University of Virginia Information Technology Security Risk Management (ITS-RM) Program

Version 3.0

Revised 08/03/10

Contact: its-rm@virginia.edu
http://www.itc.virginia.edu/security/riskmanagement/

Contents

I. Executive Support and Policy Statement ***1***
II. Background Information ***2***

A. Why Security is Important **2**

B. What's a Risk Management Program? Why It's a Best Practice **3**

C. U.Va.'s IT Security Risk Management Program **3**

D. Responsibilities **5**
Expectations for Departments 6

E. Terminology **7**
III. Risk Management Instructions and Templates ***8***

A. Process Overview **8**
Chart 1: IT Security Risk Management Process Flow 9

B. Step 1: IT Mission Impact Analysis **10**
Table 1: Critical Asset Criteria 10

C. Step 2: IT Risk Assessment **15**
Step 2.1: Risk Assessment Questions 15
Step 2.2: Threat, Attack and Vulnerability Scenarios 39
Step 2.3: Security Plan Development 48

D. Step 3: IT Mission Continuity Planning **52**

E. Step 4: Evaluation and Reassessment **63**

F. Reporting Requirements **67**
IV. Appendices ***68***

Appendix A: Sample Responses **69**

Appendix B: Systems and Services Supported by ITC **70**

Appendix C: Systems Supported by the Health System **71**

Appendix D: Does HIPAA Apply to Our Department? **73**

Appendix E: Does Gramm-Leach-Bliley Apply to Our Department? **75**

Appendix F: Does FERPA Apply to Our Department? **76**

Appendix G: What is Highly Sensitive Data? **77**

Appendix H: Related Policies and Resources **78**

Appendix I: Terminology **79**
Source of Terminology 79
Definitions 79

This is version 3.0 of the University of Virginia Information Technology Security Risk Management (ITS-RM) Program materials.

I. Executive Support and Policy Statement

Given the serious security risks to information technology (IT) assets, managing those risks effectively is an essential task for the University and its departments. The process is one that will benefit both the individual department and the University as a whole. Completing such a risk management process is extremely important in today's advanced technological world. It is important that both management and staff understand what risks exist in their IT environment and how those risks can be reduced or even eliminated.

Like fire insurance, Information Technology Security Risk Management (ITS-RM) is a form of protection that the University simply can't afford not to have. The University has business processes, research and instructional efforts, and highly sensitive data that the institution cannot afford to lose or have exposed that depend on IT assets. Unfortunately, these IT assets are subject to an increasing number of threats, attacks and vulnerabilities against which more protection is continually required. The ITS-RM program is an essential component in this overall effort.

The University's policy on ITS-RM requires the management of each department to complete the process outlined in the ITS-RM Program at least once every three years, when there are significant changes to departmental IT assets, or when there are significant changes to the risk environment. The department head will sign off on the deliverables from this process and file these deliverables in the University's central repository for these documents. The ITS-RM program applies to agencies 207 (Academic Division), 209 (Medical Center) and 246 (College at Wise). (See section III. F. for complete reporting requirements.)

II. Background Information

A. Why Security is Important

The U.Va. Information Technology Security Risk Management program is intended to provide University departments with the information and tools they need to properly manage the security risks associated with their information technology assets.

Why is managing IT security risks important?

First, the financial consequences of failing to do so can be significant.

- The University and its units must protect the heavy investments they have made in IT and personnel that support technology.
- Given the increasing reliance on IT to provide mission-critical academic, instructional and administrative functions, loss or interruption of IT-based functions is not merely an inconvenience but could lead to the inability of a unit to perform its core mission.

Second, the threats to IT assets are only getting worse.

- The invaluable, fast, direct connection to the Internet at U.Va. makes us both a direct target and a tempting source of hijacked bandwidth.
- IT security efforts are required at all network levels, meaning that responsibility for security is highly distributed, and therefore difficult to manage.
- More sophisticated and dangerous exploits and attacks are released almost daily, via viruses and worms, intentional compromises that threaten the privacy and integrity of highly sensitive data, and denial of network service.
- The potential for terrorist attacks or natural disasters to strike exists.

Fire. The University's Treasurer's Office is left with burned files and melted computers.

Flood. Health System Computing Services responds to a report of a down server and finds water rushing from the ceiling.

Loss of access. University Hall is closed for several months on 15-minutes' notice after failing a routine structural safety inspection.

Cyber-attack. Machines containing sensitive data are hijacked via the network.

This is just a selection of actual events that have occurred at the University. How prepared is your department to mitigate the risks of these types of occurrences and respond appropriately should they strike?

- Will your department have the money to deal with any clean up, including the replacement of expensive hardware?
- How will your department respond to the legal and public relations consequences if private data is released or your devices are commandeered and used to attack other people's machines?
- What are the financial consequences if research is delayed (or destroyed) or if other mission-critical functions are interrupted?

B. What's a Risk Management Program? Why It's a Best Practice

Given the serious security risks to IT assets outlined above, managing those risks effectively is an essential task for the University and its departments.[1] ***Risk management*** has been defined formally as "*The total process to identify, control, and manage the impact of uncertain harmful events, commensurate with the value of the protected assets*."[2] More simply put: "Determine what your risks are and then decide on a course of action to deal with those risks." Even more colloquially: What's your department's threshold for pain? Do you want failure to deal with a particular risk to end up on the front page of *The Daily Progress* or *Washington Post*?

Why do the work of identifying your mission-critical IT assets, analyzing the associated security risks and developing both security and mission continuity plans? Who will it benefit? The process is one that will benefit both the individual department and the University as a whole. It is important that departments and their IT users understand what risks exist in their IT environment and how those risks can be reduced or even eliminated.[3] 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*." It is both prudent practice and, in many cases, a legal necessity.

C. U.Va.'s IT Security Risk Management Program

A design team composed of members from throughout the University has identified some common risks and put together a process and templates for departments to use in their risk management effort. Individual departments are encouraged to review those common risks to see which might apply to their specific environment. They should then review

---

[1] Throughout this document, the term "department" is used generically to refer to any organizational unit with some level of autonomy within the University, including schools, departments, centers, units, etc.

[2] National Information Systems Security Glossary, NSTISSI No. 4009 and AFR 205-16, AFR 700-10. Unless otherwise noted, all definitions in quotation marks are appropriated from a National Security Agency (NSA) curriculum used by the National Colloquium for Information System Security Education (NCISSE). See Appendix I for definitions of key terms and a full reference to the original sources.

