



# **Student Financial Assistance HR Modernization**

## **Risk Assessment Report**

**An Evaluation of the SFA HR Modernization  
Security and Privacy Risk Management and Control Environment  
With Recommendations for Improvement**

Prepared by:



**October 18, 2001**

# TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY .....</b>	<b>3</b>
BACKGROUND & METHODOLOGY .....	3
FINDINGS .....	3
<b>BACKGROUND .....</b>	<b>5</b>
TASK OVERVIEW AND SCOPE .....	5
SYSTEM OVERVIEW .....	6
RISK ASSESSMENT BACKGROUND .....	9
<b>CONCLUSIONS .....</b>	<b>51</b>

# Executive Summary

## Background & Methodology

KPMG Consulting evaluated the risks inherent in the HR Modernization (HR Mod) project supporting the Office of Student Financial Assistance's (SFA) core business process. The HR Mod project's purpose is to provide overall savings and increased performance capabilities in SFA's Human Resources department by outsourcing the support applications into an Application Service Provider (ASP) model run by Jamcracker, Inc.

To accomplish this task, KPMG Consulting security analysts collected information on Jamcracker's systems, network architectures, operations, physical environment where hardware is located, data elements and business processes. The approach used to gather this information included inquiries to Jamcracker and SFA Modernization Partner management, staff and information technology contractors, and a thorough documentation review of Jamcracker's security policies and procedures. The information was then analyzed to evaluate the maturity of Jamcracker's risk management model and to determine how well that model was being applied at the system level for the HR Mod project.

The standard used to measure the maturity of SFA risk management was derived from guidance provided by the General Accounting Office (GAO), summarized below in Figure 1; security and privacy standards contained in Appendix I and Appendix III of the Office of Management and Budget (OMB) Circular A-130; and National Institute for Standards and Technology (NIST) Special Pubs 800-14, 800-18, and 800-30. This measurement guidance was developed based on the Privacy Act of 1974 and the Computer Security Act of 1987.

## Findings

First and foremost, it must be understood that HR Modernization is launching as a pilot program with minimal users and supporting fairly innocuous data. A level of security risk determination is comprised of the likelihood of a threat occurrence balanced against the impact of that threat occurring. Due to the very nature of the pilot launch, any exploitation will have a very low impact to SFA as a whole, regardless of how likely the threat may occur. For this system, the likelihood of threats occurrence has also been minimized by the existing/planned system security controls, creating an overall risk level of low.

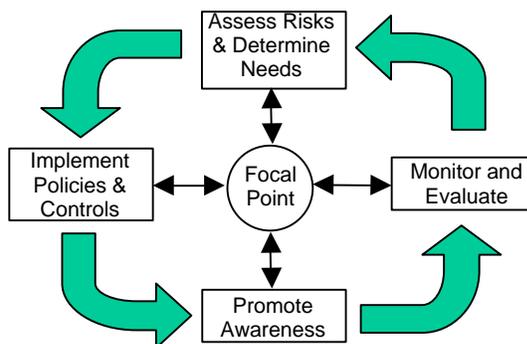


Figure 1: GAO Risk Management Cycle

The risks identified within HR Modernization are mostly administrative in nature, and should be fairly easy to incorporate in the near future. This is important, because as the pilot program is expanded to incorporate all SFA employees, and HR Modernization begins to incorporate additional ASPs, it will be vital to have a solid procedural foundation to support the additional risks inherent with more users and more data. Fortunately, the very aggregate model that Jamcracker relies upon makes it easy for new documented security procedures to be incorporated in this expansion. We recommend the following actions, in priority order:

1. Assign an SFA System Security Officer for HR Modernization.

2. Create explicit security requirements which provide precise standards with detailed examples of what is to be expected in data confidentiality and integrity controls.
3. Physically separate “Hot” and “Cold” production environments to allow immediate backup operations in the “Cold” environment.
4. Provide list of hardware and software used for HR Modernization for inclusion in the System Security Plan
5. Require background checks for all critical positions at Jamcracker before access to sensitive systems is permitted.
6. Increase expiration period for SFA user passwords from 30 days to 60-90 days.
7. Finish documentation of remaining Jamcracker security procedures.
8. Expand contingency plans to incorporate all possible types of incidents.
9. Incorporate relevant security portions of SFA SDLC Guidelines into future system modifications.
10. Develop SFA specific Rules of Behavior.

# Background

The Office of Student Financial Assistance (SFA) is an independent agency under the U.S. Department of Education (ED). SFA's mission is to manage disbursements of annual student aid appropriations. A distinct Human Resources department within SFA handles all HR related work at an enterprise level for all of SFA.

The HR Automation vision was created to provide a framework for the rapid deployment of "Best-of-Breed" Human Resource and Human Capital ASP systems, facilitate the automation of these core processes, and thereby support SFA's PBO transformation. Through this vision, SFA HR has taken a lead in establishing a direction for SFA to follow in using net-sourced applications. The SFA HR Automation vision utilizes an Aggregator model (Jamcracker) to connect multiple Application Service Providers (ASPs). Users access individual applications through the aggregator using a single sign-on. The HR functional areas that will be integrated into the aggregator and represented in the model include: classification/recruiting/staffing, performance management, knowledge management, skill/career development and training, payroll administration and benefits administration. These functional areas were targeted to be synergistic improvements to processes and/or systems currently provided by the Department of Education (or other Agencies), and to enable SFA to achieve its PBO goals using these new best-of-breed ASP solutions.

The security, privacy and risk management yardstick has already been established for Federal entities through laws, regulations, and standards. Relevant laws include the Privacy Act of 1974 and the Computer Security Act of 1987. These laws are implemented through regulatory guidance as follows:

1. The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, establishes policy. Procedural and analytic guidelines for implementing A-130 are provided in its appendices. The two appendices relevant to this task are A-130 Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*, and A-130 Appendix III, *Security of Federal Automated Information Resources*. Appendix I provides overall guidance for implementing the Privacy Act, while Appendix III provides overall guidance for implementing the Computer Security Act. Appendix III also points Federal managers to specific guidance relating to computer security that has been promulgated by the National Institute of Standards and Technology (NIST).
2. NIST has issued a series of publications that provide highly detailed guidance for establishing a secure environment in Federal automated information systems in accordance with A-130. These are: NIST Special Pub 800-12, *Introduction to Computer Security*, NIST Special Pub 800-14, *Generally Accepted Best Practices for Securing Information Technology Systems*, NIST Special Pub 800-18, *Guide for Developing Security Plans for Information Technology Systems*, and NIST Special Pub 800-30, *Risk Management Guide*.

An example of a government-wide risk management process is described in General Accounting Office (GAO) report GAO/AIMD-98-92, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk*, September 1998. This document describes a risk management model based on OMB and NIST policy and guidance. While OMB/NIST describe *what* to do to mitigate risks in automated information systems, the GAO risk management model describes *how* to do it.

## Task overview and scope

KPMG Consulting performed a risk assessment of the proposed HR Mod that will eventually be used by SFA to replace many of the existing human resource applications. This project was developed as a major application designed to support SFA's business processes. Our goal was to assess the inherent risks of the HR Mod system, evaluating how security controls could be improved in order to help protect the system from threats it could face upon entering production.

