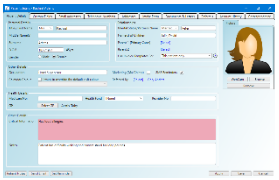
Appendix B – Example of Assigning Risk to a Data Set

Calculating Risk Levels

Risk levels are calculated by the impact (to the University) of a potential event/threat for the three security objectives. Each information item is reviewed by the "Security Objectives" presented on page 9 and a **Low**, **Moderate**, or **High** risk assigned to the Confidentiality, Integrity, and Availability of the information item reviewed. The assigned risk follows the information item regardless of its form including paper or digital to the point where it is transmitted, processed, or stored including file drawers, desks, application servers, database servers, a user's desktop or tablet, and cloud based computing solutions.

Examples:

Patient Health Record would be scored **High for Confidentiality**, **High for Integrity** (an altered record could cause catastrophic results), and **Low for Availability** if it was a backup record. ***The final risk would be High*** since that was the highest risk assessed for the three security objectives.



Class Syllabus might be assessed with a **Low for Confidentiality**, a **Moderate for Integrity**, and a **Low risk for Availability**. In this case, the overall ***risk rating would be Moderate*.**

Student Financial Aid Record could be assessed as **High for Confidentiality**, **High for Integrity**, and **High for Availability**. The ***final risk level would be High***.

My Finances

Financial Aid | Student Accounts | FSUCard

Consumer Information
Federal Work Study Information
New and Noteworthy
Office of Financial Aid Website
Satisfactory Progress
Scholarship Information
[+] View Financial Aid Awards/Status

General Campus Maps might be assessed as **Low for Confidentiality**, **Low for Integrity**, and **Low for Availability**. The ***overall risk rating would be Low***.

Potential Impact -->

Security Objective	**Low**	**Moderate**	**High**
Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary university information.	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Integrity - Guarding against improper information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious adverse effect on organizational** operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.
Availability - Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have **a serious adverse effect** on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

Appendix C – Example of Mapping Logical and Physical Controls to Information or Application

Data Set/Application Description	FSU Class	Risk Level	How are data/information/systems/databases safeguarded?
Unit-Academic Affairs	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring, Security, Alerts, Advisories, and Directives
Unit-Accounting	Private	Medium	User Account Management, Malicious Code Protection, Information System Monitoring, Baseline Configuration
Unit-Admin Dean's Office	Private	Medium	Transmission Confidentiality and Integrity, Public Key Infrastructure Certificates, User Account Management
Unit-Advising	Public	Low	User Account Management, Spam Protection, Security, Alerts, Advisories, and Directives
Unit-RTED	Protected	High	Cloud Service-Vendor controls for unit information are defined in the university security and privacy terms and conditions for contracted services (Controls for Unit Computing Devices Accessing Cloud Services) User Account Management, Security Awareness and Training Policy and Procedures, Physical Access Controls
Unit-Database	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring
Unit-Dean's Office	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring
Unit-Faculty Records	Private	Medium	User Account Management, Information Handling and Retention, Malicious Code Protection, Information System Monitoring, Monitor Security, Alerts, Advisories, and Directives
Unit-BCC Office	Public	Low	User Account Management, Malicious Code Protection, Information System Monitoring, Monitor Security, Alerts, Advisories, and Directives
Unit-Graduate Office	Protected	High	User Account Management, Security Awareness and Training Policy and Procedures, Software, Firmware, and Info Integrity(Vulnerability Management, Secure Baseline Server Configuration