[3] Much of this paragraph is adapted from "Introduction to the Business Impact Analysis/Risk Assessment Process," <http://www.security.vt.edu/Downloads/riskanalysis/Star-Risk Assessment.pdf>.

their own surroundings to determine what specific risks exist for inclusion into the process.

The University maintains a University-wide IT Security Risk Management Program for:

1. IT Mission Impact Analysis – The identification of information, computing hardware and software, and associated personnel that require protection against unavailability, unauthorized access, modification, disclosure or other security breaches.

2. IT Risk Assessment – The determination and evaluation of threats to the resources identified through a mission impact analysis.

3. IT Mission Continuity Planning – 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.

4. Evaluation and Reassessment – The reiteration of these steps at least every three years, or when there are significant changes to departmental IT assets or risk environment.

Why is such a program needed?

- Mission impact analysis, risk assessment, and mission continuity planning are not one-time projects, but rather tactical operational processes that incorporate the most current thinking on security threats and appropriate safeguards.

- The University needs proactive mechanisms for tracking the frequency with which assessments and plans are updated and for assuring quality and consistency as they are developed.

- The University needs a central repository for safeguarding assessment and planning documents.

- The University needs the assurance that available resources for IT security across the organization are being focused on the most important needs; resources are limited, so they should be targeted as efficiently as possible.

- Several internal University policies and standards can be addressed through ITS-RM. Approximately twelve percent of the questions on the Internal Controls Questionnaire concern issues addressed by this program,[4] including completion of an IT risk analysis and departmental security plan. In addition, the University's Critical Incident Management Plan (CIMP) requires departmental planning to

[4] As of this date, questions 1.4, 1.5, 1.6, 1.7, 1.18, 2.11, 2,14, 2.15, 9.2, 9.7, 9.8 9.9 and 11.9.

protect departmental assets, with specific reference to IT assets and IT security measures. Moreover, the ITS-RM helps a department maintain compliance with the University's information policies on

  - Protection and Use of Social Security Numbers
  - Electronic Storage of Highly Sensitive Data
  - Electronic Data Removal
  - Administrative Data Access and the related Institutional Data Protection Standards (IDPS)
  - Records Retention and Disposition

- A risk management program helps the University comply with various external IT security standards that may apply to individual departments, including
  - HIPAA (Health Insurance Portability and Accountability Act)
  - HITECH (Health Information Technology for Economic and Clinical Health) Act
  - FERPA (Family Educational Rights and Privacy Act)
  - GLBA (Gramm-Leach-Bliley Act, common title of the Financial Services Modernization Act (FSMA))
  - NIST (National Institute of Standards and Technology)
  - PCI (Payment Card Industry), and
  - the University Information Technology Security Program required by the Commonwealth of Virginia Restructured Higher Education Financial and Administrative Operations Act of 2005

D. Responsibilities

U.Va. has a highly complex and resource rich computing environment, without which the University simply could not accomplish its mission. The management structure for this environment is necessarily complex as well. While the central IT organization manages the network infrastructure and other enterprise-wide computing services, there are many servers, desktops and databases managed by various departments and research projects. Additionally, the University's hospital has its own central computing center.

The Assistant Vice President for Information Security Policy, and Records, who reports to the University's Vice President & Chief Information Officer (VP/CIO), has, among other functions, the responsibility for coordinating security activities at the University. Medical Center-specific security is handled by Health System Computing Services (HS/CS). U.Va.'s College at Wise also has an IT Security Office. Various divisions within the Information Technology and Communication (ITC) Department, also reporting to the VP/CIO, implement and support security-related infrastructure and provide security-related services. Personnel in individual departments are responsible for assessing risks and choosing and implementing appropriate safeguards to mitigate unacceptable risks to departmental IT assets, i.e. those not centrally managed by ITC. (See Appendix B: Systems and Services Supported by ITC for a list of centrally managed services; note; ITC provided server space is often jointly managed between departments

and ITC, with each retaining some level of responsibility.) Individual departments are also responsible for the security of data records not in electronic form.

The Information Security, Policy, and Records Office (ISPRO) assumed primary responsibility for ITS-RM program design and implementation supported by HS/CS, Internal Audit, Risk Management, U.Va. Police and the University Development Office. ISPRO and HS/CS, where appropriate, will provide ongoing support. Ongoing support will include compilation of completed assessments and plans into a repository, consulting and guidance where appropriate, and monitoring compliance and progress with the overall program.

Input from the Internal Audit Department was essential to the design and implementation planning processes. It is not expected the program would in any way alter the need for review of security plans during routine department audits. In fact, several of the ITS-RM program templates employ questions used by Audit for that purpose.

Because risk assessment and mission continuity planning are included in the security standards for HIPAA, the HIPAA Initiative Office and HS/CS have participated in design and implementation to avoid duplication of effort and inconsistency in approach.

Although the program includes instructions, templates and guidance, the department needs to own the risk management process. Departments have to do the work of risk management: only they know their mission, what assets are critical to that mission, how to prioritize resources to address those assets and how best to get back up and functioning following a disaster (big or small).

If your department has one fileserver that is well-configured and professionally maintained (with regular backups with off-site rotation), uses central services (which someone else is responsible for protecting) for everything else and hosts no highly sensitive data, this process is easy. Of course, if you have a dozen servers, including e-mail, multiple research projects and sensitive data, the process will require more work.

Expectations for Departments

- Departments are expected to complete this process and return a report to the University's central repository for these documents according to the policy timeline.
- After initial completion of the required analysis and planning, additional follow up may be necessary to address key issues.
- Both administrative/business and technical leaders from the department must be involved in the process.
- The department head will sign off on the completed report.

Reporting requirements are fully explained in section III.F. below.

Any department that has questions concerning the process should contact ISPRO:

IT Security <its-rm@virginia.edu>
Messenger mail: ISPRO, P.O. Box 400898
http://www.itc.virginia.edu/security/riskmanagement/

This office is available to assist departments in understanding the process and getting started on completing their report. Each department should send their completed reports (as well as updates) to this office so that a central repository can be maintained.

E. Terminology

Adoption of a reference for terminology associated with this program ensures that all the participants have a common understanding. This is important as we seek to educate departmental leaders about risk management issues and elicit responses from them that are both appropriate for a specific department and comparable across departments. Please see Appendix I.

III. Risk Management Instructions and Templates

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, state and federal 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

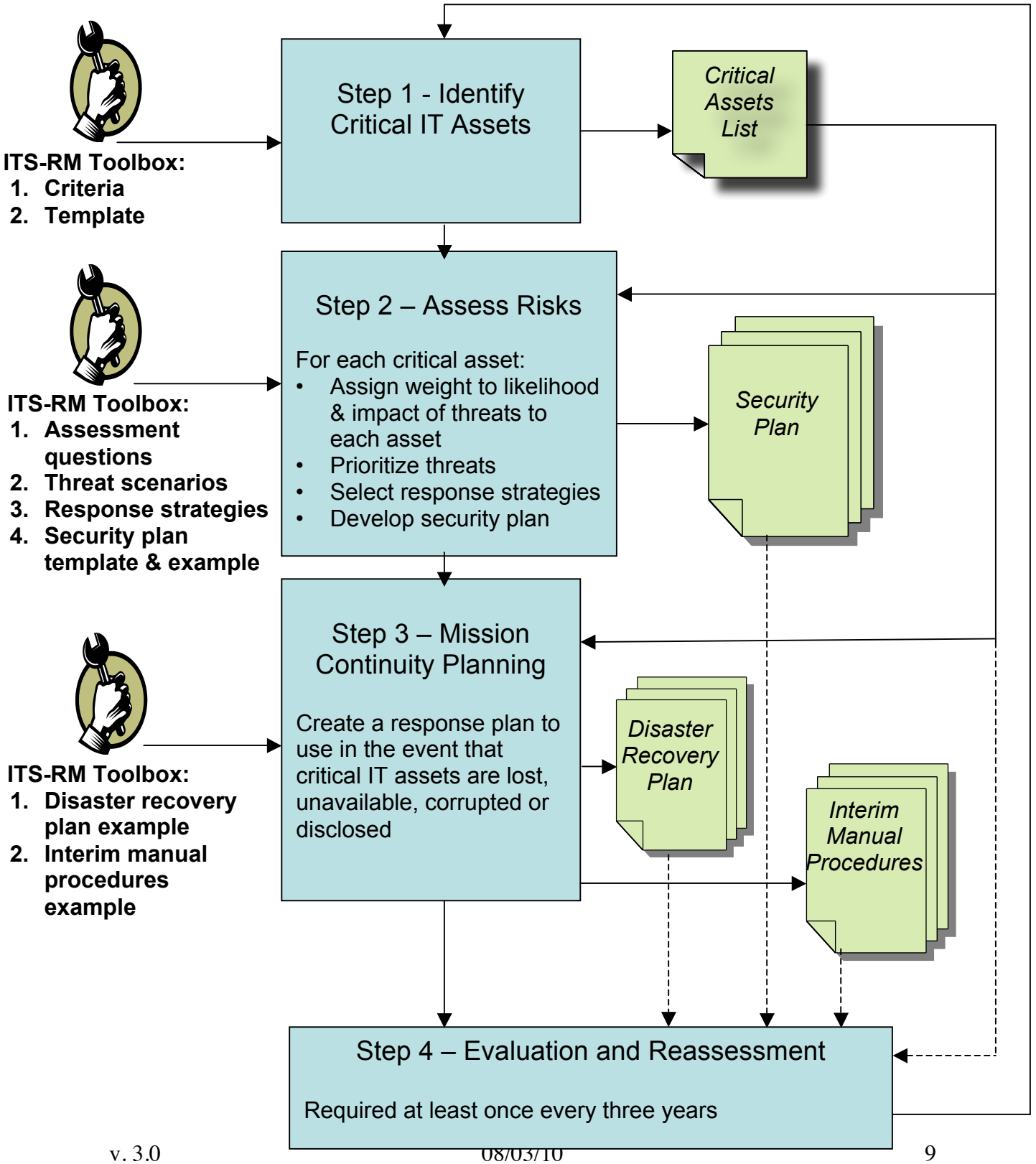
Step 4: Evaluation and Reassessment

- 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. below for the reporting requirements of this process, and see Appendix A 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



Make liberal use of copy/paste as you move from step to step, and utilize any previous work your department has done in security planning and disaster recovery, including previous iterations of your department's ITS-RM documents (which should be used as a starting point for this iteration). This process should build on what you have already done rather than causing you to redo work.

Additional resources for departmental managers regarding IT security are available at <http://www.itc.virginia.edu/security/manager.html>.

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*** when its disclosure, modification, destruction, or misuse will cause harmful ***consequences*** 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 1: Critical Asset Criteria
The asset is required to perform functions that result in life or death to University community members or the general public.
The asset is required to perform functions that provide public safety and other social services to University community members or the general public.
The asset is required to support local, state or national Homeland Security efforts.
The asset is required to support patient care services.
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 is required to support a vice-presidentially designated critical function area.
The asset concerns data which is highly sensitive or in other ways access restricted.
The asset is required to perform state or federally regulated functions.
The asset is required to perform other functions essential to a department's mission.

As you can see from Table 1, for purposes of this process the definition of "critical" goes well beyond the medical sense of "life and death." Based on your mission, what functions do you perform with safety or legal ramifications? What do you do that is important to the University as a whole or to other departments? What's important for your department to get its job done? What unanticipated failure don't you want to end up on a vice-president's desk?

The process of mission impact analysis requires the input of both the administrative leaders and information technology experts in each department. It is important to understand, for example, that a mission-critical departmental function may depend on multiple IT assets, or that a single IT asset may be critical to multiple departmental functions. IT personnel and administrators have both been known to underestimate the complexity and misunderstand the nature of the other's function.

Below is the template for doing a Mission Impact Analysis. (A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.) Determine your department's critical assets (hardware, software, information and people) based on Table 1 above and your department's mission. (Information on centrally-supported assets is available in Appendices B and C.)

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, protected health information, 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*	
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 U.Va. 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 U.Va. 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 U.Va. 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 •*Health-related*: sensitive patient data, both clinical and research •External data provider	
6. Provide a complete location inventory of all data of the following types used or stored in the department, whether in paper or electronic form: • Social Security Numbers (SSNs) • Health Insurance Portability & Accountability Act (HIPAA) or Health Information Technology for Economic and Clinical Health (HITECH) Act protected health information (PHI) • Family Educational Rights and Privacy Act (FERPA) protected student data • Gramm-Leach-Bliley Act (GLBA) protected financial data • Payment Card Industry (PCI) data, including credit card numbers and transaction information • Passport numbers	

<table>
<tr><td>

- Any other highly sensitive or legally protected data

Other examples of legally protected data may include data related to patents, contracts, and national security.