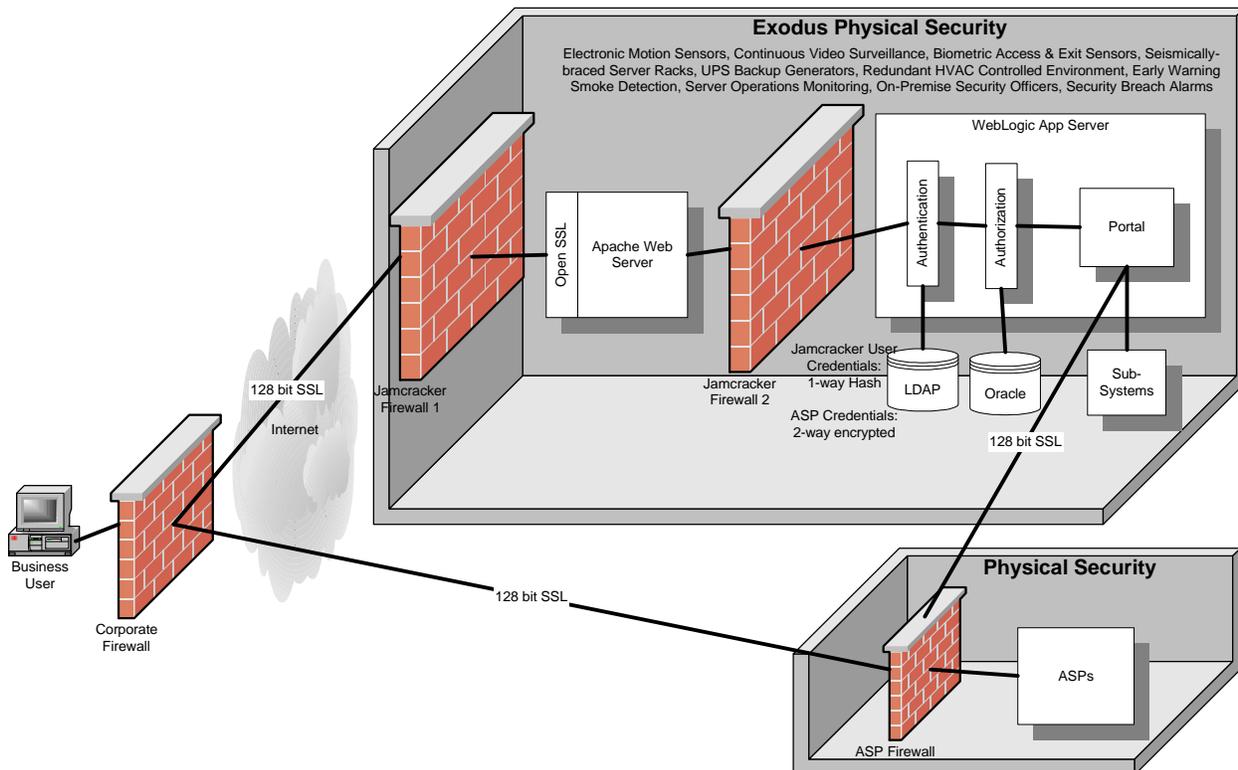
KPMG Consulting employed several methods for obtaining information. This included a review of system documentation, recommendations for and a review of suggested procedural documentation, and interviews and meetings with Jamcracker system management and security personnel, and Modernization Partner developers. This assessment did not include any physical testing or inspection of equipment.

The security system boundaries used for this assessment encompass the Jamcracker platform housed at Exodus Communications, Jamcracker HQ, and the communication links used between the Jamcracker platform and SFA employees as well as to all associated ASPs. The security capabilities of the ASPs themselves were not reviewed, as their practices will be held to their respective Service Level Agreements (SLAs) and contracts with Jamcracker. The SLAs and contracts themselves were reviewed for security content. For this assessment, only the content of the pilot ASP, Perform.com (a performance management database), was included. Future ASPs were examined only for their potential impact on the system's sensitivity and criticality analysis.

### System overview

The HR Mod project's goal is to replace existing HR support software with a common outsourced platform in order to reduce operating costs, support overhead, and application downtime. The replacement will occur in a phased rollout taking place over two years. See below for more details about the specific applications.

The primary functionality of Jamcracker in the HR Mod is to control the access of users to a series of separate human resource websites using an Aggregator model (Jamcracker) to connect multiple Application Service Providers (ASPs). Essentially, a user will log into the Jamcracker website using his/her e-mail name as the user identification and a Jamcracker password. Once authentication is complete, Jamcracker will determine which areas of the HR Mod the user is authorized access and show these options on the Jamcracker webpage. The user at that point can choose which website to visit and Jamcracker will redirect him/her to the new site and perform the log in functions at the new site for the user. No user information is kept at Jamcracker except for the authentication and authorization information.



Although the initial roll-out of HR Mod will only consist of Perform.com, a goal-setting and performance evaluation tool, it will eventually also include five other ASPs to be implemented in two separate roll-outs. The following gives a description of the different portals:

Portal	Description
Perform.com (Performance Management)	Goal setting, job reviews
Classification/Staffing/Recruiting	Job postings, job classification codes, resume submittal
Knowledge Management	Training information, HR policies and procedures, enterprise financial reports (FMS)
Benefits Administration	Available benefits, forms, online application for benefits
Skill/Career Development and Training	Training documentation, resources, career path info
Payroll Administration and Personnel Management	Pathway to FPPS for internal information transfer

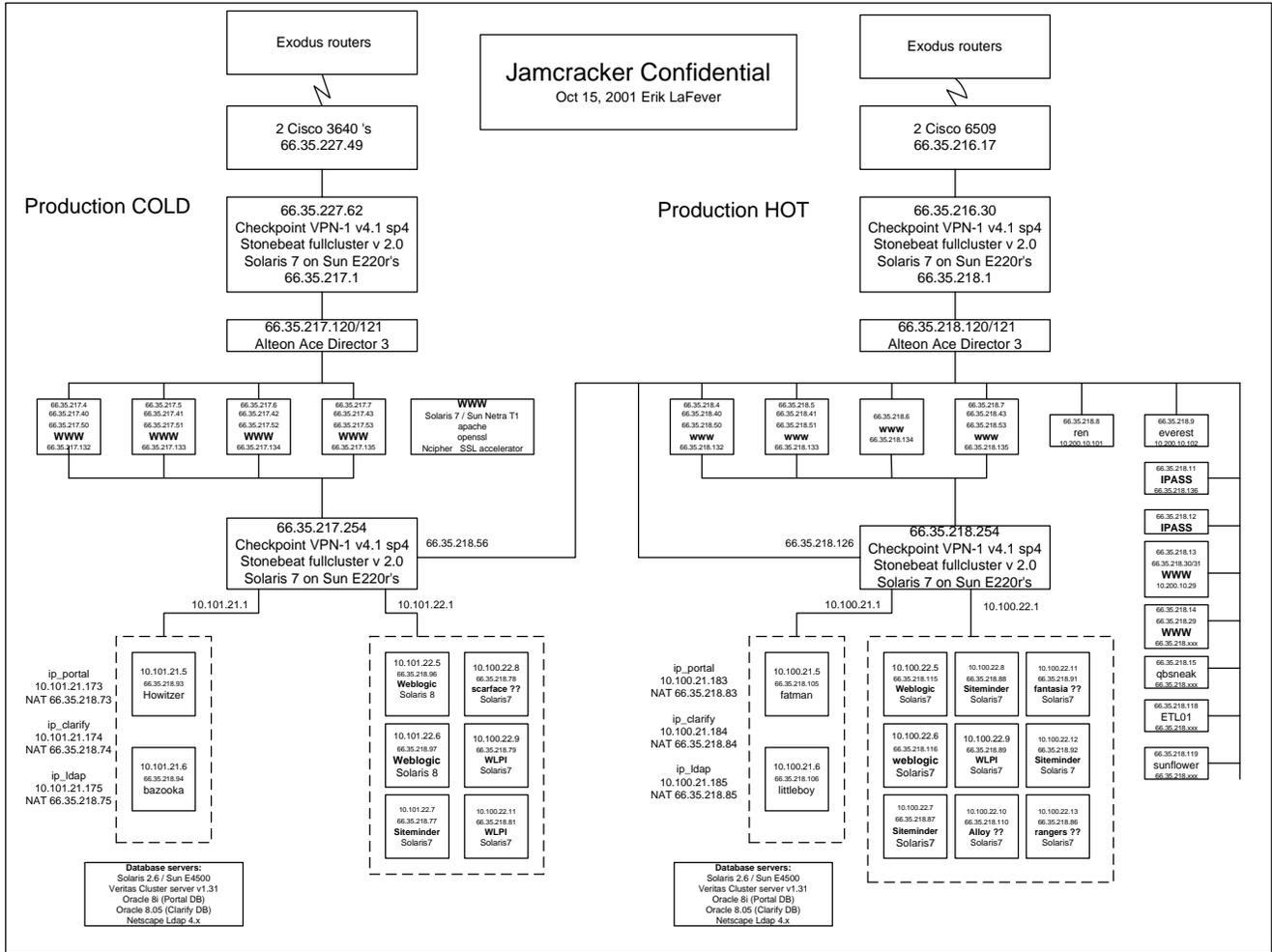
### System Description

The Jamcracker environment is a robust, redundant, multitiered network that is designed for maximum security and high availability. The network is comprised primarily of Sun Microsystems and Cisco Systems hardware and best-of-breed software providing the best service possible to the customers. In case of a full network operational failure, a cold production facility is available for automatic switchover after internal sensors have determined a catastrophic failure. See network diagram below.

The perimeter of the Jamcracker network is protected by a Cisco 3640 with advanced ACLs to filter inbound connections and Checkpoint VPN-1 clustered firewalls for high availability and immediate fail over capability. The Checkpoint firewall is configured to prevent all inbound connections except for those specifically authorized.

