Lusaka Elunda2 University

Risk management

## A. Process Overview

Step 1: IT Mission Impact Analysis

* Determine your department’s ***critical assets*** (hardware, software, information, people) based on Table 1 below and your department’s mission

Step 2: IT **Risk Assessment**

* Assess departmental security practices against University, national and international standards
* Map your department’s assets from Step 1 to the threat scenarios provided (and others that your department identifies)
* Assign weight to each threat to your assets based on the likelihood of it occurring in your environment and the impact of any vulnerability
* Prioritize the threats you face
* Map these threats back to response strategies provided (and others your department develops)
* Create (or update if you already have one) your department’s security plan for mitigating or accepting the identified risks
* Take into account previously implemented strategies and existing plans – use (and document) effort and analysis that you have already produced
* Document your key decisions and justifications

Step 3: IT Mission Continuity Planning

* Create (or update) a response plan for your department to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed
* Test your plan

Step 4: Evaluation and Reassessment

* Repeat Steps 1-3 every three years or when there are significant changes to departmental IT assets or risk environment
* Review the success of your prior analysis, testing and any responses made, whether they were corrective, preventative or post-incident
* Incorporate responses to any intervening changes (new operating system, critical applications or data, or University, state or federal standards)

See [section F.](#_F._Reporting_Requirements) below for the reporting requirements of this process, and see [Appendix A](#_Appendix_A:_Sample) for sample responses to these steps. These examples do not necessarily cover all the issues facing your department, but they are intended as examples of the type and level of response expected. The time necessary to complete the ITS-RM process will vary with the size of the department, the breadth of its mission and the complexity of its IT infrastructure. Departments should establish internal deadlines for the completion of each step of the process in order to ensure steady progress.

### Chart 1: IT Security Risk Management Process Flow

w_bnidno[1]w_bnidno[1]w_bnidno[1]

1. **Disaster recovery plan example**
2. **Interim manual procedures example**
3. **Criteria**
4. **Template**
5. **Assessment questions**
6. **Threat scenarios**
7. **Response strategies**
8. **Security plan template & example**

*Security*

*Plan*

*Interim*

*Manual*

*Procedures*

*Disaster*

*Recovery*

*Plan*

Step 4 – Evaluation and Reassessment

Required at least once every three years

Step 3 – Mission

Continuity Planning

Create a response plan to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed

Step 2 – Assess Risks

For each critical asset:

1. Assign weight to likelihood & impact of threats to each asset
2. Prioritize threats
3. Select response strategies
4. Develop security plan

*Critical*

*Assets*

*List*

Step 1 - Identify

Critical IT Assets

## B. Step 1: IT Mission Impact Analysis

The purpose of an information technology impact analysis is to identify IT-related departmental assets (e.g., information, people, software, hardware, facilities, etc.) and determine which of those assets are most critical to protect. As a general rule, [***an asset is critical***](#CriticalAsset) when its disclosure, modification, destruction, or misuse will cause harmful [***consequences***](#Consequence) to the department’s — or the University’s — goals and mission, or will provide an undesired and unintended benefit to someone. If an asset has any of the characteristics listed in Table 1, it should likely be deemed critical.

|  |
| --- |
| Table : Critical Asset Criteria |
| The asset is required to perform functions that result in existence or closure of the University or the Department |
| The asset is required to perform functions that instruction and other training services to University community members or the general public. |
| The asset is required to support teachers in their job. |
| The asset is required to support instruction. |
| The asset is required to support research grants. |
| The asset is required to provide central University business and support functions. |
| The asset is required to provide services on which multiple University departments or other institutions or agencies depend. |
| The asset concerns data which is highly sensitive or in other ways access restricted. |

Below is the template for doing a Mission Impact Analysis. Determine your department’s critical assets (hardware, software, information and people) based on Table 1 above and your department’s mission.

|  |  |
| --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Mission Impact Analysis Questions  The identification of information, computing hardware and software, and associated personnel that require protection against unavailability, unauthorized access, modification, disclosure or other security breaches.  *Note:* Any use of highly sensitive data (including Social Security numbers, student profile or history, etc.) is inherently a critical component of the unit’s mission and a source of significant risk. | |
| 1. What’s your department’s mission?  *See related list in* [*Table 1*](#_Table_1:_Critical) |  |
| 2. What are the key functions your department performs to implement your mission? |  |
| 3. What IT hardware infrastructure and assets are critical to the performance of those key functions? Please list these assets and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central and external (e.g., vendor) assets as appropriate, and list a system administrator, model number and operating system, where applicable, for each asset.  *Examples*: •Servers (including those hosted by others) •Desktops/laptops/PDAs that host critical or highly sensitive data |  |
| 4. What software applications are critical to the performance of those key functions? Please list these and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central and external (e.g., vendor, federal and state) assets as appropriate.  *Note:* Even common applications, like web browsers and Microsoft Office, may be critical and must be kept updated and secure to protect your systems. |  |
| 5. What IT data assets are critical to the performance of those key functions? Please list these assets and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central and external (e.g., vendor, federal and state data swapping) assets as appropriate.  *Examples*: •*Academic*: instructional resources, databases necessary to maintain a given research program •*Administrative*: sensitive student or financial data necessary for business operations and student services •External data provider |  |
| 6. Provide a complete location inventory of all data used or stored in the department, whether in paper or electronic form |  |
| 7. What IT personnel are critical to the performance of those key functions? Please list the job roles and the incumbents’ names and prioritize them based on their criticality to the functions identified above. Be sure to include individual, departmental, central and external (e.g. vendor) personnel as appropriate.  *Examples*: •Server administrators •Local Support Partner (LSP) or Associate (LSA) •Database administrators •ITC Engineers who provide contracted support |  |
| Prepared by: Administrative contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Prepared by: Technical contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

## C. Step 2: IT Risk Assessment

In Step 1 you identified the critical IT assets in your department. In Step 2 you will analyze the risks facing those assets and identify and prioritize strategies for protecting them.

A focus on departmental mission is vital; departments cannot – and are not expected to – mitigate every risk but must prioritize based on the threat to their mission and available resources.