</td><td></td></tr>
<tr><td>

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 U.Va. 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

</td><td></td></tr>
<tr><td>

Prepared by: Administrative contact

Name: _____
Signature: _____
Title: _____
Date: _____

</td><td>

Prepared by: Technical contact

Name: _____
Signature: _____
Title: _____
Date: _____

</td></tr>
<tr><td colspan="2">

Approved by: Unit head

Name: _____ Signature: _____
Title: _____ Date: _____

</td></tr>
</table>

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*** *(with paths determined by applicability of laws)*

- Assess departmental security practices against University, state and federal standards

2.2 ***Threat, attack and vulnerability scenarios*** *(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*** *(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

Below are four sets of questions to help you assess risk and associated security practices in your department: a general risk assessment, a HIPAA supplement (also useful for HITECH compliance), a GLBA supplement and a FERPA supplement. For each question set the template asks you: 1) to indicate whether your department is currently following the identified practice, and 2) to record the location of compliance documentation or an explanation of why a practice is not followed.

Note:

Certain standards may require special diligence on your department's part. See Appendices D, E and F to determine if HIPAA/HITECH, GLBA or FERPA

> legislation applies to your department. A requirement for departmental compliance with these laws will affect decision points in the question sets below. Your department should answer the general question set, as well as all supplemental sets that cover types of data that you house. Likewise, the use of highly sensitive data requires adherence to a more stringent set of security standards under the University's Institutional Data Protection Standards.

The general risk assessment questions (as well as some of the IT mission continuity questions in the next section) come from several sources: 1) an Internal Audit questionnaire that was adapted from an earlier ITC Department Computer Security Self-Assessment Checklist; 2) questions developed independently by HS/CS, 3) questions developed by the Virginia Alliance for Secure Computing and Networking; 3) questions regarding compliance with the University's IDPS; and 4) other questions identified during ITS-RM design and implementation planning that seemed prudent to include. These were edited and adapted where appropriate.

The HIPAA/HITECH-related questions come from HS/CS.

The GLBA-related questions are adapted from "Financial Institutions and Customer Data: Complying with the Safeguards Rule," Federal Trade Commission, September 2002. The FERPA-related questions are also adapted from the FTC document, which outlines best practices in securing protected data. Additional questions appropriate to the University environment were added.

If any of these question sets do not apply to your department, please skip down to the next set.

(A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.)

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)? See FM key policy.			
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?			

	Yes	No	Documentation location or explanation for not following
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. *Note:* No justification is possible for highly sensitive data on shared accounts.			
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? (See Responsible Computing Handbook and Electronic Access Agreement.)			
9. Does the department assist users in selecting passwords that will ensure privacy while promoting regular use? (See ITC guidelines and/or HS/CS guidelines.)			
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? (A short overview of and rationale for password escrow is available here.)			
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?			

	Yes	No	Documentation location or explanation for not following
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? (The U.Va. Audit Department suggests locking out a user after three unsuccessful log-in attempts.)			
17. Does the department prohibit modems attached to servers and desktops that can receive calls?			
C. Virus Protection			
1. Is Symantec (Norton) or other 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 remind users to scan regularly for viruses in addition to updating?			
4. If a computer becomes infected with a computer virus, do users know to follow the IT Security Incident Reporting policy?			
5. 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?			

	Yes	No	Documentation location or explanation for not following
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, including ImageNow?			
E. Operating Systems			
1. Are only ITC and/or HS/CS-supported 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 ITC 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?			

	Yes	No	Documentation location or explanation for not following
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)?			
2. Have faculty and staff been instructed to place on-line orders only through secure Web sites?			
3. If employees are allowed to install U.Va. and/or HS/CS licensed software at home, is it installed in compliance with the license, 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, a) are all data and software removed from hardware and electronic media prior to transfer within U.Va., and b) are all hardware and media processed through Procurement's designated vendor when leaving U.Va.? 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?			

	Yes	No	Documentation location or explanation for not following
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?			

	Yes	No	Documentation location or explanation for not following
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?			
25. If the department accepts credit cards (over the web or through a point-of-sale terminal), are all credit card numbers collected, stored, protected and destroyed in accordance with the University's PCI-compliant Credit Card Requirements?			

	Yes	No	Documentation location or explanation for not following
26. Have you returned your SSN Inventory and Remediation Status Report, indicating that you have completed your remediation plan?			
27. Do you understand and acknowledge the on-going responsibilities you have regarding the use and protection of SSNs as outlined in the Protection & Use of Social Security Numbers policy, Institutional Data Protection Standards, Electronic Storage of Highly Sensitive Data policy, and Guidance on Social Security Number Redaction and Records Management?			
28. Do you submit a Request for Approval to Use Social Security Numbers and receive approval before using SSNs for any new purpose?			
29. Do you regularly review the necessity of, and seek to reduce, any continued use of SSNs?			
30. Do you periodically scan computing devices with Identity Finder or similar software to ensure that SSNs have not reappeared; delete any newly found instances and determine how to prevent future recurrences?			
31. As required by state law, do you promptly destroy records containing SSNs *within six (6) months of their completed retention period* by following the procedures established by the University Records Officer?			
H. Security Awareness and Education			
1. Are faculty and staff aware of their responsibility for computer security according to the Responsible Computing Handbook?			
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?			

	Yes	No	Documentation location or explanation for not following
4. Have University and/or Medical Center and department-specific security policies and procedures been documented and shared with all faculty and staff?			
5. Are faculty and staff keeping current on University and/or HS/CS 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 LSPs 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 ITC cyber security awareness classes?			
11. Do all departmental staff take the Information Technology Security Awareness 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?			

	Yes	No	Documentation location or explanation for not following
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:	Approved by: Unit head
Name: _____	Name: _____
Signature: _____	Signature: _____
Title: _____	Title: _____
Date: _____	Date: _____

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: HIPAA Supplement

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.

In addition to the issues covered in the general questions, additional HIPAA issues focus on the need for documenting each policy and process, knowledge and training on compliance regulations, facility access controls, workstation use and location and the review of logs and other auditing measures.

Note: The HITECH Act extended the reach of HIPAA. See Appendix D for additional details.

Note: As HIPAA data is defined as highly sensitive data, in addition to the HIPAA specific requirements below, all HIPAA data must be protected as required by the Electronic Storage of Highly Sensitive Data policy and the Institutional Data Protection Standards for highly sensitive data.

	Yes	No	Documentation location or explanation for not following
A. Documentation			
1. Does your organization have complete and current formal documentation instructions for reporting security breaches including both report procedures and response procedures entity-wide? Do they include formal written mechanisms to document security incidents?			
2. Are documented formal procedures that establish and maintain personnel security in place and current?			
3. Does the organization maintain a record of the transport, movement, and location of hardware, software, and electronic media?			
4. Do you retain for at least six years after their last effective date all compliance planning records along with decisions and justifications?			

	Yes	No	Documentation location or explanation for not following
5. Have access control policy and procedures been implemented which formally document authorization, establishment, and modification of system accounts which access protected healthcare information (PHI)? Do they include: • Access-establishment information use policies and rules to determine initial right of access to a terminal, transaction, program, process or transfer to some other user? • Access-modification information policies and rules to determine the types of and reasons for modification to established right of access to a terminal, transaction, program, process or transfer to some other user? • Access authorization records? (Access authorization could be recorded as part of a job description or other policy for the end user that details level of access in accordance with job function.) • Assurance that operating and maintenance personnel have appropriate access authorization?			
B. Compliance Knowledge and Training			
1. Have you reviewed all Administrative Simplification regulations for their applicability to your business? (This refers to standardization of billing and claims transactions; contact the Office of the Director of Patient Financial Services for information about transactions and coding issues.)			
2. Are the mandated, formal policies and procedures about sanctions or disciplinary actions in place and communicated to the entire workforce including notice of civil or criminal penalties for the misuse or abuse of health information?			

	Yes	No	Documentation location or explanation for not following
3. Does your organization have a documented, formal process assuring that security awareness training is provided on a routine basis, including all system users, workforce and maintenance personnel? Does this include periodic awareness reminders?			
C. Facility Access Controls, Workstation Use and Location			
1. Are formal, current physical access control policies and procedures in place which allow only appropriate access to an entity including visitor control, and control of access to software programs for testing and revision? Do they include: • Validation of access privileges prior to granting physical access to the facility/ facilities? • A plan for security of the facility/facilities to safeguard against unauthorized access?			
2. Are formal, current documented policies and procedures in place that • Decrease or limit the chance that PHI can be viewed inappropriately? (E.g., terminal placement in any area of a doctor's office where the screen contents can be viewed from the reception area.) • Define the functions, manner of performance, and physical attributes of the surroundings of a computer terminal site based on the sensitivity of the data accessed from that site?			
3. Is each workstation and printer labeled to identify it as a part of a specific system or network and for maintaining inventory?			
D. Review and Audit			
1. Does the department take responsibility for monitoring its own compliance as required by Health System Policy 0217 (*Compliance Auditing and Monitoring Program*)?			

	Yes	No	Documentation location or explanation for not following
2. Does the security awareness training program include mandatory information about monitoring log-in successes and failure and reporting discrepancies or suspicions?			
3. Are audit controls in place and documented to record and examine system activity?			
4. Is there a data authentication mechanism in place to corroborate that data have not been altered or destroyed? (This could include the use of a check sum, double keying, message authentication code, or digital signature.)			
Prepared by: Name: _____ Signature: _____ Title: _____ Date: _____	Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____		

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: GLBA Supplement

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.

In addition to the issues covered in the general questions, additional GLBA issues focus on the need for specific training of employees on GLBA compliance, confidentially agreements and safeguards and the protection of paper-based data.

Note: Since GLBA data may be some combination of highly and moderately sensitive data, in addition to the GLBA specific requirements below, all GLBA data must be protected as required by the Electronic Storage of Highly Sensitive Data policy and the Institutional Data Protection Standards for highly and moderately sensitive data.

	Yes	No	Documentation location or explanation for not following
A. Employee Training and Management			
1. Do you train employees to take at least the basic steps below to maintain the security, confidentiality and integrity of customer financial information (hereafter "protected data")? • Locking rooms, file cabinets where records kept • Locking access to terminals with strong passwords • Changing passwords periodically • Maintaining password confidentially, including not posting them • Encrypting sensitive customer communication when transmitted or stored electronically • Referring requests for information only to other authorized individuals who have been trained			
2. Do you obtain signed confidentiality agreements from all employees handling protected data?			
3. Do you limit access to protected data to those who have a business reason to see it?			

	Yes	No	Documentation location or explanation for not following
B. Information Systems			
1. Do you store records in a secure area? • Paper records in a room, cabinet or container that is locked when unattended • Storage areas are protected from physical hazard like fire or flood • Store electronic data on a securely administered server located in a physically secured area, and limit local workstation storage as much as possible • Maintain and secure backups of protected data			
2. Do you provide for secure data transmission? • Use SSL or other secure connection to encrypt protected data in transit • Caution customers and/or students against transmitting sensitive data by e-mail • If e-mail is used, secure the receiving account and encrypt transmission, if possible			
3. Do you dispose of protected data in a secure manner? • Shred or recycle protected paper-based information securely • Remove all data and software from hardware and electronic media prior to transfer within U.Va. • Process all hardware and electronic media through Procurement's designated vendor when it is leaving U.Va. • Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices			
4. Do you use audit and oversight procedures to detect improper disclosure or theft of protected data?			

	Yes	No	Documentation location or explanation for not following
C. Detecting, Preventing & Managing Systems Failures			
1. Do you follow the best practices outlined in the main question set? • Timely installation of software patches • Automatic anti-virus checking and updating • Backup • Mission continuity planning			
2. Do you use tools like passwords and other personal identifiers to authenticate the identity of customers and/or students seeking to transact business electronically?			
3. Do you notify customers promptly if their non-public personal information is subject to loss, damage or unauthorized access?			
4. Do you ensure that all financial services contracts contain boilerplate language confirming third-parties will maintain appropriate safeguards?			
Prepared by: Name: _____ Signature: _____ Title: _____ Date: _____	Approved by: Unit head Name: _____ Signature: _____ Title: _____ Date: _____		

Unit Name: _____ Sub-Unit Name: _____

Risk Assessment Questions: FERPA Supplement

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.

In addition to the issues covered in the general questions, additional FERPA issues focus on the need for specific training of employees on FERPA compliance, confidentially agreements and safeguards and the protection of paper-based data.