Users obtain their services via web browsers and connect to one of four multi-homed web servers running Apache on Sun Microsystems Netra T1 servers depending upon the load balancing calculations performed by an Alteon Ace Director. The Ace Director automatically routes the user's web requests to the web server that is capable of providing the fastest service. Additional hosts provide quality assurance testing locations used to run automated use case testing against the environment before new releases.

To protect the database servers from the rest of the network, another set of Checkpoint VPN-1 fullcluster firewalls are implemented to only allow HTTP, SSL, and SSH traffic to move between the web servers and the application and database servers. Additionally, network address translation (NAT) is used to protect the true IP addresses of the systems. Oracle 8i is installed on a set of clustered Sun Enterprise 4500s. Additionally, back-end systems host products from Weblogic and Siteminder to provide analysis of ASP traffic and usage.



Users will most likely connect with Jamcracker over the internet using either EDLan or the VDC as their Internet Service Provide, although users will be able to connect using any ISP from any location.

The Jamcracker platform is located at Exodus Communications in San Jose, California. Jamcracker corporate headquarters are located in Cupertino, California.

### Sensitivity/Criticality

The sensitivity/criticality analysis focused on the confidentiality, integrity, and availability requirements necessary for the different ASPs that will be associated with HR Mod. Each was given a rating of Low, Medium, or High in each field, with the aggregate determining the system's overall rating and the approach of the assessment.

Portal	Confidentiality	Integrity	Availability
Performance	Medium	Medium	Low
Recruiting	Low	Medium	Medium
Career Devt	Low	Low	Low

Benefits	Medium	High	Medium
Knowledge Mgmt	Medium	Medium	Low
<b>HR Mod</b>	<b>Medium</b>	<b>Medium/High</b>	<b>Medium/Low</b>

The most critical function for all of the different ASPs is to maintain the integrity of the data entered and stored within their databases, whether it be the goals that employees would be reviewed upon, the benefits available and requested by employees, or even the job postings for employment opportunities. Changes within that data or an inability to tell if the data had been changed would seriously compromise the capability of SFA to function properly. Likewise, confidentiality is an important role due to sensitive information such as Social Security information, health records, and payroll records. Only in certain circumstances is availability a large issue, such as during the open period for benefits. In most other cases, however, loss of system availability, while inconvenient, would not seriously affect SFA’s mission objectives, with (if necessary) paper records able to replace electronic during a down period.

### **Risk Assessment Background**

We used GAO’s Risk Management Cycle and NIST Special Pub 800-30 as the standards for measuring compliance with federal privacy and security guidance. We related the control areas from a NIST-compliant security plan to each of the four stages in GAO’s risk management cycle, a process called “binning,” and per NIST 800-30 created the threat-source/vulnerability pairs for each control area. A-130 Appendix I, A-130 Appendix III and security guidance contained in NIST Special Pub 800-14 and Special Pub 800-18 provided the specific standards against which we could measure SFA system compliance.

During our assessment, we examined the level of compliance in each issue/control area, taking into account the business process supported by HR Mod. A “stop light” grade was assigned to each issue/control area. Using this method, ‘red’ indicates either total non-compliance or serious shortcomings; ‘yellow’ indicates either less than full compliance or room for improvement, and ‘green’ indicates either sufficient or full compliance, although it does not mean there is no room for additional improvement. Grades were assigned subjectively; generally, any failure to fully measure up to the articulated standard was sufficient for a ‘yellow’ grade, while lack of evidence for compliance, or evidence of numerous shortcomings resulted in a ‘red’ grade.

In this task a vulnerability was considered to be anything that fell short of Federal guidance. However, we also looked beyond compliance to consider what other measures might be taken to improve system level risk management. *For this reason there are a number of instances where opportunities for improvement are provided at the system level for control areas that have been given a green stoplight.*

In summary, the goal of this document is to allow SFA managers to take in at a glance the overall maturity of their risk management process, to understand their current level of compliance with OMB guidance, and to provide useful, cost-effective recommendations for improving risk management processes. A diagram of a mature risk management model follows, with links to the control areas analyzed in this assessment.

# Overview of SFA System Risk Management Maturity

[General Description/Purpose](#)  
[System Environment](#)  
[System Interconnection/Information Sharing](#)  
[Applicable Laws or Regulations](#)  
[General Description of Information Sensitivity](#)  
[Risk Assessment and Management](#)  
[Review of Security Controls](#)

[Rules of Behavior](#)  
[Security life cycle planning](#)  
[Authorize Processing](#)  
[Personnel Security](#)  
[Physical and Environmental Protection](#)  
[Production, Input/Output Controls](#)  
[Contingency Planning](#)  
[Application Software Maintenance Controls](#)  
[Data Integrity/Validation Controls](#)  
[Documentation](#)  
[Identification and Authentication](#)  
[Logical Access Controls](#)  
[Public Access Controls](#)

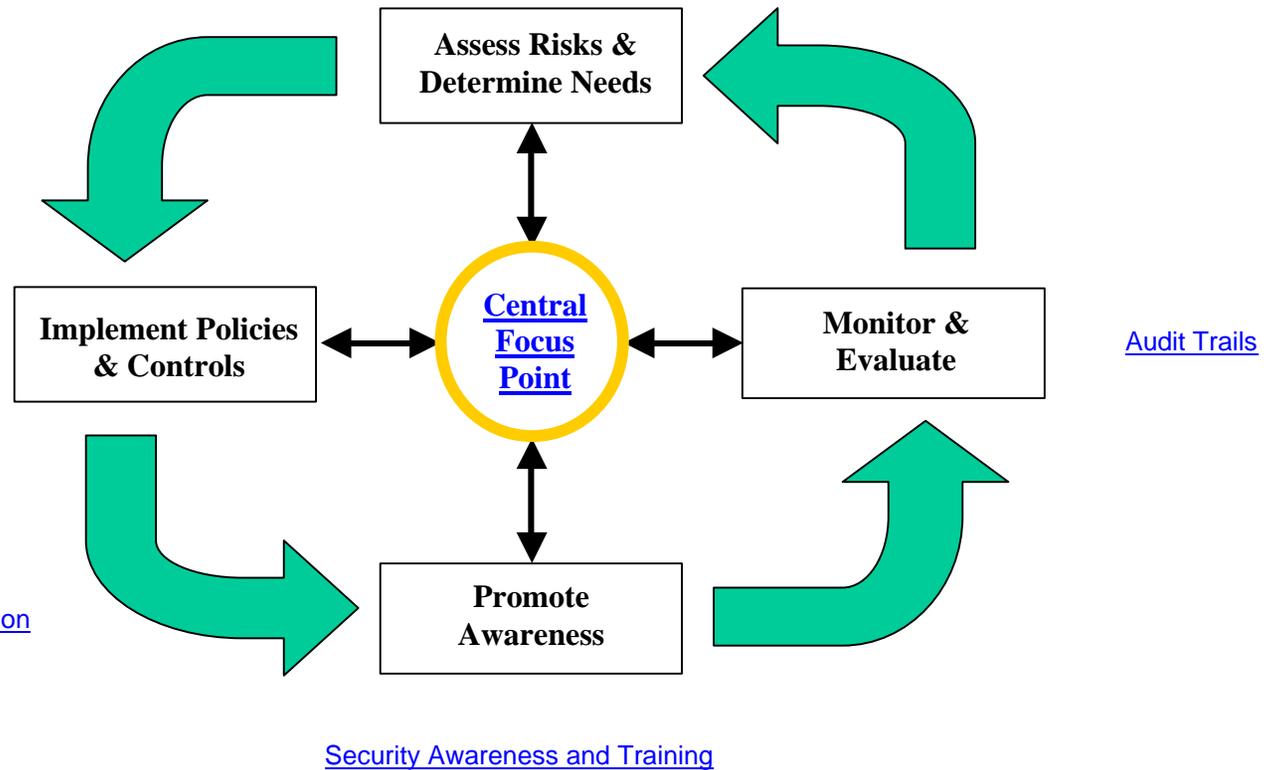


Figure 1: SFA System Risk Management Maturity Overview

**Standard:** [OMB A-130](#), [NIST Special Pub 800-14](#)

A central security program... should have the following:

- Stable Program Management Function
- Existence of Policy
- Published Mission and Functions Statement.
- Long-Term Computer Security Strategies
- Compliance Program
- Intraorganizational Liaison
- Liaison with External Groups

By definition, major applications are high-risk and require special management attention. It is important, therefore, that an individual be assigned responsibility in writing to assure the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

#### Significance in the SFA Environment:

**Threat:** Ambiguity in security policies, procedures, or management roles, leading to insecure practices with a lack of overall responsibility.

