



- UNLV Internal Use ONLY -

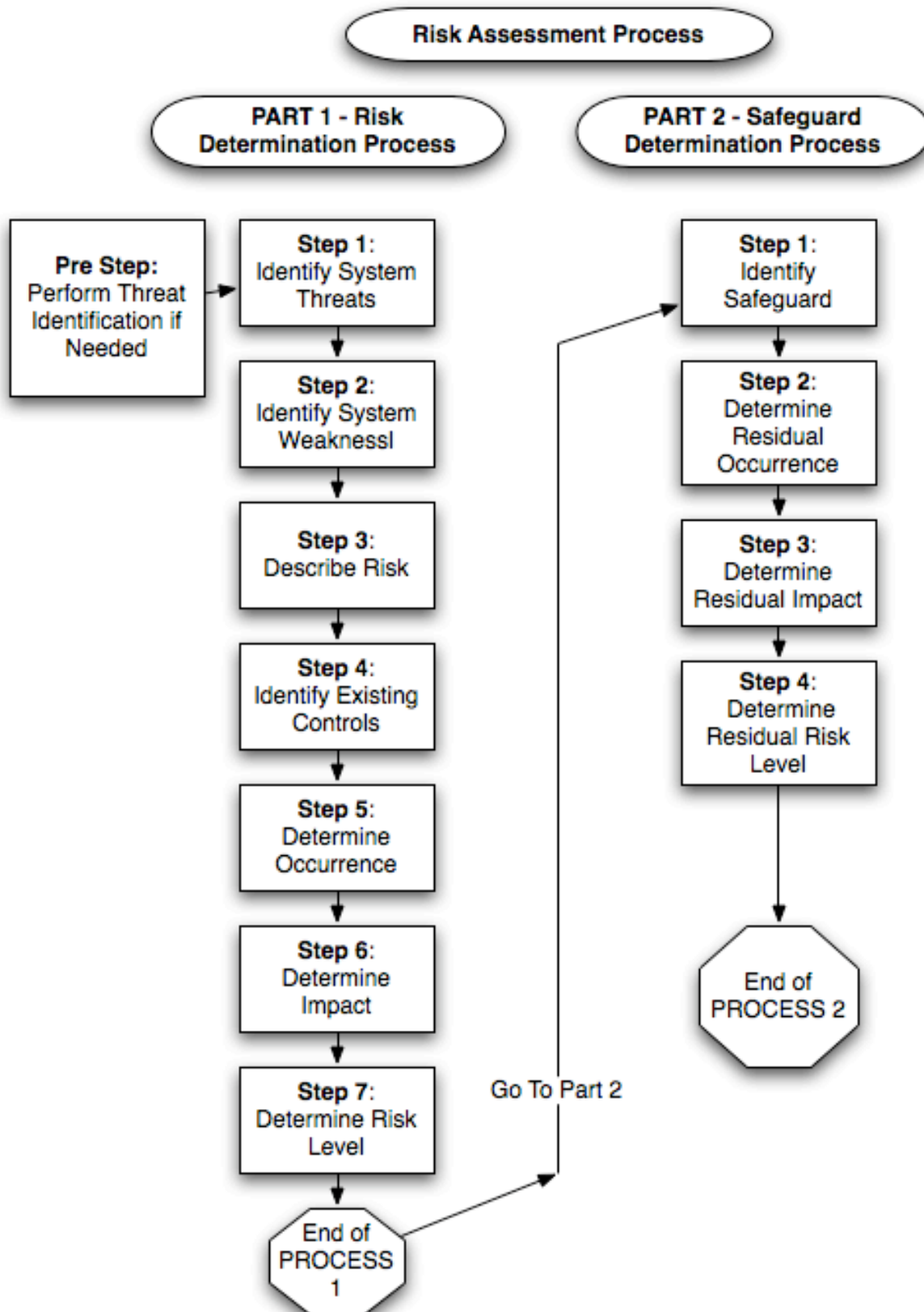
HANDBOOK FOR INFORMATION SECURITY THREAT AND RISK ASSESSMENT

RECOMMENDATIONS OF THE UNLV
OFFICE OF INFORMATION TECHNOLOGY
INFORMATION SECURITY OFFICER
*FOR PERFORMING
RISK ASSESSMENTS.*