Note: Since FERPA data is defined as moderately sensitive data, in addition to the FERPA specific requirements below, all FERPA data must be protected as required by the Institutional Data Protection Standards for moderately sensitive data.

	Yes	No	Documentation location or explanation for not following
A. Employee Training and Management			
1. Do you train employees to take basic steps to maintain the security, confidentiality and integrity of student information (hereafter "protected data")? • Knowing which student data may be released without permission and which may not • Locking rooms, file cabinets where records kept • Locking access to terminals with strong passwords • Changing passwords periodically • Maintaining password confidentially, including not posting them • Encrypting sensitive customer communication when transmitted or stored electronically • Referring requests for information only to other authorized individuals who have been trained			
2. Do you obtain signed confidentiality agreements from all employees handling protected data?			
3. Do you limit access to protected data to those who have a business reason to see it?			
4. Do you require completion of the FERPA Tutorial for anyone handling FERPA-protected data?			

	Yes	No	Documentation location or explanation for not following
B. Information Systems			
1. Do you store records in a secure area? • Paper records in a room, cabinet or container that is locked when unattended • Storage areas are protected from physical hazard like fire or flood • Store electronic data on a securely administered server located in a physically secured area, and limit local workstation storage as much as possible • Maintain and secure backups of protected data			
2. Do you provide for secure data transmission? • Use SSL or other secure connection to encrypt protected data in transit • Caution customers and/or students against transmitting sensitive data by e-mail • If e-mail is used, secure the receiving account and encrypt transmission, if possible			
3. Do you dispose of protected data in a secure manner? • Shred or recycle protected paper-based information securely • Remove all data and software from hardware and electronic media prior to transfer within U.Va. • Process all hardware and electronic media through Procurement's designated vendor when it is leaving U.Va. • Media include hard drives (from computers, printers, copiers, etc.), magnetic tapes, diskettes, CDs, DVDs and USB storage devices			
4. Do you use audit and oversight procedures to detect improper disclosure or theft of protected data?			

	Yes	No	Documentation location or explanation for not following
C. Detecting, Preventing & Managing Systems Failures			
1. Do you follow the best practices outlined in the main question set? • Timely installation of software patches • Automatic anti-virus checking and updating • Backup • Mission continuity planning			
2. Do you use tools like passwords and other personal identifiers to authenticate the identity of customers and/or students seeking to transact business electronically?			
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***, ***attacks*** and ***vulnerabilities*** 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.

(A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.)

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 Windows Update or Microsoft Update ❑ Departmental patching service ❑ ITC's free Windows Patch Management ❑ HS/CS free SMS update management service ❑ _____ ❑ _____ ❑ _____

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 (ITC | HS/CS) ❑ 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 ❑ Move to ITC's more secure network or HS/CS's secure clinical subnet ❑ ITC's Internet security scanning service ❑ ISPRO's web application security scanning service ❑ _____ ❑ _____ ❑ _____
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 ❑ Unix server 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) ❑ Move to ITC's more secure network or HS/CS's secure clinical subnet ❑ Regular staff training on legal requirements and Electronic Storage of Highly Sensitive Data Policy ❑ Follow Electronic Data Removal policy ❑ De-identify (anonymize) protected data used in research projects ❑ 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 ❑ Have ITC (HS/CS) manage or host services Win | Unix ❑ _____ ❑ _____ ❑ _____
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 ❑ _____ ❑ _____ ❑ _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
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 principal ❑ Back up frequently ❑ Have ITC (HS/CS) manage or host services Win | Unix ❑ _____ ❑ _____ ❑ _____
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 ❑ Have ITC (HS/CS) manage or host services Win | Unix ❑ _____ ❑ _____ ❑ _____

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 ❑ Have ITC (HS/CS) manage or host services Win | Unix ❑ _____ ❑ _____ ❑ _____

Potential Threat, Attack or Vulnerability	Department's Identified Assets Affected	Department's Identified Strategies
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

(A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.)

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) 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:	Approved by: Unit head
Name: _____	Name: _____
Signature: _____	Signature: _____
Title: _____	Title: _____
Date: _____	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 (what the CIMP refers to as a Level 1 incident). 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. (A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.)

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 ITC or HS/CS 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 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)? See CIMP for official University notification procedures. (Those in the Health System should route notification through HS/CS.) All contacts with the public regarding the incident should be routed through University Relations (Media Relations in the Health System).	
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.)	

	Documentation Location and/or Decision
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?	

	Documentation Location and/or Decision
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?	
18. Do your plans incorporate research groups that otherwise operate independently or ensure sure they have made plans of their own? For example, researchers who have critical data (i.e., highly sensitive or on which valuable grants depend).	
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. (A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.) This template was borrowed and adapted from a model created by HS/CS. The template is intentionally thorough to allow its use in complex situations, so some sections may not be applicable for simple and lower priority items. For example, many departments will not have items deemed critical enough to require interim manual procedures, assuming recovery can be completed within a few days. For an example, an executive summary of ITC's disaster recovery plan is available at <http://www.itc.virginia.edu/security/disaster.html>.

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. A copy of your department's general disaster recovery plan should be on file with the U.Va. Police Department, and your IT Mission Continuity Plan should be included in that filing.

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.

A. 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.

2. Scope of the Mission Continuity Plan

INSERT here what your plan covers and does NOT cover.

3. 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.

4. Interfaces

INSERT here a list of any inbound or outbound interfaces to other systems required for the departmental application's operation.

5. 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.

6. 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.

7. Interim Manual Procedures (aka Downtime Procedures)

INSERT here references to existing documented procedures to be used during a system outage.

B. 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.

2. 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.

3. Vendor Contact List

INSERT here contact information (names, phone, email, US 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.

4. 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.

5. 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 (HS/CS, ITC or a Hot or Cold site vendor), notification procedures should be included.

C. 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 HS/CS, ITC or other entity on behalf of the department.

2. 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.

3. 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.

4. 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.

5. 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 HS/CS or ITC network team to detail and diagram any alternative network connections required.

D. 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.

2. 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.

3. 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.

4. 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.

5. 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.

E. 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.).

2. 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.

F. 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.

2. 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.

G. 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.

2. 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.

3. 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).

4. 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.

H. 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.

I. 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:	Approved by: Unit head
Name:	Name:
_____	_____
Signature:	Signature:
_____	_____
Title:	Title:
_____	_____
Date:	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, ITS-RM 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 requires reassessment of your department's ITS-RM at least every 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.

