and stored within information processing facilities.

Key Question: Do we make copies of information, software, and system images regularly and in accord with policy requirements?

System backups are a critical issue and the integrity and availability of important information and software should be maintained by making regular copies to other media. Risk assessments should be used to identify the most critical data. Develop well-defined procedures. Establish well-defined long term storage requirements and testing/business continuity planning.

- University of Iowa Backup and Recovery Policy
- East Carolina University SYSTEM Server Disaster Recovery Plan
- Disaster Recovery Planning: How to Build It, How to Test It
- Preparing for Big Data: Strategic Storage Planning at Lehigh University
- Next-Generation Backup: Simpler and Cheaper, with Disaster Recovery Capability

Top of page

Logging and Monitoring

Objective: To detect unauthorized activities occurring that may have a detrimental effect upon information processing facilities.

Key Question: Do we have processes and methods to reliably record, store, monitor, and review system events?

Effective logging allows us to reach back in time to identify events, interactions, and changes that may have relevancy to the security of information resources. A lack of logs often means that we lose ability to investigate events (e.g. anomalies, unauthorized access attempts, excessive resource use) and perform root cause analysis to determine causation. In the context of this control area, logs can be interpreted very broadly to include automated and hand written logs of administrator and operator activities taken to ensure the integrity of operations in information processing facilities, such as data and network centers.

How do we protect the value of log information?

Effective logging strategies must also consider how log data can be protected against tampering, sabotage, or deletion that devalues the integrity of log information. This usually involves consideration of role based access controls that partition the ability to read and modify log data based on business needs and position responsibilities. In addition, timestamp information is extremely critical when performing correlation analysis between log sources. One essential control needed to assist with this is ensuring that institutional systems all have their clocks synchronized to a common source (often achieve via NTP server) so that timelining of events can be performed with high confidence.

What should we log?

The question of what types of events to log must take into consideration a number of factors including relevant compliance obligations, institutional privacy policies, data storage costs, access control needs, and the ability to monitor and search large data sets in an appropriate time frame. When considering your overall logging strategy it can very often be helpful to “work backwards”. Rather than initially attempting to catalog all event types, it can be useful to frame investigatory questions beginning with those issues that occur on regular basis or have a potential to be associated with significant risk events (e.g. abuse/attacks on ERP systems). These questions can then lead to a focused review of the security event data that has the most relevance to these particular questions and issues. Ideally events logs should include key information including:

- User IDs, System Activities; Dates, Times and Details of Key Events
- Device identity or location, Records of Successful and Rejected System Access Attempts;
- Records of Successful and Rejected Resource Access Attempts; Changes to System Configurations; Use of Privileges,
- Use of System Utilities and Applications; Files Accessed and the Kind of Access; Network Addresses and Protocols;
- Alarms raised by the access control system, Activation and De-activation of Protection systems, such AV & IDS

Useful Resources

- EDUCAUSE: Improving Security Event Correlation and Analysis Using Intelligent Agents
- EDUCAUSE: REN-ISAC and CSI2---The Security Event System
- E-Discovery Toolkit
- Critical Log Review Checklist for Security Incidents

Top of page

Control of Operational Software

Objective: To ensure the integrity of operating systems.

Make sure to establish and maintain documented procedures to manage the installation of software on operational systems. Operational system software installations should only be performed by qualified, trained administrators. Updates to operational system software should utilize only approved and tested executable code. It is ideal to utilize a configuration control system and have a rollback strategy prior to any updates. Audit logs of updates and previous versions of updated software should be maintained. Third parties that require access to perform software updates should be monitored and access removed once updates are installed and tested.

Useful Resources

- ASU Change Management Process
- CCIT Change Management

Top of page

Technical Vulnerability Management

Objective: To prevent exploitation of technical vulnerabilities.

Key Question: How can we effectively manage technical vulnerabilities?

Technical vulnerabilities can introduce significant risks to higher-education institutions that can directly lead to costly data leaks or data breach events. Even with this fact is widely acknowledged, developing frameworks for detecting, evaluating, and rapidly addressing vulnerabilities is often a significant challenge. To help us approach this section it is often useful to look at 5 critical success factors (below) that drive effective threat and vulnerability management approaches.

1. **Knowing What We Have (Asset Inventory):** It is imperative to have an up-to-date inventory of your asset groups to allow for action to be taken once a technical vulnerability if reviewed and a mitigation strategy agreed on. These inventories also lend us the ability identify and prioritize “high risk systems” where the impact of technical vulnerabilities can be greatest.
2. **Establishing Clear Authority to Review Vulnerabilities:** Because probing a network for vulnerabilities can disrupt systems and expose private data, higher education institutions need a policy in place and buy-in from the top before performing vulnerability assessments. Many colleges and universities address this issue in their acceptable use policies, making consent to vulnerability scanning a condition of connecting to the network. Additionally, it is important to clarify that the main purpose of seeking vulnerabilities is to defend against outside attackers. (A public health metaphor may help people understand the need for scanning-we are looking for symptoms of illness.) There is also a need for policies and ethical guidelines for those who have access to data from vulnerability scans. These individuals need to understand the appropriate action when illegal materials are found on their systems during a vulnerability scan. The appropriate action will vary between institutions (for example, public regulations in Georgia versus public regulations in California). Some organizations may want to write specifics into policy, whereas others leave policy more open to interpretation and address specific issues through procedures such as consulting legal counsel.
3. **Vulnerability Awareness and Context:** It is important that we keep up-to-date with industry notices about technical vulnerabilities and evaluate risk and mitigation strategies. Vulnerability notices are released on a daily basis and a plan needs to be in place for how to track, analyze, and prioritize our efforts.
4. **Risk and Process Integration:** Technical vulnerability review is an operational aspect of an overall information security risk management strategy. As such, vulnerabilities must be analyzed in the context of risks including those related to the potential for operational disruption. These risks must also have a clear reporting path that allows for appropriate awareness of risk factors and exposure. Lastly, vulnerability management should also integrated into change management and incident management processes to inform the review and execution of these areas.
5. **System and Application Lifecycle Integration:** The review of vulnerabilities also must be integrated in system release and software development planning to ensure that potential weaknesses are identified early to both lower risks and manage costs of finding these issues prior to identified release dates. (Three approaches to managing technical vulnerabilities in application software are described in the Application Security and Software Development Life Cycle presentation from the 2010 Security Professionals Conference.)

Technical Vulnerability Scanning

Depending on the size and structure of the institution, the approach to vulnerability scanning might differ. Small institutions that have a good understanding of IT resources throughout the enterprise might centralize vulnerability scanning. Larger institutions are more likely to have some degree of decentralization, so vulnerability scanning might be the responsibility of individual units. Some institutions might have a blend of both centralized and decentralized vulnerability assessment. Regardless, before starting a vulnerability scanning program, it is important to have authority to conduct the scans and to understand the targets that will be scanned.

Vulnerability scanning tools and methods are often somewhat tailored to varied types of information resources and vulnerability classes. The table below shows several important vulnerability classes and some relevant tools.

Common Types of Technical Vulnerabilities	Relevant Assessment Tools
Application Vulnerabilities	Web Application Scanners (static and dynamic), Web Application Firewalls
Network Layer Vulnerabilities	Network Vulnerability Scanners, Port Scanners, Traffic Profilers
Host/System Layer Vulnerabilities	Authenticated Vulnerability Scans, Asset and Patch Management Tools, Host Assessment and Scoring Tools

Common Challenges

- "Scanning Can Cause Disruptions." IT operations teams are quite reasonably very sensitive about how vulnerability scans are conducted and keen to understand any potential for operational disruptions. Often legacy systems and older equipment can have issues even with simple network port scans; To help with this issue, it can often be useful to build confidence in scanning process by partnering with these teams to conduct risk evaluations before initiating or expanding a scanning program. It is also often important to discuss the “scan windows” when these vulnerability assessments will occur to ensure that they do not conflict with regular maintenance schedules.
- "Drowning In Vulnerability Data and False Positives." Technical vulnerability management practices can produce very large data-sets. It is important to realize that just because a tool indicates that a vulnerability is present that there are frequently follow-up evaluations needed validate these findings. Reviewing all of these vulnerabilities is usually infeasible for many teams; For this reason, it is very important to develop a vulnerability prioritization plan before initiating a large number of scans. These priority plans should be risk driven to ensure that teams are spending their time dealing with the most important vulnerabilities in terms of both likelihood of exploitation and impact.

Top of page

Information Systems Audit Considerations

Objective: Minimize the impact of audit activities on operational systems.

It is important to ensure that all IT controls and information security audits are planned events, rather than reactive 'on-the-spot' challenges. Most universities undergo a series of audits each year ranging from financial IT controls reviews to targeted assessments of critical systems. Audits that include testing activities can prove disruptive to campus users if any unforeseen outages occur as a result of testing or assessments.

Through working with campus leadership, it should be possible to determine when audits will occur and obtain relevant information in advance about the specific IT controls that will be examined or tested.

Develop an 'audit plan' for each audit that provides information relevant to each system and area to be assessed. These audit plans should take into consideration:

- Asset Inventory with contact information for system administrators/owners;
- Requirements for testing/maintenance windows;
- Information about backups (if applicable) in case systems later need to be restored due to unplanned outages;
- Checklists or other materials provided in advance by auditors, etc.