- UNLV Internal Use ONLY -

TABLE OF CONTENTS

.....	3
RISK MANAGEMENT AND ASSESSMENT	4
<i>INTRODUCTION.....</i>	<i>4</i>
<i>RISK ASSESSMENT METHODOLOGY RECOMMENDATION</i>	<i>4</i>
<i>SYSTEM/ASSET VALUATION.....</i>	<i>4</i>
<i>RISK CHARACTERISTICS</i>	<i>4</i>
<i>RISK DETERMINATION.....</i>	<i>4</i>
<i>RESPONSIBILITIES</i>	<i>5</i>
<i>QUICK REFERENCE DEFINITIONS.....</i>	<i>5</i>
PART 1: RISK DETERMINATION GUIDE.....	7
<i>THE SEVEN STEPS OF RISK DETERMINATION.....</i>	<i>7</i>
Step 1: Identify/Select System Threats	7
Step 2: Identify System Weakness/Vulnerabilities.....	8
Step 3: Describe Risk	8
Step 4: Identify Existing Controls	8
Step 5: Determine the Likelihood of Occurrence.....	8
Step 6: Determine the Severity of Impact.....	9
Step 7: Determine the Risk Level	10
PART 2: SAFEGUARD DETERMINATION GUIDE.....	11
<i>THE FOUR STEPS OF SAFEGUARD DETERMINATION.....</i>	<i>11</i>
Step 1: Identify Safeguards	11
Step 2: Determine Residual Likelihood of Occurrence.....	12
Step 3: Determine Residual Severity of Impact.....	12
Step 4: Determine Residual Risk Level	12
APPENDIX 1 : RISK CHARACTERISTICS QUICK REFERENCE	13
<i>RISK CHARACTERISTICS - SENSITIVITY CHECKLIST.....</i>	<i>16</i>
<i>RISK CHARACTERISTICS - CRITICALITY CHECKLIST.....</i>	<i>17</i>
APPENDIX 2 : THREAT IDENTIFICATION GUIDE.....	18
<i>HOW TO USE THE GUIDE</i>	<i>27</i>
<i>HUMAN THREATS.....</i>	<i>28</i>
<i>TECHNICAL THREATS.....</i>	<i>38</i>
APPENDIX 3 : RISK ASSESSMENT REPORT TEMPLATE.....	51



Risk Management and Assessment

Introduction

High-level risk management provides an environment for identifying and assessing operational threats and risks (both technically and managerially), determining the relative importance of identified risks, implementing strategies to deal with these risks, and focusing attention for effective, proactive, decision making. Risk management also provides a tool for analyzing the benefits of various information security best-practice options.

Risk Assessment Methodology Recommendation

The recommended high-level information security **threat identification** model for UNLV is the simplified Threat Identification Guide that is an appendix of this handbook.

The recommended **standard** high-level risk assessment model for UNLV is the **simplified** risk assessment. Additional guidance on effective risk assessment can be found in "*An Introduction to Computer Security: The NIST Handbook*". See <http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

The standard for a **formal** risk assessment model is the "*Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)*" methodology created by Carnegie Mellon University. Further information on the OCTAVE model can be found at <http://www.cert.org/octave/pubs.html>. A **formal** risk assessment is **not** recommended except for rare and unusual circumstances or specific regulatory requirements.

This *Handbook* describes the basic elements of high-level risk management and how it is instituted at UNLV to ensure a continuous review of manual or automated systems critical to its mission at the departmental level.

System/Asset Valuation

System/Asset values included in the risk assessment are taken from the Asset Classification result. A information asset will have a classification of one of three sensitivity levels – Level 1 or Unrestricted-Public Sensitivity, Level 2 or University-Confidential Sensitivity, Level 3 or Restricted Sensitivity . These levels will be used as the valuation. IT equipment and systems used to support the asset will be assigned the same sensitivity level as the highest level related asset.

Risk Characteristics

The risk characteristics were, or should have been, developed during the Asset Classification process and threat characteristics can be developed using the threat Guide included herein. Also included in this handbook is a risk characteristics reference and checklist to help you to recall the items you will need for the risk assessment process.

Risk Determination

The objective of a risk assessment is to determine the threats and current level of risk associated with the implementation or operation of a system. The risk assessment must be included with the System Security Plan. First, the assets related to the system must be identified (from the Asset Classification) and valued. Then, specific threats and vulnerabilities are identified and analyzed for the possible losses that could be incurred. Next, potential safeguards are evaluated to select those that are most cost-effective in addressing the threats and eliminating or reducing the vulnerabilities to an acceptable level of risk.

Please Note: (1) System Developers are required to perform a information security *threat* assessment for all new UNLV major applications (GSS or MA) or whenever significant

modifications are to be made to the system. The threat assessment report and supporting documentation must be used in the mandatory risk assessment.

(2) System Owners/Managers and System Maintainers must conduct a risk assessment every year for a GSS or a high risk MA; every three years for all other MAs and "other systems"; whenever significant modifications are made to the system; whenever a major security violation occurs; or when the threat "landscape" significantly changes. The System Owners/Managers must retain all risk assessment reports and supporting documentation for at least seven years.

A complete risk assessment consists of the following:

- System/Asset Valuation (from the Asset Classification)
- Risk Determination
 - Threat Identification
 - Vulnerability Identification
- Safeguard Determination

Responsibilities

UNLV Management

UNLV Management (School Office/Department/Campus) have the responsibility to:

- Ensure that appropriate high-level risk assessments covering all data, Major Applications (MA), and General Support Systems (GSS) under their jurisdiction are performed.
- Ensure that appropriate threat assessments covering all new or significantly modified Major Applications (MA), and General Support Systems (GSS) under their jurisdiction are performed.
- Approve risk prioritization, risk mitigation through best-practices plans, and the closure of risks.
- Facilitate timely actions and decisions.
- Attach copy of RA to the System Security Plan (SSP)

Department/System Information Security Liaison (ISL)

ISLs (School Office/Department/Campus) are responsible to participate with departments to ensure that risk management is integrated into all GSSs and MAs.

System Owners/Managers

The System Owners/Managers have the responsibility to:

- Conduct regular asset classification reviews for changes.
- Conduct regular high-level risk assessment of GSSs and MAs to determine cost-effective and essential information system security "best-practice" safeguards.
- Develop and implement best-practice mitigation plans for those risks for which they have the authority to commit resources.
- Provide a copy of all system risk assessments as input for the development of System Security Plans (SSP) by his/her organization.
- Maintain a copy of risk assessment reports for seven years.

Quick Reference Definitions

GENERAL SUPPORT SYSTEMS (GSS) -Computer platform that incorporates hardware, operating system software, and environmental software to support major applications, e.g. data center, web hosting, web services. An

interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people. It provides support for a variety of users and/or applications. Individual applications supporting different business-related functions may run on a single GSS. Users may be from the same or different organizations. (SSP Methodology) An interconnected set of information resources under the same direct management control that shares common functionality. Normally, the purpose of a **general support system** is to provide processing or communication support. An interconnected set of information resources under the same direct management control, which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a LAN including smart terminals that supports a branch office, an agency-wide backbone, a communications network. A departmental data processing center including its operating system and utilities, a tactical radio network, or shared information processing service organization.

MAJOR APPLICATIONS (MA) -Major Applications consist of data and customized application software only. They are housed on one or more GSSs. Defined as an application that requires special attention due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information in the application. An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. A breach in a major application might compromise many individual application programs, hardware, software, and telecommunications components. A major application can be either a major software application or a combination of hardware/software. Its sole purpose is to support a specific mission-related function. -An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Adequate security for other applications should be provided by security of the systems in which they operate. All "Major Applications" require "special management attention." The System Security Plan for a Major Application may be defined broadly enough to include hardware, software, networks, and even facilities where it is reasonable. This permits the systems to be bounded in reasonable ways for the purposes of security planning.

PART 1: RISK DETERMINATION GUIDE

The goal of a risk determination is to determine the level of risk for each threat and vulnerability combination based on: (1) the likelihood of a threat exploiting a vulnerability; and (2) the severity of impact that the exploited vulnerability would have on the system, its data and its business function in terms of loss of confidentiality, loss of integrity and loss of availability.

The phase is comprised of seven steps and is conducted for each identified threat/vulnerability pair:

- 1) Identify potential dangers to information and system (threats).
- 2) Identify the system weakness that could be exploited (vulnerabilities) associated to generate the threat/vulnerability pair.
- 3) Describe the risk.
- 4) Identify existing controls to reduce the risk of the threat to exploit the vulnerability.
- 5) Determine the likelihood of occurrence for a threat exploiting a related vulnerability given the existing controls.
- 6) Determine the severity of impact on the system by an exploited vulnerability.
- 7) Determine the risk level for a threat/vulnerability pair given the existing controls.