Note: HIPAA requires retention for at least six years after their last effective date of compliance planning records with decisions and justifications, including the risk management portion of that planning. The ISPRO repository of your completed ITS-RM document can serve as a backup for departmental retention.

Below are a series of questions to help you complete your 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 state or federal standards)

(A copy of this template, as well as all the other templates required to complete your department's report on the ITS-RM process, is available in Word format here and Adobe PDF format here.)

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: 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 compliance 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 state or federal 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: _____	

F. Reporting Requirements

1. A copy of all ITS-RM working papers and final forms should be kept in the department, and a copy should be placed in secured off-site storage (e.g., along with your backups) for retrieval in the event local access is impossible.

2. Upon the completion of the five forms listed below (A-E) and approval of them by the department head (and the appropriate dean or vice president if he/she has decided this additional step is important), a copy (templates are available in a compact reporting format in Word format and PDF format) should be sent by e-mail to:

   its-rm@virginia.edu

   or by messenger mail to:

   ITS Risk Management
   Information Security, Policy, and Records Office (ISPRO)
   P.O. Box 400898

   A. **Mission Impact Analysis Questions**
   B. **Risk Assessment Questions and Threat/Response Scenarios**
   C. **Security Plan**
   D. **IT Mission Continuity Questions and Plan**
   E. **Evaluation and Reassessment Questions** (if appropriate)

ISPRO will file a copy of each department's mission continuity plan with the University Disaster Recovery Coordinator, U.Va. Police Department. Documentation from departments hosting HIPAA/HITECH-protected data will be shared with the HS/CS security office. These documents will be used to identify new services required and areas where central assistance is needed. Moreover, they assist the University in doing its own assessment of its overall IT security risks. They also need to be stored in a protected central location for University access in emergency situations. These documents will be kept in strictest confidence and will be used only in emergencies and to gauge an aggregate view of the University's IT security environment.

This reporting process will be repeated with each subsequent evaluation and reassessment.

IV. Appendices

Appendix A: Sample Responses

Sample responses will be added to the program web page as they become available. These will be anonymized composites of actual responses in order to provide an indication of the type and level of response expected of departments.

http://www.itc.virginia.edu/security/riskmanagement/

Appendix B: Systems and Services Supported by ITC

The systems and services listed below are maintained and supported by ITC, including risk management, as of the publication of this document.

If you have questions regarding the risk management or disaster recovery procedures related to an ITC-supported system on which your department depends or if you have a critical system that you want to place under ITC support, see the ITC Services Directory for contact information on individual services.

Administrative Systems
Messaging Services (CMS, Exchange)
Integrated System Infrastructure
Student Information Systems (SIS) Infrastructure

Infrastructure
Network Systems (Agency 207), including More Secure Network
Telephone Service

Instructional Resources
Electronic Teaching Classrooms
Collab

Server Services
Home Directory
Microsoft Server Administration*
Premium Server
UNIX Server Administration*
UNIX Web Services
Windows Web Services
Windows Patch Management Service

** These services are available on a contract basis. Note; ITC provided server space is often jointly managed between departments and ITC, with each retaining some level of responsibility. Moreover, many departments also maintain such services locally without ITC support.*

Note that your department may have chosen to provide alternatives to some of the above central services on a local basis. For example, one school has taken on certain network functions; a few departments provide their own e-mail or Web service, or host computer labs; and many departments have their own file servers.

All systems should have downtime plans and restoration/recovery plans in the event of a system failure. Each system and service has a different return to service timeframe based on its criticality and the severity of the problem. (If you have a contract for a specific service with ITC, a customized return to service time may be specified.) ITC regularly performs an IT security risk management process on its own resources in order to protect its assets and prepare for disaster recovery.

An executive summary of the ITC disaster recovery plan, including general time to recovery estimates, is at <http://www.itc.virginia.edu/security/disaster.html>.

Appendix C: Systems Supported by the Health System

The systems below are maintained and supported by the Health System, including risk management and HIPAA/HITECH compliance, as of the publication of this document. The applications listed below are the major systems supported by the Health System, but the list is not exhaustive.

If you have questions regarding the risk management or disaster recovery procedures related to a Health System-supported system on which your department depends or if you have a critical system that you want to place under Health System support, call the Computing Services Help Desk (924-5334) for contact information on individual services.

The chart below lists systems with broad use and official medical record status. The most current version of this list is maintained in Health System policy 0218 (Definition, Characteristics, and Maintenance of the Medical Record),

System	***Responsible Party***
CAOS (Heart Center Labs)	Heart Center Computing
CAS	Health System Computing
Co-path	Pathology
Eclipsys/MIS	Health System Computing
IDX Physician Billing, Charge capture (TES)	Health System Computing
LanVision document imaging	Health Information Services (HIS) and Health System Computing
ORMIS System	OR Services
PACS – Dicom Imaging	Health System Computing and Radiology
Radiology Information System (RIMS)	Radiology
SMS Registration, Patient Billing	Health System Computing
SMS Resource Scheduling	Health System Computing
SoftMed	HIS and Health System Computing
Sunquest (labs)	Pathology
Tracks	Health System Computing

In addition, Health System Computing is responsible for the following central systems:

- File Servers (e.g., O:, Q:, Z: drive)
- Microsoft SMS (update management service)
- Network Systems (Agency 209), including Secure Clinical Subnet (SCSN)
- Outlook e-mail and calendaring
- PeopleSoft
- Windows Web Services

See also HS/CS's software support policy, which places applications into four categories of support: full, partial, unsupported, and unauthorized.

Note that your department may have chosen to provide alternatives to some of the above central services on a local basis, e.g., file servers.

All systems should have downtime plans and restoration/recovery plans in the event of a system failure. Each system and service has a different return to service timeframe based on its criticality and the severity of the problem. (If you have a contract for a specific service with HS/CS, a customized return to service time may be specified.) HS/CS regularly performs an IT security risk management process on its own resources in order to protect its assets and prepare for disaster recovery.

Appendix D: Does HIPAA Apply to Our Department?

HIPAA (Health Insurance Portability and Accountability Act) places significant privacy and security requirements on health care practitioners and researchers. If HIPAA applies to your department, you must to take additional steps in your risk analysis and response.

Note: The HITECH (Health Information Technology for Economic and Clinical Health) Act extended the reach of HIPAA. It extends the HIPAA privacy and security provisions, including updated fines and penalties to business associates. It also creates new requirements regarding PHI breach notification.