**Impact:** None of the security program functions noted above can be effective if SFA management lacks the knowledge basis to fulfill their responsibility of overseeing the risk management processes. Most SFA managers and security officers do not have security backgrounds; in the near term only training can provide them with the needed knowledge baseline. The best source for that training comes from learning the underlying security policies of a given system.

### **Current Status:**

Currently, both Jamcracker and SFA are in the midst of improving their security policies and procedures. SFA has a set of security policies currently in review before being distributed throughout the organization. Jamcracker has released its “Corporate IT Security Policy” which establishes their enterprise-level security, and is currently documenting the pertinent procedures that will flush out their policies. Both are committed to ensuring compliance to their policies through the use of internal and external audits of their controls.

Although Jamcracker has an established head of security, SFA doesn’t have a System Security Officer (SSO) assigned to HR Mod, nor a person assigned temporarily. Once the current hiring moratorium has been lifted, SFA could hire a permanent SSO.

### **Opportunities for Improvement:**

Both Jamcracker and SFA need to continue documenting their policies and procedures so as to provide a complete framework with which to manage risks. Additionally, SFA needs to formally assign the SSO role to an interim SSO until a permanent SSO can be hired. The system owner should make this assignment in writing and the letter should be included in the system security plan.

Green

## General Description/Purpose

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

Present a brief description (one-three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, and crop reporting support).

If the system is a general support system list all applications supported by the general support system. Specify if the application is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements are met.

### Significance in the SFA Environment:

**Threat:** An unclear system description/purpose leads to system bloatage, inaccurate system boundaries, and offers no foundation from which to assess threats to the organizational mission.

**Impact:** Accurate, complete system descriptions in system security plans provide several long term benefits. System descriptions are required in many federal documents – A-130 reviews, security audits, certification and accreditation documents, etc. By providing a full, complete, and accurate system description in the system security plan, all other documents requiring this information can draw from a single source. This reduces the potential for conflicting information across several reports, helps to reduce the risk that out-of-date information is carried forward into future documentation, reduces the amount of time spent in duplicative information-gathering efforts, and provides managers and security staff with a single, authoritative source of information.

### Current Status:

An accurate general description and purpose has been created for HR Modernization as well as for Jamcracker. This description is paraphrased in most documentation, providing consistency throughout the system.

### **Opportunities for Improvement:**

Ensure the continued consistent use of established general descriptions and purpose passages for all future documentation. Update the description as HR applications are added to the Jamcracker platform.

**Yellow**

## System Environment

[Back to Risk Cycle Illustration](#)

### Standard: **NIST Special Pub 800-18**

Provide a general description of the technical system. Include any environmental or technical factors that raise special security concerns (dial-up lines, open network, etc.)

Describe the primary computing platform(s) used and a description of the principal system components, including hardware, software, and communications resources.

Include any security software protecting the system and information.

### Significance in the SFA Environment:

**Threat:** Unclear system descriptions hamper system reconstruction during disaster recovery, incomplete software patches or hardware maintenance, and imperfect system security coverage.

**Impact:** Remarks made in the [General Description](#) section apply here as well.

### Current Status:

General descriptions of the system's technical architecture and make-up are available and in good order. Detailed network architecture diagrams, including manufacturers and model numbers of equipment, have recently been created and distributed. A compiled list of system hardware, software, and communications resources is not currently available, but is being addressed by Jamcracker and will be corrected shortly.

### Opportunities for Improvement:

Ensure that network architecture diagrams are kept up-to-date with as much detail included as possible. Also, make sure the system security plan is kept up-to-date with any changes in software versions or hardware modifications. Add the complete list of hardware, software and communications to the security plan once completed.

**Red**

## System Interconnection/Information Sharing

[Back to Risk Cycle Illustration](#)

### Standard: **NIST Special Pub 800-18**

OMB Circular A-130 requires that written management authorization (often in the form of a Memorandum of Understanding or Service Level Agreement,) be obtained prior to connecting with other systems and/or sharing sensitive data/information. It is required that written authorization (MOUs, SLAs) be obtained prior to connection with other systems and/or sharing sensitive data/information. It should detail the rules of behavior that must be maintained by the interconnecting systems. A description of these rules must be included with the security plan or discussed in this section.

### Significance in the SFA Environment:

**Threat:** Vague rules within the MOUs or SLAs create loopholes in which security requirements can be unintentionally relaxed without notice or legal ramifications, potentially causing harm to the system.

**Impact:** Formal MOUs or SLAs that define service levels and standards of behavior increase management's confidence that information security and privacy policies and standards are being followed in areas outside SFA's control. If a system's boundaries can be defined by the business process it supports, then many SFA *system* boundaries are outside SFA's *control* boundary (e.g., on institution campuses). Formal chain-of-trust agreements with these external agencies help to extend SFA management's control boundary closer to system boundaries. While implementing compliance monitoring mechanisms may prove difficult or impractical, SFA management may at least have the confidence that proceeds from an agreed-upon set of technical and privacy/security standards.

For HR Modernization in particular, strong SLAs are vital to the security of the system. SFA will be relying on the security requirements laid out in the SLA between SFA and Jamcracker to set the security expectations for the ASPs. Because these ASPs will be where SFA's data will reside, it is imperative that explicit security requirements are stated in the SLA so that SFA's data is protected adequately.

### **Current Status:**

The current SLA provides very good and concise specifications for the availability requirements for the HR Modernization project. Additionally, a recent addendum provides specific guidance for how to adhere to Privacy Act requirements. This will be very valuable when ASPs that contain Privacy Act data are added to the system. What the SLA lacks, however, are details on the specific confidentiality and integrity controls that are required for Jamcracker and therefore all ASPs. Instead, it relies on the boilerplate phrase, “Contractor through its service provider will use commercially reasonable efforts to enforce industry standards for network, data and physical site security in order to protect the privacy and confidentiality of the SFA’s data and to prevent access to such data by unauthorized users with respect to the Services and Other Services.” This imprecise phrasing provides enough ambiguity that an exploited weakness in an ASP’s security plan could easily be dismissed as still being above “industry standards.”

### **Opportunities for Improvement:**

Precise standards with detailed examples of what is to be expected should be included in the next modification to the SLA. This modification should be made before the next ASP is added to the HR Modernization project.

**Green**

## Applicable Laws and Regulations

[Back to Risk Cycle Illustration](#)

### Standard: [NIST Special Pub 800-18](#), [Privacy Act of 1974](#), [OMB A-130 Appendix I](#)

List any laws, regulations, or policies that establish specific requirements for **confidentiality**, **integrity**, or **availability** of data/information in the system.

Comply with the provisions of the Privacy Act, Appendix I of A-130

### Significance in the SFA Environment:

**Threat:** Not knowing which laws are applicable makes it impossible to self-assess a system's compliance and ensure adequate measures have been taken to protect information.

**Impact:** SFA collects and maintains sensitive Privacy Act data, including name, address, social security number, birthdate, as well as financial information, including income and assets, and tax information, relating to a student loan applicant and the applicant's family. It is unlawful to collect, use, or disclose privacy data except in accordance with the authorized uses for which the data was collected. Unauthorized disclosures or compromise of privacy act data could result in severe adverse consequences to the applicant, and adverse public reaction and/or liability for the agency that improperly collected, used, or disclosed the data.

### Current Status:

Currently no Privacy Act data is stored in the HR Modernization system. Future ASPs, however, will interact with Privacy Act information, and will have to be protected in accordance with the applicable regulations.

### Opportunities for Improvement:

Before ASPs that contain Privacy Act information are activated, a privacy assessment should be performed to ensure legal compliance. Additionally, explicit instructions should be provided to the affected ASPs, as mentioned in [System Interconnection/Information Sharing](#).

**Green**

## Description of Information Sensitivity

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

Describe, in general terms, the information handled by the system and the need for protective measures. Relate the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicate if the requirement is: **High, Medium, or Low**.

Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.

### Significance in the SFA Environment:

**Threat:** Misappropriation of security assets and funding may be assigned to low-ranking threats while higher ranking requirements are under-protected or neglected.

**Impact:** A security model that categorizes information sensitivity and assigns information ownership is a keystone activity in establishing a control environment. SFA systems process, store and transmit a great deal of sensitive information, including information protected by the Privacy Act and other financial information that must have its integrity maintained. Safeguarding the privacy and security of sensitive information requires all managers, system operators, and users to proceed from a common understanding of varying levels of information sensitivity, as well as the protection standards that apply to each.