What is Threat Identification - Threat identification requires the determination and assessment of potential threats to UNLV IT resources. Potential threats include both natural disasters and people who can disrupt operations, or time-dependent services, or can cause loss of physical assets, loss of system integrity, or harm to the business of the organization, whether intentional or unintentional. The threat identification must result in a list of threats, practical not theoretical, for every aspect of the sensitive GSS and/or MA including the hosting facility.

What is Vulnerability Identification - Vulnerability identification involves the determination of weaknesses or flaws that exist in a sensitive system or facility that could allow a threat to affect its security. Vulnerability identification must be performed on new, existing, and recently modified sensitive systems and facilities. A summary list of vulnerabilities must be prepared for each sensitive system and facility being analyzed.

The Seven Steps of Risk Determination

Perform each of the seven steps as directed.

Note – The phrase "the Table" used below refers to the appropriate Table in the RA Template at the end of the document. The Item Number designated in the left-most column is for reference purposes only. It is assigned in numerical order as rows are added to the table for different threat/vulnerability pairs. The Item No. is also used in Table 5 in the Safeguard Determination Phase, to correlate the analysis done in both tables.

Step 1: Identify/Select System Threats

Identify and select the threats that could have the ability to exploit system vulnerabilities. These are environmental/physical, human, natural, and technical threats that may affect General Support Systems, Major Applications, and Other Type Systems, when applicable. The system owner must consider interconnection and interdependencies with other systems that may introduce new threats to the system under review. Therefore, an understanding of the system's interconnections and subordinate processes, if any, will provide significant information regarding inherited and new risks and controls that may affect the system and they must be identified in this section.

It is recommended to use the Threat Identification Guide (Appendix 2) and associated reference tables for establishing the system threats.

Complete the columns labeled “Item No.” and “Threat Name” in the Table with the result of this step.

Step 2: Identify System Weakness/Vulnerabilities

Select vulnerabilities associated with each threat to produce a threat/vulnerability pair. Vulnerabilities may be associated with either a single or multiple threats. Previous risk assessment documentation, audit and system deficiencies reports, security advisories and bulletins, automated tools and technical security evaluations may be used to identify threats and vulnerabilities. Testing results during and after system development as part of the system’s System Development Life Cycle (SDLC) may be used to identify vulnerabilities for new systems or systems undergoing major modifications.

Complete the column labeled “Vulnerability Name” in the Table with the result of this step.

Step 3: Describe Risk

Describe how the vulnerability creates a risk in the system in terms of confidentiality, integrity and/or availability elements that may result in a compromise of the system and the data it handles. If possible identify any compliance regulations impacted by the risk.

Complete the column labeled “Risk Description” in the Table with the result of this step.

Step 4: Identify Existing Controls

Identify existing or new controls that reduce: (1) the likelihood or probability of a threat exploiting an identified system vulnerability, and/or (2) the magnitude of impact of the exploited vulnerability on the system. Existing controls may be management, operational and/or technical controls depending on the identified threat/vulnerability pair and the risk to the system.

Complete the column labeled “Existing Controls” in the Table with the result of this step.

Step 5: Determine the Likelihood of Occurrence

Determine the likelihood that a threat will exploit a vulnerability. The likelihood is an estimate of the frequency or the probability of such an event. Likelihood of occurrence is based on a number of factors that include system architecture, system environment, information system access and existing controls; the presence, motivation, tenacity, strength and nature of the threat; and the presence of vulnerabilities; and the effectiveness of existing controls. Refer to the information provided in Table 1 for a guideline to determine the likelihood of occurrence of the threat.

Table 1. Likelihood of Occurrence Levels

Likelihood	Description
Negligible	Unlikely to occur.
Very Low.	Likely to occur two/three times every five years.
Low	Likely to occur one every year or less.
Medium	Likely to occur once every six months or less.
High	Likely to occur once per month or less.
Very High	Likely to occur multiple times per month.

Extreme	Likely to occur multiple times per day
---------	--

Complete the column labeled “Likelihood of Occurrence” in the Table with the result of this step.