Three sets of templates and/or tools are included to assist in this process:

*2.1*[***Risk assessment questions***](#_Step_2.1:_Risk)*(with paths determined by applicability of laws)*

* Assess departmental security practices against University, national and international standards

*2.2* [***Threat, attack and vulnerability scenarios***](#_Step_2.2:_Threat,) *(with response strategies)*

* Map your department’s assets from Step 1 to the threat scenarios provided (and others that your department identifies)
* Assign weight to each threat to your assets based on the likelihood of it occurring in your environment and the impact of any vulnerability
* Prioritize the threats you face
* Map these threats back to response strategies provided (and others your department develops)

*2.3* [***Security plan development***](#_Step_2.3:_Remediation) *(template)*

* Create (or update if you already have one) your department’s security plan for mitigating or accepting the identified risks
* Take into account previously implemented strategies and existing plans – use (and document) effort and analysis that you have already produced
* Document your key decisions and justifications

### Step 2.1: Risk Assessment Questions

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Risk Assessment Questions: General  These questions will help determine and evaluate threats to the resources identified through a mission impact analysis, as well as adherence to general secure computing practices. | | | |
|  | Yes | No | Documentation location or explanation for not following |
| ***A. Physical Security*** | | | |
| 1. Are all computers located in areas that are not easily accessible to outsiders? |  |  |  |
| 2. Are mission critical systems located in a locked location to which access is restricted to authorized personnel only? |  |  |  |
| 3. Are faculty and staff taking responsibility for locking doors and windows where computers are housed? |  |  |  |
| 4. Has physical security been reviewed with the University Police and Facilities Management? |  |  |  |
| 5. Are department desktops and notebooks equipped with anti-theft devices? |  |  |  |
| 6. Are departmental keys logged in and out individually with one staff person responsible for the tracking of the keys? Has this procedure been approved by Facilities Management (FM)? |  |  |  |
| 7. Are department servers physically secure in a separate area, i.e., physically restricted, a double-locked door, with card access and access logging.? |  |  |  |
| 8. Are servers in environmental control areas that include:  Smoke detectors?  Water detectors?  Fire suppression systems?  Temperature sensors? |  |  |  |

|  | Yes | No | Documentation location or explanation for not following |
| --- | --- | --- | --- |
| 9. Are mission critical servers away from high-traffic areas; e.g., not near an auditorium or along a well-travelled hallway? |  |  |  |
| 10. Are uninterruptible power supplies (UPS) with surge protection used on servers and other important hardware? |  |  |  |
| 11. Are surge protectors (at least) used on desktop computers? |  |  |  |
| 12. Are individual firewalls (software or hardware) installed on any desktops, laptops or servers in the department? |  |  |  |
| 13. Are security incidents (for example, unauthorized use, loss, theft, or compromise of devices) reported in compliance with the IT Security Incident Reporting policy? |  |  |  |
| 14. Is there an accurate inventory of all computing equipment and software? If so, is a copy of the inventory stored off-site? |  |  |  |
| 15. Do you have individual use devices with sensitive data in a publicly accessible area? |  |  |  |
| ***B. Account & Password Management*** | | | |
| 1. Do you have defined, documented criteria for granting access based on job responsibilities? |  |  |  |
| 2. Are all sensitive data used for authenticating a user, such as passwords, stored in protected files? |  |  |  |
| 3. Are users authorized to access only those resources required to perform their jobs and nothing more? |  |  |  |
| 4. Does the department deactivate accounts for terminated or transferred employees in a timely manner? |  |  |  |
| 5. Does the department periodically review current employee accounts that have not been used in a long time and consider deactivating them? |  |  |  |
| 6. Does the department prohibit shared accounts? If shared accounts are not prohibited, please list what systems/applications require shared accounts and justify continued use. |  |  |  |
| 7. Has the department emphasized to users that their password, along with their computing ID, is the key to their electronic identity? |  |  |  |
| 8. Does the department have a policy on keeping passwords confidential? |  |  |  |
| 9. Does the department assist users in selecting passwords that will ensure privacy while promoting regular use? |  |  |  |
| 10. Does the department require that passwords not be written down or shared, except for purposes of escrow? |  |  |  |
| 11. Does the department securely escrow passwords for accounts that may need to be accessed in the absence of their normal administrator or in an emergency situation? |  |  |  |
| 12. Does the department require that passwords on departmental workstations and servers be changed periodically? |  |  |  |
| 13. Is there a reasonable “previous used” password history list to deter users from repetitive use of the same password? |  |  |  |
| 14. Does the department require passwords for access to department workstations and servers? |  |  |  |
| 15. Does the department require the use of password-protected screen savers, automatic application timeouts and automatic network log-offs? |  |  |  |
| 16. Does the department log and review more than three attempts to enter a password for a given account? |  |  |  |
| 17. Does the department prohibit modems attached to servers and desktops that can receive calls? |  |  |  |
| C. Virus Protection | | | |
| 1. Is anti-virus software installed on all department computers? |  |  |  |
| 2. Is a procedure for updating the anti-virus software in place? For personal systems, if this is up to the user, are instructions and recommended update intervals provided? |  |  |  |
| 3. Does the department periodically remind users to open only attachments they are expecting? |  |  |  |
| ***D. Data Backup and Recovery*** | | | |
| 1. Have faculty and staff been advised of their personal computer backup options? Do they have instructions for the options and recommended backup cycles? |  |  |  |
| 2. Does the department regularly back up department servers? Does the server backup procedure include secure off-site storage? |  |  |  |
| 3. Does the department periodically test restoration of personal and server files? |  |  |  |
| 4. Do users store all local data in a single directory to simplify backup of personal data and ensure all data is captured? |  |  |  |
| 5. Are backup needs periodically reviewed? |  |  |  |
| 6. Does the department comply with University’s Records Retention and Disposition Policy? |  |  |  |
| 7. Does the department consult with the University Records Officer before implementing any electronic document management system? |  |  |  |
| E. Operating Systems | | | |
| 1. Are only officially allowed operating systems used? |  |  |  |
| 2. Are appropriate operating system updates and security patches being applied in a timely manner to all department computers and servers? |  |  |  |
| 3. Are servers and desktops periodically scanned by IT services for security vulnerabilities? |  |  |  |
| 4. Have unnecessary services and features in desktop and server operating system configurations been disabled? |  |  |  |
| 5. Is the use of shared drives or folders between desktop computers (peer-to-peer sharing) prohibited or restricted? |  |  |  |
| 6. Is it verified that file permissions are properly set on servers? |  |  |  |
| 7. Is Autorun and AutoPlay functionality disabled for removable disks and shares? |  |  |  |
| F. Application Software | | | |
| 1. Are appropriate application software updates and security patches being applied in a timely manner to electronic devices *on which University-related data reside or business is done* (whether University or personally owned devices)? |  |  |  |
| 3. If employees are allowed to install University applications at home, is it installed in compliance with the license, with security of the device, and has any necessary user acceptance form been completed and returned to the appropriate person? |  |  |  |
| 4. Does the staff have the appropriate level of access to applications based on their current responsibilities? |  |  |  |
| 5. Is application access promptly removed for employees who have left the department? |  |  |  |
| G. Confidentiality of Sensitive Data | | | |
| 1. Are all departmental locations of highly sensitive data, both electronic and paper, inventoried? |  |  |  |
| 2, Following the Electronic Data Removal policy,   1. are all data and software removed from hardware and electronic media prior to transfer within the university 2. are all hardware and media processed through appropriate Security check, Property Disposal, Transporting to the Depot, etc. when leaving the university? Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices. |  |  |  |
| 3. Is access to sensitive departmental data restricted? |  |  |  |
| 4. Is ownership of data clearly defined? |  |  |  |
| 5. Do data owners determine and periodically review appropriate levels of data security required? |  |  |  |
| 6. Is access to information technology resources explicitly granted to personnel by data owners? |  |  |  |
| 7. Have the faculty who are conducting research determined if the data they are collecting should be classified as sensitive? |  |  |  |
| 8. Do the faculty and staff who administer sensitive data understand and follow appropriate federal, state, grant agency, or university regulations for protecting and backing up data? |  |  |  |
| 9. Are student workers given access to confidential teaching, research or administrative data? If so, is their use of such data monitored closely? |  |  |  |
| 10. Are authentication, authorization, and data security policies established by data owners protected from compromise during data sharing and systems interoperability? |  |  |  |
| 11. Are user agreements clearly stating required authentication and protection levels established with all external agencies and institutions with which data are shared?  List all such data sharing relationships, indicating the data shared and the transmission method used (e.g. VPN, SFTP). |  |  |  |
| 12. Is the unencrypted transmission of highly sensitive data through e-mail prohibited? |  |  |  |
| 13. Do web-enabled transactions that require user authentication, transfer highly sensitive data, or transfer funds use encryption? |  |  |  |
| 14. Are the employees who have VPN access aware they should be disconnecting from the VPN when not in use and when away from their desk? |  |  |  |
| 15. If the department has a wireless network, is the network encrypted? If so, what type of encryption? |  |  |  |
| 16. Are cryptology technologies for data storage and transmission of data based upon open standards? |  |  |  |
| 17. Are encryption key management policy and procedures in place to ensure the integrity and recovery of encryption keys? |  |  |  |
| 18. Are all sensitive data stored and transmitted in compliance with the University’s Institutional Data Protection Standards and the Electronic Storage of Highly Sensitive Data policy? |  |  |  |
| 19. Do all iKey hardware token users disconnect from the VPN when not in use and/or when away from their desk? Are users aware of their responsibilities regarding the protection of the iKey token? |  |  |  |
| 20. Are all highly sensitive data files routinely and promptly deleted in a secure manner when no longer needed for their approved business purpose or official records retention? |  |  |  |
| 21. If highly sensitive data are stored on individual use devices or media, has the appropriate vice president or dean completed the approval form? |  |  |  |
| 22. If highly sensitive data are stored on individual use devices or media, is it encrypted? |  |  |  |
| 23. If highly sensitive data are stored on individual use devices or media, are all security requirements strictly followed? |  |  |  |
| 24. Do you have a regular schedule for scanning departmental devices for highly sensitive data? If so, what is it? |  |  |  |
| 26. Have you returned your SSN Inventory and Remediation Status Report, indicating that you have completed your remediation plan? |  |  |  |
| H. Security Awareness and Education | | | |
| 1. Are faculty and staff aware of their responsibility for computer security according to the University Policy? |  |  |  |
| 2. Have all copies of department software been properly licensed and registered? |  |  |  |
| 3. Has the University’s copyright policy been distributed and discussed within the department? |  |  |  |
| 4. Have University and department-specific security policies and procedures been documented and shared with all faculty and staff? |  |  |  |
| 5. Are faculty and staff keeping current on faculty and university security issues and alerts? |  |  |  |
| 6. Are suspected violations of security appropriately reported to a designated system or departmental administrator? |  |  |  |
| 7. Do your system administrators and other IT managers have training commensurate with the level of expertise required, which may include ability to identify threats, vulnerabilities and risks specific to your information resources? |  |  |  |
| 8. Are individuals involved in information technology management, administration, design, development, implementation, and/or maintenance aware of their security responsibilities and how to fulfill them? |  |  |  |
| 9. Does training for these individuals enable them to identify and evaluate threats, vulnerabilities, and risks and understand best practices relevant to the systems components and resources for which they are responsible? |  |  |  |
| 10. Does the department encourage staff to take available cyber security awareness classes? |  |  |  |
| 11. Do all departmental staff take any “Information Technology Security Awareness” like Tutorial annually? |  |  |  |
| ***I. Publicly Accessible Computers (Computing lab, public kiosks, etc.)*** | | | |
| 1. Are the computers created with a software image configured for the greatest practicable restrictions on disk access, software installation and user rights? |  |  |  |
| 2. Are the computers refreshed frequently (daily, if possible) to force reversion to the designated software image and the removal of personal data? |  |  |  |
| 3. Are log-in IDs required? |  |  |  |
| 4. Is information posted (either by sign or log-in screen) warning users to log out of all applications, Web sessions, server connections, etc. to prevent access to their personal data by subsequent users? |  |  |  |
| 5. Are extensive anti-theft devices utilized, including locking down all peripherals and locking the computer case? |  |  |  |
| 6. Are users automatically logged-off after a short period of inactivity? |  |  |  |
| ***J. Review and Response*** | | | |
| 1. Is there a documented procedure for handling exceptions to security policies and standards? Does this procedure include higher management level review of exception approvals? |  |  |  |
| 2. Are critical systems and infrastructures, including all those storing or transmitting highly sensitive data, formally identified on a periodic basis? |  |  |  |
| 3. Do procedures for development, installation, and changes to systems and infrastructures include review and approval steps for security implications and design features? |  |  |  |
| 4. Do you have a written process for handling suspected breaches to security safeguards (e.g. intrusion detection)? |  |  |  |
| 5. Is a process in place to identify and evaluate threats and to assign appropriate action based upon risks? |  |  |  |
| 6. Does your hardware firewall technology have security logging turned on? |  |  |  |

| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| --- | --- |

### Step 2.2: Threat, Attack and Vulnerability Scenarios

Completion of the previous section of risk assessment questions (Step 2.1) provided a sense of current vulnerabilities. Addressing all these vulnerabilities may not be practical, however; and a way to hone in on the most vital ones to address is needed. This section guides you in thinking of these vulnerabilities in the context of potential threats and the likelihood these threats will occur. Once these connections are well understood, you will be ready to move on to development of a security plan (Step 2.3).

Below is a template for a threat-based risk assessment. It provides a checklist of strategies to deal with common threats. The information collected during this process can be plugged into and expanded upon to create (or update) your security plan (Step 2.3), identifying which strategies are already in place, which ones need to be implemented and which ones are either unnecessary or unjustifiable.

In this template, [***threats***](#Threat), [***attacks***](#Attack) and [***vulnerabilities***](#Vulnerability) are roughly sorted from most common to least common, which is also, fortunately, roughly least dire to most dire. Strategies to deal with the more dire threats at the end of matrix may require subsuming the strategies identified for the less dire circumstances. In those cases, feel free to refer to strategies identified previously (e.g., “see strategies for 2.B. above”) rather than duplicating information.

*Hint:* In most cases, your department’s desktops can be treated as a single item for purposes of this analysis, unless some of them uniquely host a mission-critical function.

*Note:* Do not forget paper-based data when determining which data to protect. Also, paper can serve as a backup for electronically-based data or vice-versa, assuming they are not co-located.

|  |  |  |
| --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Threat, Attack and Vulnerability Scenarios  In priority order, categorize each of the assets identified in Step 1 by threat; most assets are vulnerable to multiple threats. Then identify strategies that your department *currently* follows or *plans to* follow to address these threats. | | |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| 1. System Software | | |
| ***A. Automated or user-initiated network-aware attacks*** (viruses, worms, trojan horses, peer-to-peer)  Consider these assets:   * Destroyed files * Exposed data * Lost productivity * Lost machine control * Lost IT staff time to rebuild machines |  | * Automatic anti-virus software updates and regular scans * Don’t open attachments * Limit use of attachments * Back up frequently * Patch applications, including e-mail clients * Managed desktop services * Configure automatic Operating Systems update and applications update * Departmental patching service * [ITC’s free Windows Patch Management](http://www.itc.virginia.edu/microsys/patchmanagement.html) * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| B. Malicious system misuse  Consider these assets:   * Ownership of shared resources (e.g. Web sites, research data) * Any resource with a password * Exposed data |  | * Effective password policies * Access controls, including access revocation ASAP but no later than one day after transfer or termination * Don’t allow applications to save passwords * Least privilege principal * Configure security settings properly, e.g. disable unused services * Implementation of a more secure network * Enforcing secure access to Internet * Enforcing web application security * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| ***C. Unmanaged (uncontrolled) software installation* (**“unknown” items installed along with intended items; untested or unstable programs that interfere with supported applications)  Consider these assets:   * System reliability * Lost productivity |  | * Policies re testing software before deployment * Standard desktop configurations with limited administrator privileges * Managed desktop services * Servers administration service * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

|  |  |  |
| --- | --- | --- |
| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| 2. Data Integrity, Confidentiality and Availability | | |
| A. Compromise, theft and/or disclosure of databases (due to outsider cyberattack or malicious or accidental insider actions)  Consider these assets:   * Research databases * Grants * Reputation * Reproduction time * Effect on publishing (past, present, future) * Graduate student work * Financial, student, health, social security numbers and/or personnel information |  | * Prevention: see 1.B. above * Periodically compare electronic data to paper (or off-line) data (e.g. backup) * Store data encrypted * Back up frequently * Use encrypted network data transport (SecureCRT, SecureFX, ssh; VPN) * Implementation of a more secure network * Regular staff training on legal requirements and Electronic Storage of Highly Sensitive Data Policy * Follow Electronic Data Removal policy * Regularly scan with Identity Finder to remove non-essential highly sensitive data * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. Data loss  Consider these assets:   * Any resource with electronic data storage |  | * File management practices * Back up frequently * Test backups * Off-site backup, documentation * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 3. Staffing | | |
| A. People critical to support of IT equipment/ services not available (due to illness, weather, etc.)  Consider these assets:   * IT staff |  | * Cross-training * Remote access * Documentation of procedures and practices * Common procedures across departments with partnerships for mutual backfill * Contract for backfill * Escrowed passwords * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| B. Untrained services administrators (system, database, Web, etc.)  Consider these assets:   * Servers * IT staff |  | * Hire appropriately * Provide thorough administrator training * Security training * Provide time for knowledge and skills maintenance * Provide time for on-going systems maintenance * Remote access restrictions * Strict access controls * [Least privilege](http://hissa.ncsl.nist.gov/rbac/paper/node5.html) principal * Back up frequently * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 4. Older and Specialized Hardware and Software | | |
| A. Non-replaceable equipment (no longer manufactured); operating systems no longer supported by vendor  Consider these assets:   * Assets more than 3 years old * Specialty, unique systems |  | * Fund technology migration in coordination with vendors’ product end of life schedule * Interim manual procedures * Contingency plan for parts and emergency migration * Perform frequent, secure and tested backups * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. “Black box” devices (non-upgradeable systems, often with unchangeable passwords)  Consider these assets:   * Specialized devices with Web interfaces (e.g. facilities control modules) * Non-computer “intelligent” devices on network; web-enabled appliances * Engineering devices |  | * Procurement contracts allowing for replacement as needed * Remove device from general network * Contingency plan for parts and emergency migration * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 5. Equipment and/or Service Unavailability | | |
| A. Unavailability of departmental IT equipment/services (due to damage from burst waterpipes, power failure, hard drive failure, confiscation by law enforcement for cybercrime investigation, denial of service attack, need to rebuild OS, human error, theft, etc.) – consider short and long term scenarios  Consider these assets:   * All assets identified in Step 1 |  | * Back up frequently * Test backups * Partnerships with other departments (instead of redundant equipment) * Service contracts * Parts on hand * Off-site backup, documentation * Interim manual procedures * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

| Potential Threat, Attack or Vulnerability | Department’s Identified Assets Affected | Department’s Identified Strategies |
| --- | --- | --- |
| B. Unavailability of central IT equipment/services or voice communication services (due to network failure, equipment failure, denial of service attack, telecom overloads, etc.) – consider short and long term scenarios  Consider these assets:   * All assets identified in Step 1 |  | * Partnerships with other departments * Interim manual procedures * Vendor contracts for services * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 6. Loss of Facilities | | |
| A. Short term – building intact, but no access (due to structural problems, biological or chemical contamination, etc.)  ***B. Long term – building completely or substantially destroyed*** (due to fire, earthquake, missile attack, etc.)  Consider these assets:   * All assets identified in Step 1 * Paper copies of procedures, policies and plans * Local backups * Local software media and licenses * Loss of people |  | * Back up frequently * Test backups * Partnerships with other departments * Redundant equipment * Alternate space plans * Vendor contracts for services * Interim manual procedures * Off-site backup, media, licenses and documentation * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| 7. Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | |
| Consider these assets:   * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  | * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ * \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Prepared by: Technical contact:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

### Step 2.3: Security Plan Development

The ***aim of*** ***risk management*** is “to aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks.” ***Risk mitigation*** is the actions or countermeasures taken to reduce risk.

*Countermeasure Examples*

* Fix known exploitable software flaws
* Enforce operational procedures
* Provide encryption capability
* Improve physical security
* Disconnect unreliable networks
* Train system administrators (*Train everybody!*)

A department must either take specific actions that will mitigate risks to its mission, or reject countermeasure recommendations and accept risks to its mission. Use the template below to document your decisions regarding:

1. Countermeasures you are already taking
2. Countermeasures you will implement going forward
3. Countermeasures you have identified but decided not to implement

In most risk management literature, risk is defined as

R = C x L x V (Risk = Criticality x Likelihood x Vulnerability)

The more critical the asset, the more likely the threat and the greater the vulnerability, the more risk your department faces. So you need to look at your most important assets first (identified in Step 1) and then prioritize your actions by likelihood and severity of the threats, attacks and vulnerabilities you face (identified in Step 2.2): What are the consequences to you if this happens? How can you prepare? How does the cost of preparedness compare to the cost of not acting? Then make decisions based on available resources. If resources are not sufficient, your department has prepared a case for additional resources.

The good news is that your selected strategies will often overlap; regular backup with off-site storage is a near universal strategy for threats to your assets. Also strategies do not necessarily need to be complex. For example:

* To protect all the department’s desktops: have a policy requiring all important documents be saved on the departmental file server; back up the server daily; store the backups off-site; and prepare a departmental software image for quick replacement if a desktop fails.
* To meet legal compliance standards for highly sensitive data: keep highly sensitive data on central systems, and do not download it to local servers or desktops; be in compliance by eliminating the data that would otherwise place you within the jurisdiction of the standards.

|  |  |  |  |
| --- | --- | --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | | |
| Security Plan Template  Strategies (identified in [Step 2.2](#_Step_2.2:_Threat,)) will overlap, protecting multiple assets. Document your current method of protecting assets against identified threats, attacks and vulnerabilities. Identify and prioritize what additional mitigation efforts you need to take (along with a timeline for completing them), and document justifications for mitigation steps you identified but decided not to implement. | | | |
| Asset (by priority) | Identified Threats (by priority) | | Mitigation Strategies (by priority) |
|  |  | | Current:  Planned:  Not implementing: |
|  |  | | Current:  Planned:  Not implementing: |
| Asset (by priority) | Identified Threats (by priority) | | Mitigation Strategies (by priority) |
|  |  | | Current:  Planned:  Not implementing: |
|  |  | | Current:  Planned:  Not implementing: |
| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

## D. Step 3: IT Mission Continuity Planning

In Step 1, your department determined what IT assets are critical to the functioning of your department. In Step 2, you analyzed risks to those assets, and determined how to mitigate those risks or accept them where mitigation was infeasible or unaffordable. Now in Step 3, you will identify short- and long-term plans for continuing to provide your mission-critical functions in the event that the mitigation responses from Step 2 prove insufficient or if an unmitigated risk becomes a reality.

What is the impact of your department being down for hours or days? Do you have a way to restore your systems if they are destroyed? Do you have a manual way of performing critical functions in the meantime?

Should a critical asset be rendered unavailable, continuity planning prepares for the continuation of critical functions, minimizes the negative effects of the problem and protects data from compromise. Concrete deliverables of such planning include backup, off-site storage, recovery plans and interim manual procedures.

In the event of a true disaster, entailing widespread damage to buildings and people, the University would activate its Critical Incident Management Plan (CIMP). However, departments are expected to plan for and coordinate recovery when problems are localized. CIMP requires critical incident planning at the departmental level, the IT component of which is included in this process.

The point of disaster recovery is to have your critical functions up and running as quickly as possible. Interim manual procedures need to be prepared for highly critical processes that need to be performed before full recovery may be possible. Create (or update) a response plan for your department to use in the event that critical IT assets are lost, unavailable, corrupted or disclosed. Below are a series of questions to help you prepare and test this plan.

*Note:* The costs associated with mission continuity preparedness can be significant, and they increase dramatically the more rapid the recovery that is required. Such efforts do benefit from economies of scale, however, allowing larger organizations to put measures in place that would be cost-prohibitive for smaller ones. Having other departments and units host services or servers for your department can pay for itself when continuity preparedness costs are factored in, even in cases where the financial case is marginal based simply on day-to-day operational costs.

