

## **Applications Evaluation Guide**

Developed by the UNM Information Assurance team in conjunction with IT Project Leaders, June 2009.

### **Audience**

Primary: IT Project Leaders

Secondary: Development Staff, Network Operating System Engineers

### **Purpose**

To help determine a system's or application's information security requirements and identify, as early in the system life cycle as possible, any information security-related requirements that will need to be addressed.

### **Introduction**

The National Institute of Standards and Technology's (NIST) Computer Security Resource Center (CSRC) and the SANS Institute have many resources that IT Project Leaders, Developers, Network Engineers and Operating System Engineers can use to learn about information assurance, to stay abreast of threat vectors, to understand how to properly configure environments to protect data, and to raise awareness with the user community. Fortunately or unfortunately, the amount of material available on the NIST CSRC website, <http://csrc.nist.gov>, and SANS' 20 Critical Security Controls website, [www.sans.org/cag/guidelines.php](http://www.sans.org/cag/guidelines.php), is massive and, in many cases, presented at a very high level. Subsequently, a fair amount of time is typically needed to peruse the materials and develop application and environment-specific security and privacy acceptance test plans and/or even rudimentary checklists.

That said, the following Applications Evaluation Guide is presented as just that—a guide—and it should not be considered comprehensive or appropriate for each and every application, operating environment, or situation; however, if used in conjunction with the NIST and SANS checklists, this Applications Evaluation Guide should be a good starting point for discussions with IT personnel, vendors and the user community.

One of the first challenges for IT Project Leaders is to develop a firm understanding of the local data requirements, the data flow, the business problem being solved, and as many of the parties and integration points involved as possible. As a matter of fact, even the NIST publication "SP 800-70: Security Configuration Checklists Program for IT Products", [http://checklists.nist.gov/docs/SP\\_800-70\\_20050526.pdf](http://checklists.nist.gov/docs/SP_800-70_20050526.pdf), states that the first step is to determine local operational requirements before reviewing and tailoring any checklists to a local environment.

Hopefully, the guide<sup>1</sup> will help UNM IT Project Leaders, Developers, Network Engineers, Operating System Engineers, and System Administrators further develop local operational requirements which should, in turn, help the IT community at UNM and the UNM user community (and/or partners, vendors, affiliates, etc.) build a more secure IT infrastructure and identify any weak links in the security chain—the risk to which can then either be accepted, shifted, or mitigated.

### **Format**

The Guide is divided into three (3) general information assurance safeguard categories:

1. **Technical Safeguards** - Technology-oriented measures such as specific hardware/software or device configurations that, if implemented properly, can often reduce or mitigate certain risks.
2. **Administrative Safeguards** - Policies and procedures that, if followed, can often prevent or mitigate certain risks.
3. **Physical Safeguards** - Non-high-technology approaches such as doors, locks, cameras, and fencing that can often prevent or mitigate certain risks too.

While there are no guarantees that adhering to the following Guide and/or strictly following the NIST, HIPAA, or SANS checklists will prevent data loss or system breaches, one can probably guarantee that critical pieces of data and information will be compromised if appropriate IT Security and Privacy safeguards are not implemented properly. That said, one should remember that security is a business decision and is usually centered on reducing or mitigating risks. IT security risks can usually never be eliminated but they can be managed.

---

<sup>1</sup> **Note:** The IT-at-UNM Applications Evaluation Guide should be used in conjunction with other publically available checklists such as the ones developed by The NIST Checklist Program. (formerly the NIST Security Configuration Checklist Program), <http://checklists.nist.gov/>, and The U.S Department of Health and Human Services HIPAA Security Information Series, [http://www.cms.hhs.gov/EducationMaterials/04\\_SecurityMaterials.asp](http://www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp), and the SANS Institute's Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines, [www.sans.org/cag/guidelines.php](http://www.sans.org/cag/guidelines.php).