Step 6: Determine the Severity of Impact

Determine the magnitude or severity of impact on the system’s operational capabilities and data if the threat is realized and exploits the associated vulnerability. Determine the severity of impact for each threat/vulnerability pair by evaluating the potential loss in each security category (confidentiality, integrity and availability) based on the system’s information security level as explained in the UNLV Information Security Level in the SSP guide and described in the System Documentation phase of this methodology. The impact can be measured by loss of system functionality, degradation of system response time or inability to meet a business mission, dollar losses, loss of public confidence, or unauthorized disclosure of data. Refer to the information provided in Table 2 below for a guideline to determine the impact severity levels.

Table 2. Impact Severity Levels

Impact Severity	Description
Insignificant	Will have almost no impact if threat is realized and exploits vulnerability.
Minor	Will have some minor effect on the system. It will require minimal effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit negligible and perhaps only noted by a few individuals or organizations. May cause political or organizational embarrassment. Will require some expenditure of resources to repair.
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system’s resources or services. It will require expenditure of significant resources to repair.
Serious	May cause considerable system outage, and/or loss of connected customers or business confidence. May result in compromise or large amount of sensitive information or services
Critical	May cause system extended outage or to be permanently closed, causing operations to resume in a recovery site environment. May result in complete compromise of sensitive departmental information or services.

Complete the column labeled “Impact Severity” in the Table with the result of this step.

Step 7: Determine the Risk Level

The risk can be expressed in terms of the likelihood of the threat exploiting the vulnerability and the impact severity of that exploitation on the confidentiality, integrity and availability of the system. Table 3 below shows risk levels resulting from the affect of both parameters on the risk level. The system owner may increase the risk to a higher level depending on the system’s information security level and the level of compromise if a threat is realized.

Complete the column labeled “Risk Level” in the Table with the selected result from Table 3 of this step.

Table 3. Risk Levels

Likelihood of Occurrence	Impact Severity					
	Insignificant	Minor	Significant	Damaging	Serious	Critical
Negligible	Low	Low	Low	Low	Low	Low
Very Low	Low	Low	Low	Low	Moderate	Moderate
Low	Low	Low	Moderate	Moderate	High	High
Medium	Low	Low	Moderate	High	High	High
High	Low	Moderate	High	High	High	High
Very High	Low	Moderate	High	High	High	High
Extreme	Low	Moderate	High	High	High	High

This Completes Part 1 of the Risk Assessment process. Go on to Part 2.

PART 2: SAFEGUARD DETERMINATION GUIDE

The Safeguard Determination phase involves identification of additional controls, safeguards or corrective actions to minimize the threat exposure and vulnerability exploitation for each threat/vulnerability pairs identified in the Risk Determination phase and resulting in moderate or high risk levels. Identification of new security measures should address the level of risk already assessed for the threat/vulnerability pair and should reduce the risk level. The residual risk level is determined assuming full implementation of the recommended controls/safeguards.

The Safeguard Determination phase is comprised of four steps:

- Identify the controls/safeguards to reduce the risk level of an identified threat/vulnerability pair, if the risk level is moderate or high.
- Determine the residual likelihood of occurrence of the threat if the recommended safeguard is implemented.
- Determine the residual impact severity of the exploited vulnerability once the recommended safeguard is implemented.
- Determine the residual risk level for the system.

The Four Steps of Safeguard Determination

Perform each of the four steps as directed.

The Safeguard Determination Table in the RA Template can be used to summarize the analysis performed during the Safeguard Determination phase. Use the Item Numbers created for the Risk Determination Table as reference in the Table to correlate the analysis summarized in both tables to the same threat/vulnerability pair and associated risk level. The Items Numbers here are used to maintain consistency, and ease of reference, and match a recommended safeguard to a threat/vulnerability pair that resulted in moderate or high risk levels.

Step 1: Identify Safeguards

Identify controls/safeguards for each threat/vulnerability pair with a moderate or high risk level as identified in the Risk Determination phase. The purpose of the recommended safeguard is to reduce or minimize the level of risk. When identifying a safeguard, consider the:

- 1) Security area where the control/safeguard belongs, such as management, operational, technical;
- 2) Method the control/safeguard employs to reduce the opportunity for the threat to exploit the vulnerability;
- 3) Effectiveness of the proposed control/safeguard to mitigate the risk level; and
- 4) Policy and architectural parameters required for implementation in the environment.