|  |  |
| --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| Mission Continuity Questions  The development of a plan for restoration of resources identified in the mission impact analysis and for interim manual processes for continuing critical mission functions during the restoration process. | |
|  | Documentation Location and/or Decision |
| **A. Interim Manual Process Components (aka Downtime Procedures)** | |
| 1. Does the department know how long it could function without department computers, servers, or network access? |  |
| 2. For each mission-critical departmental function, what is the maximum time the department can wait on recovery efforts before proceeding with manual alternatives?  *Note: Some functions may vary in criticality depending on the time of the year. Example: Class registration procedures may have a long recovery window some weeks, but a very short window in other weeks.* |  |
| 3. How does the department proceed manually with mission-critical functions if critical IT assets are lost, unavailable, corrupted, etc.? How long can this be maintained?  Repeat for each identified function. |  |
| 4. In the event of partial damage or disruption, are the department computers standardized so that users could work from another department or University computer without difficulty? Are data necessary to such work stored on a central server or backed up so it can be restored? (See Question B.11. below.) |  |

|  | Documentation Location and/or Decision |
| --- | --- |
| **B. Disaster Recovery Components** |  |
| 1. List the team leader and members of your designated recovery team.  Include name, title, responsibility, e-mail address and telephone number(s) of each member. |  |
| 2. Do you have the necessary University and departmental personnel contact lists?   * Who will decide “this is a mission continuity problem” * Who should be notified in case of a mission continuity problem? * Who will be responsible for responding to a mission continuity problem? * How will you contact them in an emergency situation (pager, cell phone, call lists)? |  |
| 3. Do you have hardware diagrams and system configurations, including physical and data security issues? |  |
| 4. Do you have infrastructure information about your facilities (requirements for power, cooling, network cabling, etc.)? |  |
| 5. Are installations and changes to those critical physical configurations governed by a formal change management process? (This will vary from simple chronological logging of changes to assist in troubleshooting or back out, to a multilevel review involving significant testing for more complex and highly critical systems.) |  |
| 6. Do you have the necessary hardware and software vendor contact lists? |  |
| 7. Do you have a current inventory of your hardware, software and critical data files? Is it updated in real time? |  |
| 8. Does the department securely escrow passwords for accounts that may need to be accessed in the absence of their normal administrator or in an emergency situation? |  |
| 9. Do you have a plan for emergency procurement? (For example, contracts for emergency replacement and a procurement contact list.) |  |
| 10. Do you have recovery plans for each service to be restored (specific, complete, up-to-date)? Do they include a list identifying all system, application and data file systems that must be recovered for each system? |  |
| 11. Are all important data backed up, with secured off-site rotation? (Off-site rotation involves periodically and systematically moving backup media to a physically and environmentally secure facility at a significant distance from the asset being backed up.) |  |
| 12. Is system and recovery information stored off-site in a readily accessible secured location?   * Any documentation referenced above * Data backups * Software media * Software license packs * Any other key information needed for recovery or continuation of essential services |  |
| 13. Do you test your plan annually by at least doing a paper walkthrough? When was the last test? |  |
| 14. Do you update your plan after each test, or when there is a significant technology change? |  |
| 15. What training do you have for staff involved with the plan, including communicating and testing the plan? |  |
| 16. Have departmental personnel received training on what to do and whom to contact within the department and /or University if a computer security or a disaster incident should occur? |  |
| 17. Are recovery and continuing operations instructions written in simple, clear, complete sets of steps that upset, fatigued people could follow correctly? |  |
| Prepared by: Administrative contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Prepared by: Technical contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

Below are simple checklists outlining the key steps in disaster recovery and interim manual procedures. Any plan you develop will need to address at least these issues.

Disaster Recovery Plan Checklist

* Assess damage
* Notify all appropriate University personnel
* Assemble recovery teams
* Provide infrastructure (space, power, cooling, network, etc.)
* Secure needed hardware and supplies
* Return backup information from off-site storage (backup tapes, documentation)
* Install operating systems on restored servers
* Restore applications and institutional data
* Thoroughly test before going on-line

Interim Manual Procedures Checklist

* Identify the procedure
* Identify those with the knowledge, skill and ability to complete the procedure manually
* Determine how long the process can be interrupted before proceeding manually
* Develop detailed documentation on how the procedure will be performed
* Determine how data is reintegrated once the IT-based system is restored

Based on your answers to the Mission Continuity Questions and the steps outlined in the checklists, create (or update) your IT Mission Continuity Plan using the template below.

This template was borrowed and adapted from a model created by HS/CS.

Your department may also take advantage of any general disaster recovery or mission continuity plans you have in place, inserting or integrating IT assets and strategies as appropriate.

