**Borrowed and adapted from a model created by University of Virginia**

### IT Security Risk Management Process Flow

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

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

*Security*

*Plan*

*Interim*

*Manual*

*Procedures*

*Disaster*

*Recovery*

*Plan*

Step 4 – Evaluation and Reassessment

Required at least once every two or three years

Step 3 – Mission

Continuity Planning

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

Step 2 – Assess Risks

For each critical asset:

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

*Critical*

*Assets*

*List*

Step 1 - Identify

Critical IT Assets

## Step 4: Evaluation and Reassessment

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

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

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

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

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

| Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Sub-Unit Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
| --- | --- |
| Evaluation and Reassessment Questions  Complete every three years or when there are significant changes to departmental IT assets or risk environment (see Table 1 of Step 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 database from Access to SQL Server. |  |
| 3. Are there any new critical data housed in your department?  *Note:* Data may be critical based on mission criticality, sensitivity or protected status. |  |
| 4. Are there any new national or international standards or University policies or standards applicable to your department? If so, to which systems and/or data do they apply? |  |
| 5. What risk mitigation that you could not afford previously can you now afford, or – due to increased risk in that area – you can no longer afford not to mitigate? |  |
| 6. Are there any new technologies allowing for easier and/or cheaper mitigation for certain risks? |  |
| 7. Has there been an increase or decrease in the number of servers (physical and virtual) or systems? |  |
| 8. What interim risk mitigation measures have been put in place for new systems? |  |
| 9. Are there any systems that are no longer mission-critical? If so, are there risk mitigation efforts that can be discontinued? |  |
| 10. What functions have been moved to central servers, so that you no longer have risk management responsibility for them? |  |
| 11. What functions have been moved to local servers, so that you now have risk management responsibility for them? |  |
| 12. What new functions has your department taken on in pursuit of its mission? Are any IT-asset-dependent? |  |
| 13. What old functions have become IT-asset-dependent? |  |
| 14. What relevant personnel turnover, additions or subtractions, or role changes have occurred? |  |
| 15. Do you have any long-term backups (archives) that need to be refreshed on new media (or destroyed)? (Please review and follow Records Management guidance regarding retention and disposition of records.) |  |
| Prepared by: Administrative contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Prepared by: Technical contact  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Approved by: Unit head  Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |