



P U B L I C S E R V I C E S

Risk Assessment Methodology and Reporting Guidance

February 7, 2002

Brian Sizemore

bsizemore@kpmg.com

Brian Fuller

brianfuller@kpmg.com

OCIO contacts:

Andrew Boots

Bob Ingwalson

Bob Clayton

- At 6:37 pm a man enters the ATM room. He inserts his card, inputs his P.I.N. and attempts a transaction.



- To his surprise no transaction has occurred and his card has been captured. He's confused as to why this happened.



Risk Assessments in Everyday Life

- An unknown man enters the room and offers assistance.



- The man offering his assistance states that this happened to him before, and convinces the customer that he will be able to retrieve his card if he enters his P.I.N. while holding down both the “cancel” and the “enter” buttons.



- After several attempts at this, the customer is convinced that the machine has captured his card. Both he and the man who “helped” him leave the room.



- Now lets turn back the clock about 5 minutes. Recognize this guy?

What we didn't show you was the "helper" inserting a simple device into the ATM slot that captures the card of the next person who uses it.



- Now let's go back to our scenario ...

Satisfied that the coast is clear, the thief returns to retrieve the card that has been captured by his trap. He not only has the customer's card but now he has the P.I.N. too.



- Armed with the card and the man's P.I.N. the thief was able to withdraw \$1000 from the account.



Interpret ED guidance for Risk Assessment completion.

■ Assumptions:

- Risk Assessments due to SFA CSO no later than 4/8/02.
- All assessments must be conducted by an independent assessor (per NIST, OMB and ED).
- Many paths to completing a Risk Assessment.

■ Training Outcome:

- Tools needed to fill in Risk Assessment Matrix and complete Risk Assessment Report.

- **Risk Assessment Template**
- **Risk Assessment Matrix**
- **PowerPoint Presentation**

Presentation material will be sent soft copy after training.

Why a Risk Assessment?

- GISRA requirement
- System Owners need to know
- Most important –

It makes good business sense!!

- Define System Boundaries
- List System Vulnerabilities
- Establish Threats and Threat Agents
- Gauge Impact
- Determine Likelihood
- Calculate Level of Risk

- **What makes up a system's boundary?**
 - Where is data handled?
 - When is data part of system vs. when not?
 - When is it government data vs. when not?

- **Where do I get this information?**

- **Why do I need to define system boundaries?**
 - Scope – Avoid assessing assets outside of your control

- **Where do I get this information?**
 - NIST Self-Assessment
 - Baseline Security Requirements questionnaire
 - Recent Audits
 - Physical or Network Testing

- **Organize vulnerabilities within MOTA:**
 - **M**anagement
 - **O**perational
 - **T**echnical
 - **A**ministrative

- **Number vulnerabilities M1/O1/T1/A1**

- **Assuming abundant resources and capabilities, who/what could exploit a given vulnerability?**

- **Select from one of the following threat categories:**
 - **Natural**
 - **Environmental**
 - **Human**
 - **Administrative**

- Without considering security controls, how could the threat exploit a known vulnerability?
- Where do I go for this information?

Impact	System Criticality		
Information Sensitivity	<i>Mission Critical</i>	<i>Mission Important</i>	<i>Mission Supportive</i>
<i>High</i>	High	High	Medium
<i>Medium</i>	High	Medium	Medium
<i>Low</i>	Medium	Medium	Low

- Given countermeasures, how likely is it that the Threat could exploit the Vulnerability?

Threats	Capabilities	Countermeasures
Natural	Location Based H/M/L	Building codes, cold sites
Environmental	History Based H/M/L	Back-ups, redundancies
Human	Access based H/M/L	Firewalls, guards, IDS, audit logs, RoB
Administrative	H	Documentation

Determine Likelihood (continued)

Likelihood	Countermeasure Effectiveness		
Capability	<i>High</i>	<i>Medium</i>	<i>Low</i>
<i>High</i>	Medium	High	High
<i>Medium</i>	Low	Medium	Medium
<i>Low</i>	Low	Low	Medium

Calculate Risk

Risk	Impact		
Likelihood	<i>High</i>	<i>Medium</i>	<i>Low</i>
<i>High</i>	High	High	Medium
<i>Medium</i>	High	Medium	Low
<i>Low</i>	Medium	Low	Low

Prioritize by:

1. Within a MOTA category
2. Risk Level
3. Immediacy of vulnerability
4. Time required to complete countermeasures

List Recommended Additions to Countermeasures

- **What actions could...**
 - Neutralize the vulnerability?
 - Remove the threat?
 - Lessen the impact?

- **Keep countermeasures reasonable, but do not factor costing requirements... yet.**

List Vulnerabilities



When the thief offers to help the ATM user, the user himself creates the vulnerability by allowing the thief to watch him input his P.I.N.

This would be considered an operational vulnerability.



VULNERABILITY

Establish Threats and Threat Agents



The thief exploits the operational vulnerability. He captures the card and obtains the P.I.N.

The threat in this scenario would be human, specifically a physical threat.



THREAT

Gauge Impact



The thief exploited the vulnerability utilizing the stolen card and P.I.N to withdraw money from the victim's account. The impact is high because of the sensitivity of the P.I.N information and account information.

The impact to the victim is a loss of at least \$1000 and a potential for more unauthorized withdrawals.



IMPACT = HIGH

Determine Likelihood



- Capability:**
- Human – Physical
 - Easy to do and easy to make
- = HIGH**

- Countermeasures:**
- Limit Total Transaction Amounts
 - Use of Video/Security Cameras
- = MEDIUM**



LIKELIHOOD = HIGH

Calculate Risk

Impact + Likelihood = Risk

	Impact		
Likelihood	<i>High</i>	<i>Medium</i>	<i>Low</i>
<i>High</i>	High	High	Medium
<i>Medium</i>	High	Medium	Low
<i>Low</i>	Medium	Low	Low

High Impact + High Likelihood =

HIGH RISK VULNERABILITY

■ Fill in provided template fields

- System name
- Assessors
- Details from Departmental Inventory sheets, Security Plan, etc.
- Write over any gray fields

1.1 BACKGROUND

Insert System Description from Executive Summary

1.2 PURPOSE

The purpose of this report is to provide the Department and SFA management with an assessment of the adequacy of the management, technical, operational and administrative security controls used to protect the confidentiality, integrity, and availability of **Insert System Name**. This risk assessment report identifies threats and vulnerabilities applicable to **Insert System Name**; the impact associated with these threats and vulnerabilities; the likelihood that a vulnerability will be exploited; countermeasures in place to mitigate the risk; and the existence of any residual risk.

This report documents the risk assessment activities that **Insert Contractor Name** performed from **Insert Month and Day, 2002** to **Insert Month and Day, 2002**, and will help SFA management understand the security posture of **Insert System Name** and its risk exposure. The risk assessment is part of SFA's continuing effort to ensure compliance with Federal policies and guidance as well as the Department's IT Security Policy.

1.3 SCOPE

This risk assessment is limited to the **Insert System Name**. **Insert description of risk assessment scope**. For example, "which is a Microsoft Access '97 database, its host general support system (GSS) EDNet server ROB3FPR02\Groups\OEP, and the remote access server (RAS). The servers are housed in Room 1234 at the Department's ROB3

Things to Provide Contractors

- **All training material**
- **Department of Education GSS/MA Inventory Submission Forms**
- **Completed 2001 NIST Self-Assessment**
- **Any additional vulnerability testing conducted since April 2001**