|  |  |
| --- | --- |
| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| IT Mission Continuity Plan Template  Based on your answers to the Mission Continuity Questions, replace *the italicized text* below with the appropriate information. | |
| * 1. Mission Continuity Requirements      1. Mission Continuity Plan Overview   *INSERT here your overview of the departmental plan, identifying the systems it includes and the mission impact of their unavailability.*   * + 1. Scope of the Mission Continuity Plan   *INSERT here what your plan covers and does NOT cover.*   * + 1. Mission Continuity Plan Assumptions   *INSERT here any assumptions implicit in the plan—e.g., nature of the service interruption; availability of staff; what backups are available…. This section should identify existing downtime procedures and include the time tolerance during which the procedures may be used by departmental personnel.*   * + 1. Interfaces   *INSERT here a list of any inbound or outbound interfaces to other systems required for the departmental application’s operation.*   * + 1. Escalation Plan   *INSERT here steps taken to evaluate an outage, declare a disaster, and notify departmental and senior management of the event and the decision to invoke this plan.*   * + 1. Decision Timeframes for Plans   *INSERT here the timeframe in which an event is assessed for mission impact; if a disaster is declared, the timeframe in which staff must respond; the timeframe for notifying senior management.*   * + 1. Interim Manual Procedures (aka Downtime Procedures)   *INSERT here references to existing documented procedures to be used during a system outage.*   * 1. Team Structure, Contacts, and Call Lists      1. Team Structure and Tasks   *INSERT here a description of the major activities that must be completed as part of the plan and the departmental teams that must be assembled for their completion; these teams may include people and vendors outside the department and the University.*   * + 1. Emergency Notification Plan/Call Lists   *INSERT here lists of documentation required by the teams to accomplish the plan, including their physical location as both electronic and paper documents; contact information for all team members, including office, home, and pager telephone numbers.*   * + 1. Vendor Contact List   *INSERT here contact information (names, phone, email, Postal Service, web sites, etc.) for each vendor that may require contact during a mission continuity event. Include in an appendix a description of all software and hardware products with version and, if applicable, server/CPU serial information.*   * + 1. Assembly & Command Centers   *INSERT here designation and description of locations to which staff should report in the event of a disaster or a required evacuation of a building housing departmental equipment subject to recovery; alternate sites should be included; these will be focal points for mission continuity activities when a disaster is declared.*   * + 1. Recovery Site(s)   *INSERT here detailed information describing any alternate sites at which computer equipment will be located for recovery purposes; if these locations are provided by an organization outside the department, notification procedures should be included.*   * 1. Backup Procedures      1. Backup Procedures   *INSERT here detailed description of tools/products used to regularly back up departmental software and data; location of any off-site tape libraries or tape storage; backup schedules; reference to any backup tasks performed by any other entity on behalf of the department.*   * + 1. OS/Application Backup/Recovery Procedures   *INSERT here step-by-step actions to be taken to recover operating system, application software, and departmental system data using the tools/products outlined in the previous section; this should contain enough detail so that a knowledgeable person unfamiliar with the daily backups could complete the recovery.*   * + 1. Hardware/System Software Plan Overview   *INSERT here describes the computer hardware and operating system software necessary to restore a departmental system in the event of a disaster; includes procedures and controls to assure efficient and timely restoration at an alternate site; appendices may be used to list existing hardware and software and to detail what is available or required at an alternate site.*   * + 1. Operating Systems/Other Software   *INSERT here technical references to required OS and application software that will be restored; these should include both electronic and paper copy references as well as material available at vendor web sites.*   * + 1. Data Communications Plan   *INSERT here detailed requirements for alternative network connections that must be established in the event of a disaster; if common carrier connections are required, these should be detailed and contracted for in advance; departments should work with the University network team to detail and diagram any alternative network connections required.*   * 1. Recovery Procedures      1. Hardware/Software Recovery Overview   *INSERT here an overview of the general steps to be taken to restore a departmental application’s operation; in general, this would include hardware configuration, OS reinstallation and initialization, application reinstallation, restoring data, and application operability.*   * + 1. System Recovery Procedures   *INSERT here step-by-step actions to be taken to recover the hardware and operating system; this should contain enough detail so that a person with only general knowledge of the OS could complete the recovery.*   * + 1. System Initialization Procedures   *INSERT here step-by-step actions to be taken to initialize the operating system; this should contain enough detail so that a person with only general knowledge of the OS could complete the initialization.*   * + 1. Storage Restore List   *INSERT here a list (or references to auxiliary documentation) identifying all system, application and data file systems that must be recovered for each system included in the plan.*   * + 1. Applications Recovery   *INSERT here step-by-step actions to be taken to restore the departmental application; this should contain enough detail so that a person with only general knowledge of the application could restore it.*   * 1. Implementation Plan      1. Types of Recovery Tasks   *INSERT here definitions of task types to be accomplished by the recovery teams; examples are recovery (hardware, OS, application) and support (security, transportation, procurement, etc.).*   * + 1. Recovery Team Tasks   *INSERT here a detailed listing of all recovery tasks needed to fully restore the departmental application of operability on an alternate (or redundant) computer platform. Each task should include:*   1. *an estimated start time after a disaster occurs;* 2. *estimated time to complete the task;* 3. *identification of the team responsible for the task;* 4. *predecessor tasks that must be completed before each task is started;* 5. *a description of the task.*   *Step-by-step instructions for completing each task are contained in previous section of the plan.*   * 1. Mission Continuity Plan Testing      1. Mission Continuity Plan Test Objective   *INSERT here departmental disaster plans should be periodically tested. This section defines testing objectives and frequency.*   * + 1. Plan Test Requirements and Methodology   *INSERT here testing may be accomplished in many ways (paper walk-throughs, scheduled tests, unannounced tests, tactical exercise, etc.). This section defines the plan testing requirements determined to meet the department’s needs to insure plan success.*   * 1. Mission Continuity Plan Maintenance      1. Plan Maintenance Objectives   *INSERT here any disaster plan must be maintained. This section specifies departmental objectives for keeping the plan current and maintaining staff awareness of it.*   * + 1. Mission Continuity Plan Maintenance   *INSERT here maintenance of the plan will be required on a scheduled basis (periodic reviews to detect the need for plan changes) and on an unscheduled basis (due to events—an OS upgrade, an application upgrade, a network change, etc.). Periodic reviews should include verifying that recovery hardware capacity is sufficient to meet increasing application transaction processing volume.*   * + 1. Interdepartmental Relationships   *INSERT here any required relationships with other departments necessary for the successful completion of a mission continuity plan should be included here. Examples include HS/CS or ITC, Procurement (Material Support Services in the Health System), Legal, and University Relations (Media Relations in the Health System).*   * + 1. Mission Impact Analysis (MIA)   *INSERT here departments should periodically perform a Mission Impact Analysis on their operation of the effect of a departmental application failure. This section should contain a summary of the most recent MIA the department has conducted.*   * 1. Relocation Plan      1. Returning to Normal Operations   *INSERT here factors affecting a return to normal operations should be included here if temporary relocation to a Hot/Cold Site is part of the recovery plan.*   * 1. Appendices      1. Appendix A: Call Lists/Contact Information      2. Appendix B: Equipment Inventory      3. Appendix C: Software Inventory      4. Appendix D: Network Diagrams      5. Appendix E: Mission Continuity Contracts | |
| Prepared by:  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## E. Step 4: Evaluation and Reassessment

In Steps 1-3 you defined your mission-critical IT assets, developed a plan to protect them against threats and vulnerabilities and provided contingencies to fall back on in cases where the protection proved inadequate. Given the rapidly changing nature of IT and IT risks, Step 4 requires regular evaluation and reassessment of the work accomplished in Steps 1-3.

Remember, Risk Management is never a completed process: after an assessment, you create a security plan, the implementation of which will take time, from highest priority to lowest, as criticality and resources allow. By the time that plan is fulfilled, changes will have occurred in your environment requiring reassessment, although that process should get easier with each reiteration as you are working on an ever stronger security foundation.

University policy may require reassessment of your department’s risk management at least every two or three years, but that process really needs to occur whenever the technology of your identified critical assets changes, or you complete your security plan. In particular, a reassessment is critical if the changes in your department affect the larger University community and/or dependent external entities.

Below are a series of questions to help you complete your evaluation and reassessment.