### Current Status:

No initial sensitivity analysis was conducted for HR Modernization until this risk assessment was conducted (see [Sensitivity/Criticality](#)). Our analysis showed that overall, security efforts were being focused on the areas with the highest need for security, with the exception of the emphasis on availability and lack of any other specific security requirements in the SLA (see [System Interconnection/Information Sharing](#)).

### **Opportunities for Improvement:**

A sensitivity/criticality assessment should be performed after the determination of any major change to the system, especially the addition of a new ASP. An initial assessment took place in this risk assessment using what was currently known about the future ASPs, but that assessment should be kept up-to-date as the specifications for the ASPs change.

Green

## Risk Assessment and Management

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

### Significance in the SFA Environment:

**Threat:** Management ignorance or underestimation of inherent risks of a system

**Impact:** Risk assessment is another keystone activity in the GAO risk management cycle. The goal of risk management is to establish an effective and cost-beneficial control environment in which information is protected in a manner commensurate with its sensitivity and value. Risk assessment should provide a baseline understanding of vulnerabilities, threats, and relative risk; this in turn may serve as a reasonable basis for making management decisions on what controls and risk mitigation measures are appropriate in a given systems environment. Without this baseline systems managers cannot make *deliberate* risk decisions. In consequence, resources may not be efficiently allocated; managers may spend too much (or too little) time, effort and expense mitigating risks. Over-compensating for risk does not make good business sense, particularly in the resource-constrained government environment. But neither can a business case be made for under-compensating for risk; a single incident can easily wipe out whatever might have been 'saved' by not employing the proper risk mitigation measure. In addition, SFA managers have a public-service obligation to take measures to maintain public confidence in government. Privacy and security breaches may undermine this confidence; this as much as anything else recommends SFA take a purposeful approach to risk management.

### Current Status:

This risk assessment serves to allow a green stoplight for HR Mod, however, as new ASPs are added and improvements made to the system, an impact evaluation to the system's overall risk level should be made. This does not necessarily mean an additional independent risk assessment, but rather an analysis to ensure that any additional risks taken on by the modified system are acceptable. Jamcracker has scheduled risk management activities to include penetration tests and independent reviews to determine how their platform's security can be approved.

### **Opportunities for Improvement:**

The owners of HR Mod need to ensure that future risk assessments occur after any major modification to the system or to the organizations policies and procedures, and at least every three years. Whenever a new ASP is added to the system, an assessment of additional risks that the system will be accepting, and whether those risks are adequately controlled, should also take place.

Green

## Review of Security Controls

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application.

### Significance in the SFA Environment:

**Threat:** Inappropriate assignment of security resources; vulnerabilities created by lack of controls, improper controls, or controls that are no longer effective as system threats change over time.

**Impact:** Risk assessment and controls reviews are very closely related; both are crucial activities in the risk management cycle. While risk assessment is technically the process through which management determines what undesirable things could happen, and controls reviews are designed to assess the effectiveness of risk mitigation measures, in practice, both risk and controls are often addressed together in such reports as A-130 compliance reviews.

As discussed above in [Risk Assessment and Management](#), SFA managers should concern themselves with ensuring controls are in place and operating to deliberately and effectively manage risk to sensitive information. Doing so not only makes good business sense, but also helps SFA satisfy its public-service obligations.

### Current Status:

Again, this survey allows a green stoplight for HR Mod, however, as new ASPs are added and improvements made to the system, an impact evaluation to the system's security controls should be made. Per the ASP model, most changes to controls should be minimal. More importantly, as policies and procedures come out, they should be reviewed for their impact on security controls.

### **Opportunities for Improvement:**

Again, the owners of HR Mod need to ensure that future security control reviews occur after any major modification to the system or to the organization's policies and procedures, and at least every three years. Also, controls should be examined whenever a new ASP is added to ensure that no new vulnerabilities exist.

**Yellow**

## Rules Of Behavior

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

### Significance in the SFA Environment:

**Threat:** Inappropriate or insecure system usage creates system vulnerabilities, as well as possibly compromising the system itself.

**Impact:** Rules of behavior that define expected and prohibited behavior increase management's confidence that system users are following information security and privacy policies and standards. Users cannot reasonably be expected to remember in detail the laws, regulations, policies, standards, procedures and guidelines that govern the operation and use of a system. However, well-defined rules of behavior can distill the intent of law and policy into a form that is easily grasped and retained. In addition, while policies and standards are intended more to provide guidance to decision-makers, rules of behavior are designed to provide day-to-day guidance to users. Combined with a robust privacy and [security awareness and training](#) program, system rules of behavior help to ensure that everyone granted authorized access to SFA systems behaves in a consistently secure and ethical fashion.

### Current Status:

Jamcracker has a fairly in-depth set of user guidelines and requirements, principally the "Acceptable Usage Guidelines," the "Corporate IT Security Policy," the "Internet Usage Policy," and the responsibility agreements new employees sign. These, as a group, make up the Rules of Behavior for Jamcracker employees.

SFA does not currently have an enterprise-level Rules of Behavior, which hampers creating a system-level set of rules. HR Modernization does not have a set of rules for system users.

### **Opportunities for Improvement:**

A set of user rules of behavior needs to be developed and circulated before the main system rollout. Preferably, these would be based off of SFA's enterprise-level rules, but that is not required. These rules do not need to be extensive; primarily they should cover password protection and system usage guidelines.

**Red**

## Security Life Cycle Planning

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-14, NIST Special Pub 800-18

Security, like other aspects of an IT system, is best managed if planned for *throughout* the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

Organizations should ensure that security activities are accomplished during each of the phases:

*Initiation Phase:* Document the need and purpose for the system. Perform an information sensitivity assessment.

*Development/Acquisition Phase:* Develop security requirements at the same time system planners define the requirements of the system.

*Implementation Phase:* Configure and enable the system's security features; test, install, field, authorize for processing.

*Operation/Maintenance Phase:* Describe the security activities conducted or planned as the system evolves. The security plan documents the security activities.

*Disposal Phase:* Briefly describe how information is disposed of and how media are sanitized.

### Significance in the SFA Environment:

**Threat:** Inadequate implementation of security controls due to a lack of established security requirements early in the system's life cycle.

**Impact:** Information and the technology that supports it represent SFA's most valuable assets. Moreover, SFA's customer base—students and educational institutions—have heightened expectations regarding service delivery. For this reason, SFA customers require increased quality, functionality, and ease of use, decreased loan processing time, and continuously improving service levels. The constrained resource environment within the Federal government requires all these goals to be accomplished at lower cost and reduced risk. Success, however, requires SFA managers to understand and manage the risks associated with implementing and operating technologies that handle sensitive information.

One of the keys to success requires privacy, security, and risk management principles to be knit into the system life cycle. Security controls are always more expensive to retrofit than to design-in; accordingly, privacy and security should be considered in the very earliest stages of systems development and follow through the life cycle to disposal. Similarly, information passes through a predictable life cycle; controls must be in place at every stage in that life cycle from creation or entry through disposal. Planning for privacy and security in the life cycle will help SFA optimize its information investment, and mitigate information and business process risks when things go wrong.

### **Current Status:**

A preliminary examination of Jamcracker's security practices took place early in the Development phase during the Modernization Partner's technical review of Jamcracker's processes. This examination was not thorough, however, primarily focusing on password usage and network encryption methods. Furthermore, no sensitivity analysis was conducted during the Initiation phase (see [General Description of Information Sensitivity](#)), and no list of specific security requirements was created and passed to Jamcracker for implementation onto HR Modernization. This lack of specific requirements could translate to missed opportunities to strengthen system security earlier in the system's lifecycle. This must be taken into consideration, however, with SFA's until-recently lenient adherence for SDLC requirements.

### **Opportunities for Improvement:**

HR Modernization should begin using relevant security portions of SFA's SDLC worksheets to ensure that security is properly implemented throughout the remainder of the system's life cycle, and documentation is kept to help validate the fact.

Green

## Authorize Processing

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented secures the application adequately. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

### Significance in the SFA Environment:

**Threat:** Lack of acceptance of system risks; management remaining ignorant of residual risks within the system.

**Impact:** Risk management is a necessary activity in any systems environment because risk is a fact of life in virtually all IT environments – there is no such thing as a risk-free system. In consequence, before an SFA system becomes operational it makes sense for senior SFA management to decide how much risk must be mitigated prior to system use, or conversely, how much residual risk can be accepted. This is the purpose of the certification and accreditation process; to decide whether risk is mitigated to the point where from a business and legal perspective it is safe to allow a system to process information. In order to provide SFA managers with a reasonable basis for accreditation – risk acceptance – some sort of technical review must be conducted to determine if the systems' automated and procedural controls are sufficient to enforce SFA security policies and standards. In this way, risk decisions can be made deliberately rather than by default.