If applicable, work with IT and campus departments to provide audit preparation services to ensure that everyone understands their roles in the audit and how to respond to auditors' questions, issues and concerns. Protecting sensitive information during audits is critical, and documents provided to auditors should be recovered if possible, shortly before audits are completed.

Any and all audit activity, to assess an operational system, should always be managed to minimize any impact on the system during required hours of operation. Any testing of operational systems that could pose an adverse effect to the system should be conducted during off hours.

Top of page

Resources

EDUCAUSE Resources

EDUCAUSE Resources & Resource Center Pages

- 7 Things You Should Know About Cloud Security
- Cloud Computing Security
- Dropbox Security & Privacy Considerations

HEISC Toolkits/Guidelines

- E-Discovery Toolkit
- Electronic Records Management Toolkit
- Guidelines for Data De-Identification or Anonymization
- Guidelines for Information Media Sanitization
- Managing Malware
- Two-Factor Authentication

Templates/Sample Plans

- East Carolina University SYSTEM Server Disaster Recovery Plan
- University of Houston Information Security Resources and Operations Manual
- Indiana University UITS Change Management
- Northwestern University Information Technology Information and Systems Security/Compliance
- University of Missouri Systems Electronic Records Administration

Security Professionals Conference 2014

- Splunk: Quick Start and Lessons Learned from OSU

Security Professionals Conference 2013

- How Advanced Log Management Can Trump SIEM: Tales of Woe and Glory
- Bring Your Own Cloud: Data Management Challenges in a Click-Through World

Enterprise IT Leadership Conference 2013

- Providing Private Cloud Services To Support HIPAA Compliance

EDUCAUSE Annual Conference 2012

- Reaching a Higher Elevation: Supporting High-Value, High-Risk Cloud Services
- Disaster Recovery Planning: How to Build It, How to Test It
- Raising the Bar in Cloud Security for Higher Education
- Business Continuity Management Discussion
- Preparing for Big Data: Strategic Storage Planning at Lehigh University
- Next-Generation Backup: Simpler and Cheaper, with Disaster Recovery Capability
- Achieving Virtualization: The Holy Grail of IT
- Community and the Cloud: Shaping the Future of Technology Services for Higher Education

Security Professionals Conference 2012

- Tools and Methods for Managing SNORT Sensors in Distributed Environments
- DNS Sinkholing to Reduce Network Compromises

Southeast Regional Conference 2012

- The EITS Analysis Committee: A Grassroots Effort at Standardized Documentation and Diagramming Templates
- Inform, Engage, and Educate: How to Communicate Major Service and System Updates and Changes to the Campus
- Personal Storage in the Cloud

Mid-Atlantic Regional Conference 2012

- Leverage the Cloud + Leverage In-House + Improve Security = Save Money

EDUCAUSE Annual Conference 2011

- Building a Business Case for the Cloud
- The Titan Cloud: CSU Fullerton's Virtual Computing Infrastructure Implementation

Security Professionals Conference 2011

- Information Technology Standards at the University of Illinois: Common Challenges and Solutions
- Network Segmentation: Virtual Routing Implementation
- Seminar 02P - Malware Detection and Mitigation with Passive DNS and Blackhole DNS
- A Gentle Introduction to Bro

Initiatives, Collaborations, & Other Resources

- ECAR Working Groups; Bring together higher education IT leaders to address core technology challenges.

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security

27002:2013 Information Security Management **Chapter 12**: Operations Security **ISO/IEC 27003:2010** **ISO/IEC 27004:2009**	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO12.01** **APO12.02** **APO12.03** **APO12.04** **APO13.01** **BAI01.06** **BAI06.01** **BAI07.04** **BAI10.01** **BAI10.02** **BAI10.03** **BAI10.05** **DSS02.07** **DSS05.01**	**Req 2** **Req 6** **Req 12**	**ID.BE-4** **ID.4A-1** **ID.RA-5** **PR.DS-4** **PR.DS-6** **PR.DS-7** **PR.IP-1** **PR.IP-3** **PR.IP-4** **PR.IP-12** **PR.PT-1** **DE.CM-3** **DE.CM-4** **DE.CM-5** **DE.CM-8**	**45 CFR 164.308(a)(5)(ii)(B)** **45 CFR 164.308(a)(7)(ii)(A)** **45 CFR 164.308(a)(7)(ii)(A)** **45 CFR 164.316(a), 45 CFR 164.316(b)(1)** **45 CFR 164.308(a)** **45 CFR 164.310(d)(1)** **45 CFR 164.310(d)(2)(iv)** **45 CFR 164.312(c)(1)** **45 CFR 164.312(b)** **45 CFR 164.308(a)(5)** **45 CFR 164.312(a)(1)**

Top of page