Recommended safeguards will address the security category identified during the risk analysis process (confidentiality, integrity and availability) that may be compromised by the exploited vulnerability.

Complete the column labeled “Recommended Safeguard” in the Table with the result of this step. If more than one safeguard is identified for the same threat/vulnerability pair, list them in this column in separate rows and continue with the analysis steps: the residual risk level must be evaluated during this phase of the assessment and may be further evaluated in risk management activities outside of the scope of this methodology.

If a complete implementation of the recommended safeguard cannot be achieved in the environment due to management, operational or technical constraints, annotate the circumstances in this space and continue with the analysis.

Step 2: Determine Residual Likelihood of Occurrence

Follow the directions described in Step 4 of the Risk Determination phase while assuming full implementation of the recommended safeguard.

Complete the column labeled “Residual Likelihood of Occurrence” in the Table with the result of this step.

Step 3: Determine Residual Severity of Impact

Follow the directions described in Step 5 of the Risk Determination phase while assuming full implementation of the recommended safeguard.

Complete the column labeled “Residual Impact Severity” in the Table with the result of this step.

Step 4: Determine Residual Risk Level

Determine the residual risk level for the threat/vulnerability pair and its associated risk once the recommended safeguard is implemented. The residual risk level is determined by examining the likelihood of occurrence of the threat exploiting the vulnerability and the impact severity factors in categories of Confidentiality, Integrity and Availability.

Follow the directions described in Step 6 of the Risk Determination Phase to determine the residual risk level once the recommended safeguard is fully implemented. Depending on the nature and circumstances of threats and vulnerabilities, a recommended safeguard may reduce the risk level to Low. Annotate with a narrative below the table, if needed, if such special conditions exist.

Complete the column labeled “Residual Risk Level” in the Table with the result of this step.

This Completes Part 2 of the Risk Assessment process.

Checklists & Risk Assessment Report Template

Appendix 1 contains the **Risk Characteristics checklists** for Data Sensitivity and EIR Criticality should be used as a reference for the information selected or assigned during the Asset Classification process.

Appendix 2 contains the information security **Threat Identification Guide** that should be used during the system development cycle and during any major modification to an existing system. It may be used at any time to refresh the threat identifications facing a system and should be reused each annual cycle of risk assessment. The threat report should be used as input to the Risk Assessment process.

The **Risk report template** is in Appendix 3. The Risk report template is a "fill in the form" type of document. The finished report should be attached to the SSP or filed as an amendment to the current SSP for the annual update.

APPENDIX 1 : RISK CHARACTERISTICS QUICK REFERENCE

Risk, Sensitivity and Criticality

Each department or organization must determine which specific Electronic Information Resources (EIR) warrant protective or preventive measures based on a high-level risk assessment.

A. Risk Characteristics. When determining the level of security required for an EIR, there are two basic risk characteristics to be assessed:

- The level of *sensitivity* of the EIR (The level of access controls required for an EIR depends on the *sensitivity* of the EIR.); and
- The level of *criticality* or overall importance of the EIR to the continuing operation of a campus, department, or of the University. (The requirement to include a particular EIR in Disaster Recovery Plans as part of overall business continuity planning depends on the *criticality* of the application to the University.)

Both of these characteristics are identified and documented in the Asset Classification process.

An EIR assumes "system high" risk status – That is, the status is determined by the highest level of sensitivity and criticality of any data item contained within it.

B. Electronic Information Resource Sensitivity. The sensitivity of an EIR, and therefore the level of security required, depends upon the sensitivity of the data retained by or accessible through the EIR. It is identified as a product of conducting the Asset Classification.

Note: A security designation under these guidelines shall have no effect on the treatment, consideration or disclosure of any document or information under state or federal law, including the Family Educational Rights and Privacy Act of 1974 (FERPA).

Data falls into one of two levels of sensitivity: Restricted or Unrestricted. The EIR Owner, with any needed input from UNLV legal counsel, is responsible for determining the level of sensitivity of data based on:

- 1) The level of security required for protecting the data from unauthorized read-only access; and
- 2) The level of security required for protecting the data from unauthorized creation, deletion, or modification, collectively termed "modification" for purposes of these guidelines.