### **The Guide's Goals**

Generally speaking, the Guide's goals are to protect the **confidentiality, integrity, and availability** of information regardless of the form the data may take (electronic, print, or other forms).

1. **Confidentiality** is the property of preventing disclosure of information to unauthorized individuals or systems. This simply means that the information is known no more widely than necessary.
2. **Integrity** means that data cannot be modified without authorization and is the assurance that the information is untainted. Note that this does not deal with the *accuracy* of the information—it strictly means that the information put into the computer is the same as the information that comes back later.
3. **Availability** means that, when the information is needed, it is ready for use. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to be available at all times and are designed to prevent service disruptions due to power outages, hardware failures, denial-of-service attacks, and/or system upgrades.

### **Data Classification**

While a copy of the UNM Data Classification Standard is attached; visit <http://cio.unm.edu/standards> to be assured you have the most recent version.

## Applications Evaluation Guide

### I. Technical Safeguards

I.1	<p>Are Credit Card Numbers or Primary Account Numbers (PAN) being accessed, collected, stored or transmitted?</p> <p>If so, then the Payment Card Industry Data Security Standard (PCI DSS) must be reviewed and adhered to (or, if not followed, the business decision and rationale should be documented.)</p> <p>The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.</p> <p><a href="https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml">https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml</a></p> <p><b><i>Credit Card Numbers and PANs are the only data element that we are absolutely required to encrypt.</i></b> These data elements are defined as "E" Class by the UNM Data Classification standard, <a href="http://cio.unm.edu/standards/DataClassificationStandard041608.pdf">http://cio.unm.edu/standards/DataClassificationStandard041608.pdf</a>. Examples of acceptable encryption technologies can be found in the draft UNM Data Encryption standard, <a href="http://cio.unm.edu/standards/UNMDataEncryptionDRAFTStandard-v01.pdf">http://cio.unm.edu/standards/UNMDataEncryptionDRAFTStandard-v01.pdf</a>.</p>
-----	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

I.2	<p>Are Social Security Numbers being accessed, collected, stored or transmitted? If so, encryption technologies are <i>recommended</i> for both data at rest and data in transit.</p> <p>Currently, SSNs are <i>not</i> "E" class data but could be classified as such if the Data Steward(s) makes that determination.</p> <p>By itself, the SSN is often not encrypted; however, when used in conjunction with other personally identifiable data elements such as Date of Birth, Name, and Address, many organizations encrypt the records since, when used together, the data can be used to conduct identity theft. Additionally, many data breach notification laws do not require customer notification of a breach if SSNs and other personally identifiable data elements are compromised so long as the data elements were encrypted.</p>
-----	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.3	<p>Are any other "E" or "C" Class data elements being accessed, collected, stored or transmitted? If so, encryption technologies are recommended for both data at rest and data in transit.</p> <p>Often, individual data elements such as Date of Birth, Name, and Address may be considered to be "P" Class (i.e. data which may be released to the public) and may not warrant encryption; however, when used in conjunction with financial account numbers such as checking account number, these same data elements may warrant a reclassification to "C" Class or "E" Class (and, subsequently, may need to be encrypted.)</p>
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.4	<p>What Access Controls are in place and is there an auditable process by which only those individuals with a documented business need are given permission to access, create, update, or delete?</p> <p>Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum (and only the minimum) necessary information needed to perform job functions.</p> <p>Generally, permissions should be "deny by default" and should not be granted beyond what is minimally necessary to perform one's job.</p>
-----	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.5	<p>Is there a means of uniquely identifying each user to the system?</p> <p>Without unique userIDs or with shared IDs, accountability is problematic.</p> <p>While the use of functional or shared userIDs is generally discouraged, business needs may warrant their use. In such cases, compensating controls should be implemented to mitigate the risk associated with sharing IDs and not having individual accountability.</p>
-----	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

1.6	Are all individuals or userIDs with broad access identified or can they be?
	<p>Many applications and databases permit having a person or a series of persons with System Administrator rights or very broad permissions. Often such permissions enable the person(s) to access, create, update, and/or delete outside of any audit logging process. Keeping track of these userIDs and roles is an important aspect of auditing an application.</p>

1.7	Is application and/or database logging enabled and how are logs maintained?
	<p>If data is manipulated improperly or if there is unauthorized access, often the application and/or database logs can be used to determine the series of events, identify the parties involved, and help define the scope of any activities.</p> <p>Such logs should also not be able to be disabled without appropriate permissions via an auditable process.</p>

1.8	Is direct application and/or direct database access needed or permitted from "off site"?
	<p>Often, programmer/analyst and System Administrator access is restricted to local workstations or to only those computers with certain IP addresses. Occasionally, access is requested or needed from off site—using a computer outside of the local or restricted IP address range. In just instances, a secure remote access technology, such as VPN, may be implemented.</p> <p>The use of remote access technologies, such as VPN, should be denied by default and only used/permitted when no other means of securely accessing the application or database can be identified or when business needs dictate the need for remote access directly into the application or database management system.</p> <p>"One-over-one" approvals should be required before permission to use remote access technologies is granted. Such requests should be logged and their use limited to only those days and times of day when absolutely necessary. Remote Access logs should also be enabled to track actual use.</p>

I.9		<p>Are perimeter firewalls, application firewalls, and/or intrusion detection/prevention systems implemented and being managed appropriately?</p> <p>Having hardware or software-based defense-in-depth technologies are a good practice; however, to be truly effective, these technologies must be maintained, kept up to date, and have their logs reviewed daily by security analysts.</p> <p>How these devices are configured should be documented; changes should be vetted by a review board; and their configurations should be backed up (and able to be restored) in case the device fails.</p>
I.10		<p>What is the patch management policy?</p> <p>While regularly applying vendor-supplied patches to the operating system, anti-virus software, the application, and/or to the database management system requires regression testing, not regularly applying patches is a risk (especially if the patches fix vulnerabilities that have been exploited "in the wild.")</p> <p>Patch management should be addressed for both workstations (i.e. PC, laptop) and servers.</p>
I.11		<p>Are web and email clients (and servers) configured to filter and block traffic/messages that could contain malicious content (including SPAM)?</p> <p>While anti-virus software and anti-malware software catch the majority of virus-laden email attachments, defense-in-depth is a best practice. Having several means of catching or preventing malicious software from infecting a workstation or server is prudent.</p>
I.12		<p>Are there restrictions on sharing resources such as directories or printers (and when such digital assets are shared, is the request and approval logged and periodically reviewed)?</p>
I.13		<p>Have default administrative userIDs and passwords been changed or disabled?</p> <p>This is an issue for servers, multi-function printers, demote access technologies, routers, switches, firewalls, database management systems, and even workstations.</p>

I.14		<p>What are the backup policies? How often are servers, application data, and database management systems backed up and where do the backups go? Is that facility secure? Are there appropriate and reasonable backup storage access and media sign-out procedures? Are the backups encrypted?</p> <p>Part of information security's responsibility is ensuring "availability". Subsequently, having backups is important as is periodically testing the restoration process. Also, if the backup media are not properly secured, "E" Class and "C" Class data can be compromised without a single system being breached.</p>
I.15		<p>On all servers, printers, workstations, routers, switches, firewalls, IDS, etc., all ports and services should be disabled and turned off except for those minimally needed to get the job done (i.e. deny-by-default.)</p> <p>Rather than having all ports and services enabled and running and then turning those off that are not believed to be needed, all ports and services should be disabled and turned off and only turned on if absolutely necessary. The activation of ports and/or services should be part of a Change Review Board process and copiously documented.</p>
I.16		<p>Are all servers, printers, workstations, routers, switches, firewalls, IDS, etc. scanned periodically with vulnerability assessment tools (to ensure that all appropriate patches have been applied)?</p>
I.17		<p>Is the application web-based with web-based authentication?</p> <p>If so, is Transport Layer Security (TLS) or its predecessor, Secure Sockets layer (SSL), being used?</p>