Note: As HIPAA data is defined as highly sensitive data, in addition to the HIPAA specific requirements below, all HIPAA data must be protected as required by the Electronic Storage of Highly Sensitive Data policy and the Institutional Data Protection Standards for highly sensitive data.

Does your department handle medical information that is combined in any way with one or more of the following personal health identifiers (PHI)? If the answer is "yes," then HIPAA applies to your department.

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains less than 20,000 people
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images; and

18. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual

For more information, researchers and other Agency 207 employees should contact its-rm@virginia.edu; Agency 209 employees should contact the U.Va. Health System Corporate Compliance and Privacy Office (924-9741).

Appendix E: Does Gramm-Leach-Bliley Apply to Our Department?

Does your department provide financial services that place you under the security provisions of the federal Financial Services Modernization Act, also known as the Gramm-Leach-Bliley Act, which includes regulations to protect consumers' personal financial information?

- Do you collect personal financial information pursuant to *issuing* credit, including credit cards? (*Accepting* credit does not apply.)
- Do you collect personal financial information pursuant to granting loans?
- Do you collect payments on which interest is paid? (Deferred payment plans that do not charge interest do not apply.)
- Do you broker investments or mortgages?
- Do you provide financial advice for a fee?
- Do you collect personal financial information pursuant to any other "financial product or service"? (Think about the services banks, brokerages and insurance companies provide.)
- Have you negotiated a contract with a financial service provider or do you plan to in the future?

Note: The Health System does not appear to be covered by GLBA at this time. However, from an operational standpoint, the issue is moot, because HIPAA standards are more comprehensive than GLBA's; all the practices required by GLBA are also required by HIPAA.

Note: For details on the Financial Services Modernization Act see

http://counsel.cua.edu/FEDLAW/glb.cfm

Appendix F: Does FERPA Apply to Our Department?

FERPA (Family Educational Rights and Privacy Act) restricts access and release of student information. Full information on the University's FERPA-related policies are at <http://www.virginia.edu/registrar/privacy.html>.

The University may disclose personally-identifiable information designated as directory information from a student's education records without prior consent, unless the student informs the Office of the University Registrar in writing that directory information should not be released without written consent. This certification does not preclude the verification of degrees awarded. Directory information consists of:

- student name
- home and school addresses, telephone numbers, e-mail address
- year of birth
- country of citizenship
- major(s)
- school of enrollment
- full or part-time status
- year in school
- participation in officially-recognized activities and sports
- dates of attendance
- degrees, honors, scholarships, and awards received
- most recent previous educational institution attended
- names of parents or guardians
- and weight and height of members of athletic teams.

All other information not specifically listed, including grades, courses, days and times of course meetings, withdrawals, suspension, and month and day of birth, cannot be disclosed without the student's permission. Such information needs to be protected not only from external release, but also protected from access by those within the University who do not have an authorized, job-related need to see it.

Appendix G: What is Highly Sensitive Data?

By University policy, highly sensitive data currently include personal information that can lead to identity theft if exposed and health information that reveals an individual's health condition and/or history of health services use. While other types of sensitive data, such as student names in combination with course grades obviously exist, the negative impact of unauthorized exposure of data specifically designated highly sensitive (and described in detail below) is especially acute.

- *Personal information that, if exposed, can lead to identity theft*. "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements about the individual:

1. Social security number;
2. Driver's license number or state identification card number issued in lieu of a driver's license number;
3. Passport number; or
4. Financial account number, or credit card or debit card number.

- Health information that, if exposed, can reveal an individual's health condition and/or history of health services use. "Health information," also known as "protected health information (PHI)," is defined in Appendix D: Does HIPAA Apply to Our Department?

Appendix H: Related Policies and Resources

- IT Security Risk Management page (for updates and new tools)
  - http://www.itc.virginia.edu/security/riskmanagement/

- ITC's Security and Policy pages
  - http://www.itc.virginia.edu/security/
  - http://www.itc.virginia.edu/policy/
  - Responsibilities for Computing Devices Connected to the University of Virginia Network
    http://www.itc.virginia.edu/policy/netdevices/
  - IT Security for Departmental Managers:
    http://www.itc.virginia.edu/security/manager.html
  - Responsible Computing Handbook for Faculty and Staff
    http://www.itc.virginia.edu/pubs/docs/RespComp/resp-comp-facstf.html

- Health System Computing Services (HS/CS)
  - http://www.healthsystem.virginia.edu/intranet/computing

- University Policies
  - University Information Technology Security Program
    https://policy.itc.virginia.edu/policy/policydisplay?id=IRM-011
  - Administrative Data Access
    http://www.itc.virginia.edu/policy/admindataaccess.html
    - Institutional Data Protection Standards
      http://www.itc.virginia.edu/security/dataprotection/
  - Electronic Data Removal
    https://etg07.itc.virginia.edu/policy/policydisplay?id=IRM-004
  - Electronic Storage of Highly Sensitive Data
    https://etg07.itc.virginia.edu/policy/policydisplay?id=IRM-015
  - IT Security Incident Reporting
    https://etg07.itc.virginia.edu/policy/policydisplay?id=IRM-012
  - Protection and Use of Social Security Numbers
    https://etg07.itc.virginia.edu/policy/policydisplay?id=IRM-014
  - Records Retention and Disposition
    http://www.virginia.edu/finance/polproc/pol/iic1.html
  - Protecting Privacy Rights of Students
    http://www.virginia.edu/finance/polproc/pol/xvd1.html
  - Internal Controls
    https://policy.itc.virginia.edu/policy/policydisplay?id=FIN-021
  - Internal Audit
    http://www.virginia.edu/audit/faq.html#charter

- University's Critical Incident Management Plan (CIMP)
  - http://www.virginia.edu/emergency/plan.html

Appendix I: 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).[5] Although the project design team ended up adopting most of the source's original text, it was edited and supplemented to improve U.Va.-appropriateness. Comments and additions are indicated below in brackets.

Definitions

[These definitions are in logical, not alphabetical, order so that one could read them through and learn about how the pieces of the ITS-RM process fit together.]

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: "The combination of events harmful to an entity's desired state of affairs, the chance that the events will take place, and the consequences of their occurrence, as a function of time." (NSA Corporate Plan for INFOSEC Action, April 1996)

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*?"]

[5] 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/>.

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