Information Resource Risk Assessment Guideline
Syracuse University – Information Technology and Services
Information Security Guideline – G0102

1.0 Scope
This document covers all information technology assets that store, transmit or process SU data.

2.0 Purpose
The purpose of this document is to provide a consistent process and approach for assessing the risk introduced by a particular IT asset by not complying with an external requirement, SU policy, ITS standard or guideline, or not mitigating of an identified vulnerability.

It should be noted that many factors can affect a risk assessment. This guideline attempts to identify, quantify or qualify only the most common factors. It is the role of the Information Security Officer (ISO) and the individual requesting the assessment to evaluate other less common factors to determine a realistic risk score.

3.0 Guideline
NOTE*: While this document attempts to describe the method SU has adopted to assess an Information Security risk, the process itself is simplified by opening an issue in the "Information Risk Assessment" (IRE) project on Orange Tracker. See section 5.0.*

In order to assess the risk presented by a particular system, the following items must be quantified.

1. **Data Classification Score (See section 3.1)**: Determined by the identifying the highest level classification of data that is stored or processed on the system being assessed as per the *Syracuse University Information Security Standard*.
2. **Data Exposure Score (See section 3.2)**: Determined by evaluating the overall exposure of the data housed on the system or service being assessed.
3. **Admin Control Score (See section 3.3):** Determined by evaluating the administrative control of the system or service being assessed.

Once these three components are identified, the asset's **Threat Exposure Score** can be calculated by the Information Security department using the following equation:

Threat Exposure Score = Data Classification Score * (Data Exposure Score + Admin Control Score)

A **Vulnerability Score** is also applied arrived at as follows:

- **High, Medium** or **Low** as provided by the weekly InfoSec vulnerability scans. (Scores labelled "critical" are considered "high" for this process)

- **High** for any external requirement, SU policy, or ITS standard or guideline that an exception is being sought for.
- A value of **High, Medium** or **Low** to be determined by the ISO in conjunction with the school or unit seeking the exception if the other scoring methods do not make practical sense.

The combination of the **Threat Exposure Score** with the **Vulnerability Score** will then provide a qualified **Risk Score** of **CRITICAL, HIGH, MEDIUM**, or **LOW**. Based on the **Risk Score**, the individual requesting the exception or extension will need to seek and obtain the appropriate approvals. *Note: Approvals are tracked via the active IRE issue in Orange Tracker.*

Required Approvals

- RISK SCORE = LOW: Unit's IT Director
- RISK SCORE = MEDIUM: Unit's IT Director and DDD
- RISK SCORE = HIGH: Unit's IT Director, DDD, ISO
- RISK SCORE = CRITICAL: Unit's IT Director, DDD, ISO, CIO

3.1 Quantifying Data Classification Score

A risk assessment is not complete without classifying the data on the system to be protected. Based on the type of data as defined by the *Syracuse University Information Security Standard*, the **Data Classification Score** is as follows:

Type of Data	**Data Classification Score**
Confidential or federally funded research data	4
Enterprise	2
Public	1

3.2 Quantifying Data Exposure Score

Risk assessments must also include an evaluation of the exposure/availability of the information in question. We have classified assets based on their data's exposure as follows to determine the **Data Exposure Score**:

Asset Availability	**Data Exposure Score**
External /Internet service provided available to large number of users *In general, vulnerable **systems** or **services** that are publically available to the Internet.*	4
External/ Internet available	3

*In general, vulnerable **services** that are available to off campus users with some form of access control in place.*	
Internal Campus Available/To small number of users *In general, vulnerable **systems** or **services** that are available to campus system or user.*	2
Firewalled/Exposure Limited with other means like 2Factor authentication etc. *In general, vulnerable **systems** or **services** that are restricted or protected by some method other than username/password such as strict firewall rules, 2 factor authentication, etc…*	1

3.3 Quantifying Admin Control Score

The Admin Control Score is an attempt to use the job function and/or the skill set of the individual(s) managing a system or service in assessing risk. Full time IT staff members are expected to spend more time and have more background in managing a system than a non-IT staff member who is managing a system as an additional duty. These roles imply a higher or lower overall risk to the data housed on the system.

Asset Control	**Admin Control Score**
Staff/Faculty/ Student Managed	3
Staff/Faculty/Student Managed with oversight from ITS/DSP Admin	2
ITS/DSP Managed	1

4.0 Risk Score

Using the **Threat Exposure Score** described above in conjunction with the **Vulnerability Score** from the weekly vulnerability scans or non-compliance, the matrix below is used to determine a final, qualified **Risk Score** with the value of **CRITICAL, HIGH, MEDIUM** or **LOW**. The **Risk Score** is used to determine who must "sign off" on the exception or extension request.

Vulnerability Score →

Threat Exposure ↓

Vulnerability / Threat	Low	Medium	High
Low (2-5)	LOW RISK IT Director Approval	LOW RISK IT Director Approval	MEDIUM RISK DDD and IT Director approval
Medium (6-12)	LOW RISK IT Director Approval	MEDIUM RISK DDD and IT Director approval	HIGH RISK ISO, DDD and IT Director Approval
High (16-28)	MEDIUM RISK DDD and IT Director approval	HIGH RISK ISO, DDD and IT Director Approval	CRITICAL RISK CIO, ISO, DDD and IT Director Approval

5.0 Work Flow

By opening an issue in the Information Risk Assessment (IRE) project on Orange Tracker and filling out the required fields, a requester initiates a workflow with the Information Security Department. The workflow is described in the Answers document "*Information Risk Assessment Workflow*" located at https://answers.syr.edu/display/infosec101/Information+Risk+Assessment+Workflow

6.0 Referred Documents, Web Pages and Contact Information

Item	Location/Info
Answers Document: Information Risk Assessment Workflow	https://answers.syr.edu/display/infosec101/Information+Risk+Assessment+Workflow
Standard: *Syracuse University Information Security Standard*	http://its.syr.edu/infosec/docs/standards/ITSecurity-standard.pdf
Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.1
Effective Date:	Dec 01, 2014
Date of Last Review	May 23, 2016
Date of Next Mandatory Review	May 23, 2017