## II. Administrative Safeguards

II.1		<p>Is there a means by which only those individuals who absolutely need access are granted access?</p> <p>Such a process often involves defining roles and determining what access is warranted by each role. Then, individuals are mapped against those roles.</p> <p>The process should have an audit trail with justification of roles and permissions.</p>
II.2		<p>Have the personnel who develop, support, maintain, install, patch, grant access to others and/or access "E" or "C" Class data been vetted prior to and throughout their employment?</p> <p>Just because someone had a clean criminal record when they started working does not mean that they haven't had a run in with law enforcement since that makes giving them access to a server or application problematic.</p>
II.3		<p>Are LoginIDs and passwords required to gain access to the network and/or application (i.e. single-factor authentication)? Is there a business need/requirement for stricter controls (i.e. one-time passwords)?</p> <p>A password standard should exist that addresses password length and complexity as well as time between changing. Also, the standard should address attempts to compromise or guess passwords (i.e. after 3 guesses, the account is disabled and a re-activation process must then be followed.)</p>
II.4		<p>Are duties periodically rotated among personnel and segregated?</p> <p>A "jack of all trades" system administrator or database administrator is more likely able to get away with bad behavior if s/he does not have to share responsibilities and no one is aware of what s/he is doing.</p>
II.5		<p>Is there an acceptable use policy (AUP) and are users, system administrators, etc. required to annually read and sign it?</p> <p>Are AUP violations taken seriously, investigated consistently, and applied equitably? If not, don't expect users to honor it.</p>

II.6		<p>Are users required to sign a non-disclosure agreement (NDA)?</p> <p>Inadvertent data disclosures may occur. Without an NDA in place, users, system administrators and database administrators may not know that they are required to keep data and information confidential.</p>
II.7		<p>Are service and operating level agreements agreed upon and in place?</p> <p>Unplanned outages may be an indication of a failed hack or of a successful breach that is being cleaned up after by the cyber criminal. Worst case: unscheduled or unplanned outages negatively affect the availability of the application.</p>
II.8		<p>Have Data Flow Diagrams (DFD) been developed that document the flow of data into and out of the application? Have these DFDs been verified?</p> <p>If no one knows and/or if no one has verified the DFDs, securing the data will be almost impossible. In order to know how to secure or when to encrypt, one must "know they data."</p>
II.9		<p>Have Data Dictionaries been developed that document what the operational definition is for each data element, how the data is created, what its retention requirements are, etc.?</p> <p>Similar to DFDs, if no one knows what the data is and how it is used, securing the data is almost an impossible task. In order to know how to secure or when to encrypt, one must "know they data."</p>
II.10		<p>Is there a policy or procedure for shredding reports that may or do contain "E" or "C" Class data?</p> <p>Dumpster diving still occurs and is still a viable way for criminals to obtain tidbits of data that, when aggregated, are turned into information.</p>
II.11		<p>Can responsibility and/or liability for a breach be shifted to someone else?</p> <p>Information security insurance is becoming more and more available and vendors can often be held responsible if their application fails.</p>

### III. Physical Safeguards

III.1		<p>Is there an inventory management system and/or process for all hardware (i.e. servers, workstations, printers, fax machines, etc.)?</p> <p>If you do not know what you are supposed to have, you have little chance of knowing when something is missing (or has been stolen or lost.)</p>
-------	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

III.2		<p>Is there a physical access control system, is it monitored, and managed properly?</p> <p>If personnel, customers, or vendors are permitted to enter the data center or programmer/analyst facilities without escort, there is an increased risk that printed reports or hardware will be absconded.</p>
-------	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

III.3		<p>Are the physical safeguards "detective" or "preventive"?</p> <p>There are no "right" answers here but it is important to know so that risks can be assessed.</p> <p>Detective safeguards are ones that detect when a breach or loss has occurred or can provide evidence of a breach or loss. Alarms, motion detectors, and surveillance systems fall into this category.</p> <p>Preventive safeguards are ones that try to prevent a breach or loss from occurring. Fences, locks, safes, guards and dogs fall into this category..</p>
-------	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

## Applications Evaluation Guide

abbreviated version - checklist oriented

### I. Technical Safeguards

I.1	Are Credit Card Numbers or Primary Account Numbers (PAN) being accessed, collected, stored or transmitted?
I.2	Are Social Security Numbers being accessed, collected, stored or transmitted? If so, encryption technologies are <i>recommended</i> for both data at rest and data in transit.
I.3	Are any other "E" or "C" Class data elements being accessed, collected, stored or transmitted?
I.4	What Access Controls are in place and is there an auditable process by which only those individuals with a documented business need are given permission to access, create, update, or delete?
I.5	Is there a means of uniquely identifying each user to the system?
I.6	Are all individuals or userIDs with broad access identified or can they be?
I.7	Is application and/or database logging enabled and how are logs maintained?
I.8	Is direct application and/or direct database access needed or permitted from "off site"?
I.9	Are perimeter firewalls, application firewalls, and/or intrusion detection/prevention systems implemented and being managed appropriately?
I.10	What is the patch management policy?
I.11	Are web and email clients (and servers) configured to filter and block traffic/messages that could contain malicious content (including SPAM)?

I.12	Are there restrictions on sharing resources such as directories or printers (and when such digital assets are shared, is the request and approval logged and periodically reviewed)?
I.13	Have default administrative userIDs and passwords been changed or disabled?
I.14	What are the backup policies? How often are servers, application data, and database management systems backed up and where do the backups go? Is that facility secure? Are there appropriate and reasonable backup storage access and media sign-out procedures? Are the backups encrypted?
I.15	On all servers, printers, workstations, routers, switches, firewalls, IDS, etc., are all ports and services disabled and turned off except for those minimally needed to get the job done (i.e. deny-by-default)?
I.16	Are all servers, printers, workstations, routers, switches, firewalls, IDS, etc. scanned periodically with vulnerability assessment tools (to ensure that all appropriate patches have been applied)?
I.17	Is the application web-based with web-based authentication? If so, is Transport Layer Security (TLS) or its predecessor, Secure Sockets layer (SSL), being used?

## II. Administrative Safeguards

II.1	Is there a means by which only those individuals who absolutely need access are granted access?
II.2	Have the personnel who develop, support, maintain, install, patch, grant access to others and/or access "E" or "C" Class data been vetted prior to and throughout their employment?
II.3	Are LoginIDs and passwords required to gain access to the network and/or application (i.e. single-factor authentication)? Is there a business need/requirement for stricter controls (i.e. one-time passwords)?
II.4	Are duties periodically rotated among personnel and segregated?
II.5	Is there an acceptable use policy (AUP) and are users, system administrators, etc. required to annually read and sign it?
II.6	Are users required to sign a non-disclosure agreement (NDA)?
II.7	Are service and operating level agreements agreed upon and in place?
II.8	Have Data Flow Diagrams (DFD) been developed that document the flow of data into and out of the application? Have these DFDs been verified?
II.9	Have Data Dictionaries been developed that document what the operational definition is for each data element, how the data is created, what its retention requirements are, etc.?
II.10	Is there a policy or procedure for shredding reports that may or do contain "E" or "C" Class data?
II.11	Can responsibility and/or liability for a breach be shifted to someone else?

### III. Physical Safeguards

III.1	Is there an inventory management system and/or process for all hardware (i.e. servers, workstations, printers, fax machines, etc.)?
III.2	Is there a physical access control system, is it monitored, and managed properly?
III.3	Are the physical safeguards "detective" or "preventive"?