* Repeat Steps 1-3 every two or three years or when there are significant changes to departmental IT assets or risk environment
* Review the success of your prior analysis, testing and any responses made, whether they were corrective, preventative or post-incident
* Incorporate responses to any intervening changes (new operating system, critical applications or data, or state or federal standards)

| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| --- | --- |
| Evaluation and Reassessment Questions  Complete every three years or when there are significant changes to departmental IT assets or risk environment (see [Table 1](#_Table_1:_Critical): Critical Asset Criteria). The process gets easier because you are building on your earlier effort. All questions refer to the time period since the last evaluation. | |
| **A. Evaluation** | |
| 1. Have you adequately protected what your analysis said you should? |  |
| 2. Has there been any loss, unavailability, corruption or inappropriate disclosure of critical IT assets or data? If so, how effective was the response? |  |
| **B. Reassessment** | |
| 1. Have you changed your operating system?  *Examples:* Windows to UNIX/Linux, Windows XP to Windows 7, Mac OS to Windows |  |
| 2. Have you changed any critical applications?  Example: Migrated database from Access to SQL Server. |  |
| 3. Are there any new critical data housed in your department?  *Note:* Data may be critical based on mission criticality, sensitivity or protected status. |  |
| 4. Are there any new national or international standards or University policies or standards applicable to your department? If so, to which systems and/or data do they apply? |  |
| 5. What risk mitigation that you could not afford previously can you now afford, or – due to increased risk in that area – you can no longer afford not to mitigate? |  |
| 6. Are there any new technologies allowing for easier and/or cheaper mitigation for certain risks? |  |
| 7. Has there been an increase or decrease in the number of servers (physical and virtual) or systems? |  |
| 8. What interim risk mitigation measures have been put in place for new systems? |  |
| 9. Are there any systems that are no longer mission-critical? If so, are there risk mitigation efforts that can be discontinued? |  |
| 10. What functions have been moved to central servers, so that you no longer have risk management responsibility for them? |  |
| 11. What functions have been moved to local servers, so that you now have risk management responsibility for them? |  |
| 12. What new functions has your department taken on in pursuit of its mission? Are any IT-asset-dependent? |  |
| 13. What old functions have become IT-asset-dependent? |  |
| 14. What relevant personnel turnover, additions or subtractions, or role changes have occurred? |  |
| 15. Do you have any long-term backups (archives) that need to be refreshed on new media (or destroyed)? (Please review and follow Records Management guidance regarding retention and disposition of records.) |  |
| Prepared by: Administrative contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Prepared by: Technical contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

## Terminology

### Source of Terminology

All of the definitions and most of the examples below are appropriated from a National Security Agency (NSA) curriculum used by the National Colloquium for Information System Security Education (NCISSE).[[1]](#footnote-1) Comments and additions are indicated below in brackets.

### Definitions

**Security Management:** Managing the risks to a department’s mission

[A focus on departmental mission is vital; departments cannot mitigate every risk, but must prioritize based on the threat to their mission and available resources.]

**Risk:**

**Management:** (New World Dictionary of the American Language)

* The art or manner of *controlling* the movement or behavior of something
* To have charge of; direct; conduct; administer

**Risk Management:** “The total process to identify, control, and manage the impact of uncertain harmful events, commensurate with the value of the protected assets.” (National Information Systems Security Glossary, NSTISSI No. 4009 and AFR 205-16, AFR 700-10)

**Risk Management (Simply Put):** Determine what your risks are and then decide on a course of action to deal with those risks.

[More colloquially: “What’s your threshold for pain?” or “Do you want this to show up on the front page of the *Daily Progress*?”]

**Aim of Risk Management:** To aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks

**Critical Asset:** Something that when disclosed, modified, destroyed, or misused will cause harmful consequences to the department or its – or the University’s – goals and mission, or will provide an undesired and unintended benefit to someone

*Examples*: Information, people, software, hardware, facilities, etc.

**Risk Assessment:** A study of threats and vulnerabilities, the design effectiveness of present security mechanisms, and the potential impact of these factors on a department’s ability to perform its mission

**Threat:** The capabilities and intentions of adversaries to exploit an information system; or any natural or unintentional event with the potential to cause harm to an information system, resulting in a degradation of a department’s ability to fully perform its mission

*Examples*: adversarial (terrorists, foreign states, disgruntled employees, criminals, recreational hackers, commercial competitors) and non-adversarial (nature, unintentional human acts)

**Attack:** A well-defined set of actions by the threat (an active agent) that, if successful, would damage a critical asset – cause an undesirable state of affairs – resulting in harm to a department’s ability to perform its mission

[An attack is an *action*; a vulnerability is an *opportunity*.]

**Vulnerability:** A characteristic of an information system or its components that could be exploited by an adversary, or harmed by a natural act or an act unintentionally caused by human activity

*Examples*: Inadequate password management, easy access to a facility, weak cryptography, a software flaw, an open port

[Or a facility housing the asset that is subject to fire or flood.]

**Consequence:** The harmful result of a successful attack, degrading a department’s ability to perform its mission

*Examples of consequences to a department’s mission*

* Loss of information confidentiality
* Loss of information integrity
* Loss of availability of information or system functions [natural disaster]
* Inability to correctly authenticate sender of information [forged log-ins, redirected transactions]
* Inability to verify receipt of information by the *intended* recipient [credit card connections]

**Risk Mitigation:** Actions or countermeasures we can take to lessen risk

* Affect threat agent or their capabilities
* Eliminate or limit our vulnerabilities

*Countermeasure Examples*

* Fix known exploitable software flaws
* Enforce operational procedures
* Provide encryption capability
* Improve physical security
* Disconnect unreliable networks
* Train system administrators [*Train everybody!*]
* Install virus scanning software

**Risk Management Decision:** Determination by administration to

* Take specific actions that will mitigate risk to mission, or
* Reject countermeasure recommendations and accept risk to mission

**Residual Risk:** That portion of risk that remains

* Management decides to accept risk
* Unconsidered threat factors
* Unconsidered vulnerabilities
* Incorrect conclusions

**Goal for the department:** Defining and institutionalizing risk management

* Define the process
* Get management support
* Educate the workforce
* Practice risk management

1. The terminology lesson on which this document is based was available within a larger set of resources at <<http://www.infosec.jmu.edu/ncisse/conference99/website/>> (“NSA Courseware”) as of August 2004 but is no longer available. NCISSE has subsequently rebranded as CISSE <<http://www.cisse.info/>>. [↑](#footnote-ref-1)