A checklist (**Risk Characteristics - Sensitivity Checklist**) is contained in this document that will provide assistance in determining which data falls into which category.

Restricted Data. *Restricted* data is data that is considered sensitive to some degree. It is divided into two subcategories: *Personal* and *Limited*. **SECURITY FOR RESTRICTED EIR'S IS MANDATORY.**

Personal data refers to:

1. Any information that identifies or describes an individual, including but not limited to, his or her name, social security number, employee identification number, medical history, and financial matters. Access to such data is governed by UNLV, NSHE, local, state and federal policies, codes, laws and regulations, both in terms of protection of the data, and requirements for disclosing the data to the individual to whom it

pertains.

Limited data refers to:

1. Data whose unauthorized access, modification or loss could seriously or adversely affect the University (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the University), or adversely affect the public. Examples of such data may include selected research data where the corresponding research is incomplete, or responses to a Request for Proposal before a decision has been reached.
2. Data that the EIR Owner chooses to protect from general access or modification, although such access is not prohibited by law or University policy. An example might include data containing budget projections for a campus department.

Unrestricted Data. *Unrestricted* data is data for which access or modification is not restricted by law or University policy and is permitted by the EIR Owner. Examples of data that are Unrestricted from the standpoint of access include data contained in public financial reports, class catalogs, and campus general information handbooks.

Unrestricted data that pertains to individuals equates to "nonpersonal" information or, in the case of student records, "public information."

The same data may be classified differently for different purposes. Thus, a staff member's office address may be Unrestricted for read-only access but Restricted for modification. A *Restricted Electronic Information Resource*, as used in the remainder of these guidelines, is an EIR for which the data retained within the resource or accessible through the resource is considered Restricted for either read-only access or for modification access.

C. Electronic Information Resource Criticality. EIR criticality is a measure of the importance of an EIR to the continuing operation of a campus. It is identified as a product of conducting the Asset Classification. The criticality of an EIR determines whether or not it must be included in a campus Disaster Recovery Plan (see Section V, Disaster Recovery and Emergency Procedures. EIRs are classified into three levels of criticality as follows:

- 1) *Essential.* An EIR should be designated as *Essential* if its failure to function correctly and on schedule could result in a major failure by a campus to perform mission-critical business functions, a significant loss of funds to a campus, or a significant liability or other legal exposure to a campus.
- 2) *Required.* An EIR should be designated as *Required* if it performs an important function for a campus, but the operation of the campus could continue for some designated period of time without the function provided by the Information Resource and there is time for recovery should the Information Resource not perform correctly or on schedule.
- 3) *Deferrable.* An EIR should be designated *Deferrable* if a campus could continue operation for an extended period of time without the Information Resource performing correctly or on schedule.

The UNLV Payroll/Personnel System, the campus data network and the telephone and public safety communication systems should be considered Essential systems at all campuses. An example of an EIR that is likely to be considered Essential by a campus is a medical center's or students medical records system.

The same EIRs may be designated Essential, Required, or Deferrable depending on the period of inoperability. For example, Monthly financial reporting may be deemed Deferrable by a campus, but financial reporting at fiscal year-end would be considered Essential.

All Departments and Campuses must include all Essential EIRs in an appropriate Disaster Recovery Plan.

The designation Essential, Required, or Deferrable may be applied to various types of EIR. Thus, for example, these

guidelines also refer to Essential applications, or Required servers.

A checklist (**Risk Characteristics - Criticality Checklist**) is contained in this document that will provide assistance in determining which data falls into which category.

D. Summary Chart. The security requirements of Data Sensitivity and EIR Criticality are summarized below:

Sensitivity	Electronic Information Resource Criticality		
	Essential	Required	Deferrable
<i>Restricted</i>	<ul style="list-style-type: none"> Requires access security; Must be in Disaster Recovery plan 	<ul style="list-style-type: none"> Requires access security; May be in Disaster Recovery plan 	<ul style="list-style-type: none"> Requires access security; Need not be in Disaster Recovery plan
<i>Unrestricted</i>	<ul style="list-style-type: none"> Minimal security required; Must be in Disaster Recovery plan 	<ul style="list-style-type: none"> Minimal security required; May be in Disaster Recovery plan 	<ul style="list-style-type: none"> Minimal security required; Need not be in Disaster Recovery plan