### Current Status:

HR Modernization will receive authorization during its upcoming Production Readiness Review, currently scheduled for October 22, 2001.

### Opportunities for Improvement:

Ensure that reauthorization occurs at least every three years.

Yellow

## Personnel Security

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties an individual may perform

### Significance in the SFA Environment:

**Threat:** Improper access to information by employees; infiltration by known system intruders; increased insider threat.

**Impact:** SFA is responsible for disbursing millions of dollars annually in student aid. In this process, SFA must accurately account for allocated funds, reconcile accounts, handle personal information on thousands of individuals, and interact with hundreds of government, private, and commercial institutions. In recognition of the sensitivity of this mission and the systems, information, and processes that support that mission, the Department of Education has articulated policies and procedures for identifying sensitive positions. These policies and procedures are outlined in ED's *Personnel Security Suitability Program Handbook*. Dated November 4, 1992, and issued by the ED Office of the Inspector General (OIG), this handbook was issued to implement 5 CFR Parts 731, 732, 736 and 754, and outlines ED's personnel security suitability policies, procedures, and guidelines.

### Current Status:

Jamcracker has an effective set of management controls that will assist in personnel security. Duties have been separated between the Operations and Production groups; additionally, "root" access privileges have been limited to select individuals with the need for this access. Audit controls have been implemented which specifically search for suspicious activities, ranging from direct attacks on systems to more subtle intrusion attempts. Jamcracker provides training to all employees on their [Rules of Behavior](#), including Jamcracker's policies and employee expectations, and has in place a solid procedure for handling both friendly and unfriendly terminations. Jamcracker currently performs reference and employment checks on new hires, but does not conduct background checks (credit checks, criminal checks, etc.); it is planning on conducting background checks on employees in highly sensitive positions (system administrators, senior executives, etc.) in the near future.

### **Opportunities for Improvement:**

We would highly suggest incorporating background checks into the hiring process of sensitive positions at Jamcracker. The personnel controls in place will limit the capabilities of a malicious employee in most cases, but would be of limited assistance to preventing damage caused by an employee that was mistakenly entrusted with administrative privileges. Should any planned HR Mod applications include Privacy Act data, ensure Jamcracker employees are briefed on the protection of Privacy Act data.

**Yellow**

## Physical and Environmental Protection

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

An organization's physical and environmental security program should address the following seven topics:

- Physical access controls
- Fire safety factors
- Failure of supporting utilities
- Structural collapse
- Plumbing leaks
- Interception of data
- Mobile and portable systems

### Significance in the SFA Environment:

**Threat:** Damage of equipment through natural disasters, accidents, or improper environmental conditions; theft of IT equipment or data; ease of access to sensitive ports or servers.

**Impact:** Physical and environment protections are especially important for a number of reasons: the protection of IT equipment from damage or theft, the isolation of equipment from potential intruders, and the physical monitoring of IT equipment.

### Current Status:

The data center access controls and facility physical/environmental protection seem adequate to protect unauthorized access to sensitive systems and lessen damage from power failures. We didn't receive complete and clear information on some of the physical controls, to include the type of building access control at the Exodus facility, fire and water damage controls, and what HR Mod-related resources are at Jamcracker's HQ that may require protection. For this reason, a complete assessment couldn't be made.

### **Opportunities for Improvement:**

Jamcracker needs to separate hot and cold production facilities to prevent a complete loss of Jamcracker resources in the case of earthquake, fire, structural collapse or other major incident that would impede the data center's operation. Update the security plan with the information that wasn't received as described above.

**Green**

## Production, Input/Output Controls

[Back to Risk Cycle Illustration](#)

### Standard: **NIST Special Pub 800-18**

Describe the controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures for the information and media. The controls used to monitor the installation of, and updates to, application software should be listed. In this section, provide a synopsis of the procedures in place that support the operations of the application.

### Significance in the SFA Environment:

**Threat:** Mishandling, loss or compromise of sensitive system material, both electronic and paper; corruption of data files by improper input procedures.

**Impact:** SFA systems are complex and are located and operated in a diverse and complex environment. In these circumstances, sensitive information (and the applications that process, store, and transmit it) are vulnerable to compromise and corruption. As noted in Special Pub 800-18, "...appropriate and adequate controls will vary depending on the individual system requirements..."; the accreditation authority, in coordination with system management and security authorities, should determine what controls are appropriate. At a minimum, applications that handle sensitive information should have controls for marking, handling, processing, storage, and disposal that are sufficient to ensure this information is not mishandled through error.

### Current Status:

Jamcracker organizes all information, data, or documentation in accordance with their Data Classification Guidelines, grouping things as one of the following: Public, Internal, Confidential, or Secret. Each classification has its own guidelines for storage, transmission, and destruction commensurate with its classification, and the potential damage compromise of the data could cause. Controls are in place to ensure proper monitoring of software installations and updates, and are explored further in [Application Software Maintenance Controls](#).

### Opportunities for Improvement:

Once HR Modernization begins to transact data containing Privacy Act information, it will be imperative for procedures to be implemented for labeling Privacy Act output. No details for handling paper (non-electronic) materials were specified in the Data Classification Guidelines. Procedures for mailing or transporting HR Mod input/output were also not described. These areas couldn't be fully assessed, but it could be assessed that Jamcracker would create these type of procedures as per customer requirements.

**Yellow**

## Contingency Planning

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

### Significance in the SFA Environment:

**Threat:** Confusion or disorganization exacerbating an emergency situation; unclear or improper procedures compounding problems; extended system outage and loss of system data.

**Impact:** It is vital for SFA to have an established, coherent plan in place that will cover a wide range of possible incidents, from complete catastrophic failures to an application failure. Additionally, this plan needs to be easily available and understandable in the event of an emergency. The middle of an actual incident would not be the proper time for either training or testing of the plan.

### Current Status:

Jamcracker has a detailed Disaster Recovery Plan (DRP), and is finalizing its Incident Response Plan (IRP). The DRP provides excellent details regarding how a disaster is declared, how operations would transfer to the backup facilities, and the recovery strategies that would be used. Jamcracker is ensuring that this document is being kept up to date with current points of contact. The reviewed draft IRP provided a good framework for what to do in case of an intrusion, from initial response to analysis and recovery. The IRP does not discuss incidents other than an intrusion into the system. Also missing are procedures in place for other incidents – although the DRP states that it could be adapted to cover less-than-catastrophic events, it would be an unwieldy tool to use to respond to a small fire in the data center or a server crash.

### **Opportunities for Improvement:**

The IRP should be expanded to cover a broader range of incidents, from virus infection to application failure. These would most likely have very similar requirements as those already used for response, containment, analysis and recovery after an intrusion. Additionally, contingency plans should be created for more likely less-than-catastrophic events. Many of these could be aggregated into different categories of incidents, but there should be resources available to handle all contingencies, accidental or malevolent. Lastly, all plans should be reviewed for the inclusion of SFA points of contact and involvement.

Green

## Application Software Maintenance Controls

[Back to Risk Cycle Illustration](#)

### Standard: **NIST Special Pub 800-18**

Application controls should be established to monitor the installation and updates to application software to ensure software functions as expected and that a historical record is maintained of application changes.

### Significance in the SFA Environment:

**Threat:** Improper updates to applications; system degradation resulting from unexpected software incompatibilities; software failure.

**Impact:** As noted elsewhere in this report, the collective SFA systems environment is moderately large in terms of size, scale, complexity, and interconnectivity. Many systems and applications are required to support the SFA business process; these are developed, operated and maintained by multiple software developers. If software maintenance controls are not in place or operating effectively, unauthorized or unintended changes to application software can result in privacy or security compromises to information in the system, which may impact SFA's ability to properly service its customers. In addition, due to the interconnectedness of SFA and ED systems, errors in one application may propagate to other applications in the system in question.

### Current Status:

Change Management controls are thoroughly discussed in Jamcracker's Change Administration & Rollout Management Manual (JC-12-0043). Jamcracker utilizes sound maintenance control practices, ensuring the use of version controls of software and documentation, the separation of testing and production environments, and the analysis of potential security issues inherent to the change to ensure no vulnerabilities are being introduced into the system.

### Opportunities for Improvement:

SFA's HR Modernization System Security Officer (SSO) should be part of the approval chain for all proposed changes to system software to avoid changes being made that would compromise privacy or security controls, and to enable the SSO to act as the accrediting authority's agent in between certification cycles.

Green

## Data Integrity/Validation Controls

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-18

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirement. Describe any controls that provide assurance to users that the information has not been altered and the system functions as expected.

Data integrity controls include antivirus software, reconciliation routines, edit checks, intrusion detection, message authentication codes, and system performance monitoring.

### Significance in the SFA Environment:

**Threat:** Hardware failure or user error causing a loss of retrievable data; data entry errors creating application software corruption; system contamination by malignant software; intentional contamination of the system by unauthorized intruders.

**Impact:** Information enters SFA systems by multiple sources, some within SFA's span of control but many not. Integrity and validation checks help to ensure that as information enters, is processed, and is output from the system, it retains its integrity. As noted above for [application software maintenance controls](#), the interconnected nature of SFA systems make continued data integrity a crucial issue; information corruption can propagate throughout the system, impacting SFA's efficient execution of its business processes.

### Current Status:

Jamcracker uses a variety of controls to counter the various threats to data integrity. Monthly data backups due to SFA, and training focused on equipment maintenance and continuous backing-up of information prevent data loss. Input validation is performed on critical fields by making the fields format specific, limiting accidental corruption within the system. Virus protection software is installed on all critical servers, and is updated via live updates from the software manufacturers. Jamcracker's external e-mail service provider scans incoming messages for further virus protection. Lastly, Jamcracker's [Logical Access Controls](#) and use of [Audit Trails](#) limit contamination by intruders, whether they may be external or internal.

### Opportunities for Improvement:

As noted in the [sensitivity/criticality analysis](#), integrity is the most important security function required for HR Modernization, requiring the most controls and attention. Although Jamcracker has created a thorough set of integrity controls, it is within the ASPs that the actual HR data will reside. Because of this, it is imperative that stringent requirements for integrity controls are laid out in the SLAs between SFA and Jamcracker, thereby flowing through to the ASPs. As already stated in the [System Interconnection/Information Sharing](#) section, this should be improved before more ASPs are added to the system.

**Yellow**

## Documentation

[Back to Risk Cycle Illustration](#)

### Standard: [OMB A-130](#), [NIST Special Pub 800-18](#)

Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST.

Documentation should be coordinated with the general support system and/or network manager(s) to ensure that adequate application and installation documentation are maintained to provide continuity of operations.

### Significance in the SFA Environment:

**Threat:** Inconsistent or missing procedures; incapability to effectively operate or train because of a lack of established documented procedures.

**Impact:** System documentation (e.g., system description, technical interface description, system manager manual, user manual, security policy and standards, security features users guide, risk assessment, certification test reports, operational procedures and guidelines, etc.) help to establish a common baseline of knowledge for managers, developers, operators and users. This baseline is especially important in a complex, interconnected multi-system environment such as SFA's. In the SFA environment it is common for managers, staff, contractors, and non-SFA government employees to require information concerning SFA systems. Well maintained documentation ensures, for example, that other system developers who are writing code to interface with an SFA system have authoritative interface documentation to draw from. Similarly, as noted in the [systems environment](#) section above, adequate documentation promotes increased efficiency and effectiveness across a wide range of activities.

### Current Status:

Jamcracker is in the midst of documenting all security procedures and practices. Many are recent creations still in the draft stages, and some are still on schedule to be written. Additionally, we were not able to conduct a thorough review of all documentation to ensure all required documents were either available or properly written. That said, Jamcracker has made significant improvements in creating required documentation in acceptable formats.

### **Opportunities for Improvement:**

Continue finishing documentation on all security procedures and practices, and ensure that all documentation is kept up to date and properly accessible.

**Green**

## Identification and Authentication

[Back to Risk Cycle Illustration](#)

### Standard: [NIST Special Pub 800-14](#), [NIST Special Pub 800-18](#)

Identification and authentication (I&A) is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability.

- Describe the major application's authentication control mechanisms.
- Describe the method of user authentication (password, token, and biometrics).
- Provide the following if an additional password system is used in the application:
  - password length (minimum, maximum)
  - allowable character set,
  - password aging time frames and enforcement approach,
  - number of generations of expired passwords disallowed for use
  - procedures for password changes (after expiration and forgotten/lost)
  - procedures for handling password compromise
- Indicate the standards for of password changes.
- Describe how the access control mechanism supports individual accountability and audit trails.
- Describe the standards for password syntax.
- Describe the standards for password protection.
- State the number of invalid access attempts that may occur and describe the actions taken when that limit is exceeded.
- Describe the procedures for verifying that all system-provided administrative default passwords have been changed.
- Describe the procedures for limiting access scripts with embedded passwords.
- Describe any policies that provide for bypassing user authentication requirements, and any compensating controls.
- Describe any use of digital or electronic signatures and the standards used. Discuss the key management procedures for key generation, distribution, storage, and disposal.

## Significance in the SFA Environment:

**Threat:** Unauthorized access to system, servers, applications, etc.; inadequate procedures for the protection of passwords.

**Impact:** Access control and individual accountability are important goals in any system, but particularly so in systems that process, store, and transmit sensitive information. Attempts to gain unauthorized access and acts by disgruntled or unethical users are a growing concern in government and industry. However, the greater threat is human error; well-intentioned people who make mistakes that compromise privacy and security. In either case, it is important for system management to be able to have confidence that unauthorized users cannot access sensitive systems and data, and that mechanisms are in place to track down the source of problems quickly to prevent further data compromise or corruption. As noted above, the interconnected nature of SFA systems makes the ability to control access and maintain individual accountability all the more important. See the discussion of [logical access controls](#) below.

## Current Status:

HR Modernization has a solid identification and authentication foundation protecting against unauthorized entry. User identification for SFA employees will be the users' e-mail identification. Jamcracker provides a set of guidelines as to password length and choice to all users, suggesting a minimum of seven characters and a mixture of letters, numbers, punctuation, and multiple case formats. Jamcracker audits passwords every 60 days using NT tools with a custom dictionary to discover improper passwords (words, names, number series, etc.); these accounts are frozen and users are forced to choose another password. Jamcracker passwords expire every 90 days; SFA user passwords expire every thirty. Procedures are in place in case of a forgotten or compromised password, and Jamcracker uses internal validation software programs to check for insecurities such as default passwords before an application's startup and as a continuous form of quality assurance. Password databases are kept in encrypted format. Full details of identification and authentication controls are provided in the Platform Security Functional Requirements (PlatformSecurityFRDv0.52).

## Opportunities for Improvement:

Given the current limited usage for HR Modernization, having a thirty day password expiration is too extreme, and would encourage unsafe password protection by users as their passwords are constantly changed. The expiration period should be extended to 60-90 days; once other ASPs are added, the period could be reevaluated. Additionally, password controls specific to HR Modernization should be fully documented and included within the SFA security plan.

Green

## Logical Access Controls

[Back to Risk Cycle Illustration](#)

### Standard: [NIST Special Pub 800-14](#), [NIST Special Pub 800-18](#)

Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems. The policy should balance the often-competing interests of security, operational requirements, and user-friendliness. In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

- Discuss the controls in place to authorize or restrict the activities of users and system personnel within the application.
- Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (i.e., access control lists [ACLs]).
- How are access rights granted? Are privileges granted based on job function?
- Describe the application's capability to establish an ACL or register.
- Describe how application users are restricted from accessing the operating system, other applications, or other system resources not needed in the performance of their duties.
- Describe controls to detect unauthorized transaction attempts by authorized and/or unauthorized users. Describe any restrictions to prevent users from accessing the system or applications outside of normal work hours or on weekends.
- Indicate after what period of user inactivity the system automatically blanks associated display screens and/or after what period of user inactivity the system automatically disconnects inactive users or requires the user to enter a unique password before reconnecting to the system or application.
- Indicate if encryption is used to prevent access to sensitive files as part of the system or application access control procedures.
- Describe the rationale for electing to use or not use warning banners and provide an example of the banners used. Where appropriate, state whether the Department of Justice, Computer Crime and Intellectual Properties Section, approved the warning banner.

### Significance in the SFA Environment:

**Threat:** Unrestricted access to sensitive data or applications; improper usage of another's access privileges.

**Impact:** Closely related to [identification and authentication](#) above, logical access controls are required to limit management's information privacy and security concerns. Most SFA system users have a limited need to access sensitive information, so information risk can be significantly reduced by limiting access to only those things each user requires to perform their job or receive the required level of support from the system. Enforcing the [least privilege principle](#) also reduces management's monitoring and [audit](#) challenge; with many potentially risky transactions prohibited by logical access controls.

### **Current Status:**

Again, Jamcracker employs sound logical access controls to protect entry into their servers or applications. Given that this is Jamcracker's core business, it is not a surprise. Jamcracker stringently employs the least privilege principle on users' access privileges, and ties access rights directly to job function. For SFA users, Jamcracker will be provided and will use a database detailing the ASP access rights and levels (manager vs. normal in Perform.com, for example) by the Modernization Partner. Full details of access controls are provided in the Platform Security Functional Requirements (PlatformSecurityFRDv0.52).

### **Opportunities for Improvement:**

Again, access controls specific to HR Modernization should be documented fully within the SFA security plan.

**Green**

## Public Access Controls

[Back to Risk Cycle Illustration](#)

### Standard: OMB A-130

Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system.

### Significance in the SFA Environment:

**Threat:** Insecure public access to confidential data.

**Impact:** SFA systems must necessarily provide an interface with institutions and individuals in order to provide the expected level of service. However, without mitigating controls, providing access for so many organizations and individuals outside of the SFA span of control would be fraught with risk to privacy, confidentiality, integrity and availability. Without public access controls in place to enforce [least privilege](#) and limit access to only those things each institution or user requires to receive the expected level of service, data would quickly become unreliable, with potentially serious consequences to other system and to individual privacy.

### Current Status:

The general public does not access HR Modernization.

### Opportunities for Improvement:

None Applicable

**Green**

## Security Awareness and Training

[Back to Risk Cycle Illustration](#)

**Standard: OMB A-130, NIST Special Pub 800-14**

Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the application and the information in it. This training will be in addition to that required for access to a support system.

A computer security awareness and training program should encompass the following seven steps:

- Identify Program Scope, Goals, and Objectives.
- Identify Training Staff
- Identify Target Audiences
- Motivate Management and Employees.
- Administer the Program
- Maintain the Program.
- Evaluate the Program.

### Significance in the SFA Environment:

**Threat:** Ignorance regarding security policies and procedures can create vulnerabilities that are easily exploitable. The best policies will not help unless employees are properly trained, and proper records are kept regarding the training conducted.

**Impact:** Training is a key activity in the risk management process, and a challenge for SFA. This challenge stems from the geographic dispersion of SFA system managers, operators, developers, and users. Additionally, within this group security responsibilities are quite diverse. Everyone, regardless of their position or function, must understand some privacy and security issues; system [rules of behavior](#) probably represent the irreducible minimum for the vast majority of the audience. However, many members of the system population have additional requirements and responsibilities, depending on individual job function. For example, SFA managers must become cognizant of their role in creating and fostering a secure environment at SFA and how privacy and security support SFA's operations and missions. Management must be made aware of their responsibility to provide a SFA-wide security vision, demonstrate management commitment to privacy and security, establish and resource an information security management structure, and sponsor an effective security training and awareness program. In contrast, the training provided to developers and other privileged users might emphasize understanding the SFA information privacy and security policy and standards architecture—describing the policies that affect them in their jobs, explaining their particular responsibilities, such as remaining aware of who is covered by policy, complying with policy, reporting violations, and using common sense.

### Current Status:

Jamcracker conducts entry and refresher security training for all employees on security policies and procedures, including security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities (e.g., log-on procedure, use of software packages, etc.). Training must be completed before access to information or services is granted. Modernization Partner is providing SFA user training, including password protection and internet security.

### Opportunities for Improvement:

Once SFA system [rules of behavior](#) have been created, incorporate those rules into the SFA user training curriculum. Update the security plan with the details of Mod Partner training for SFA users.

**Green**

## Audit Trails

[Back to Risk Cycle Illustration](#)

### Standard: NIST Special Pub 800-14

In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails should be used for the following:

- Individual Accountability
- Reconstruction of Events
- Intrusion Detection
- Problem Identification

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs.

Organizations should protect the audit trail from unauthorized access. The following precautions should be taken:

- Access to online audit logs should be strictly controlled.
- Organizations should try to separate the duties of setting access controls function and audit trail administration.
- Audit trail information should be protected, for example, if it records personal information about users.

Audit trails should be reviewed periodically. The following should be considered when reviewing audit trails:

- Reviewers need to understand what normal activity looks like.
- Audit trail review can be easier if the audit trail function can be queried by some set of parameters; e.g., User ID, Terminal ID
- Administrators should review the audit trails following a known problem, violation, or unexplained event.
- Cognizant managers should determine how much review of audit trail records is necessary.
- Organizations should use audit reduction tools.

## Significance in the SFA Environment:

**Threat:** Inability to reconstruct or provide evidence regarding an incident; lack of real-time assessment of insecure practices; inability to effectively review audit logs.

**Impact:** Audit is another key activity in the GAO risk management process. In order to manage risk in a dynamic environment such as SFA's, managers must be able to assess the effectiveness of risk mitigation controls, and make adjustments as required to contain costs, reduce errors, achieve efficiencies, or contain risk. Managers must have a reasonable and rational basis for making these decisions, and monitoring for control compliance and effectiveness is the best way to achieve this goal.

Effective audit requires more than simply turning on audit logs. Most systems are now capable of producing audit logs of such length and detail that the output from a single system could keep several knowledgeable staff members occupied full time reviewing them. Since this is not practical in the SFA environment, SFA must find a way to reduce the audit burden to a manageable level – no more than can be reviewed effectively by the system SSO in a fraction of that person's available hours.

Achieving this goal enables several other key risk management activities:

- Incident response: timely review of audit logs can trigger timely response to errors and hostile activity
- Risk assessment: collecting statistics of key high-risk events provides management with a quantitative basis for risk management
- Security awareness: a better understanding of where risk is actually incurred can improve the quality of security training

## Current Status:

The Jamcracker Platform captures audit trails from many devices, including firewalls, authentication servers, LDAP and database servers, application servers and web servers. Information included would provide all necessary data to reconstruct a past incident, whether it was an application error or an attack on a Jamcracker server. All audit trails are stored on a secure logging server accessible only to the Jamcracker Security Operations team and Vinciti, Jamcracker log analysis server partner. Access to the audit logs is available in a read-only format to Jamcrackers Engineering and Developments for troubleshooting purposes. All audit logs are stored on magnetic tape for archive purposes and the tapes are retained for 90 days. Jamcracker ensures audit clock reliability and accuracy through numerous redundant references. Behavioral profiles are used to assist in detecting possible security violations and initiate automatic responses to an imminent security violation.

## Opportunities for Improvement:

Document SFA involvement in the audit review process, as well as establish an audit review schedule to examine audit logs on a periodic basis.

## Conclusions

First and foremost, it must be understood that HR Modernization is launching as a pilot program with minimal users and supporting fairly innocuous data. A level of security risk determination is comprised of the likelihood of a threat occurrence balanced against the impact of that threat occurring. Due to the very nature of the pilot launch, any exploitation will have a very low impact to SFA as a whole, regardless of how likely the threat may occur. For this system, the likelihood of threats occurrence has also been minimized by the existing/planned system security controls, creating an overall risk level of low.

The risks identified within HR Modernization are mostly administrative in nature, and should be fairly easy to incorporate in the near future. This is important, because as the pilot program is expanded to incorporate all SFA employees, and HR Modernization begins to incorporate additional ASPs, it will be vital to have a solid procedural foundation to support the additional risks inherent with more users and more data. Fortunately, the very aggregate model that Jamcracker relies upon makes it easy for new documented security procedures to be incorporated in this expansion.

Displayed in the table below are discrete activities that we recommend SFA fund and perform. These recommendations are organized to illustrate which part of the risk management cycle they are intended to support, numbered in priority order, and based on the opportunities for improvement articulated above.

Risk Management Cycle Stage	Issue Area	Recommendation	Priority
<b>Assess Risks and Determine Needs</b>	Assignment of SSO	<b>Assign an SFA System Security Officer for HR Modernization.</b>	<b>1</b>
	Security Language in SLA	<b>Create explicit security requirements which provide precise standards with detailed examples of what is to be expected in data confidentiality and integrity controls.</b>	<b>2</b>
	System HW/SW listings	<b>Provide list of hardware and software used for HR Modernization for inclusion in the System Security Plan</b>	<b>4</b>
<b>Implement Policies and Controls</b>	SFA Rules of Behavior	<b>Develop SFA specific Rules of Behavior.</b>	<b>10</b>
	Life Cycle Planning	<b>Incorporate relevant security portions of the SFA SDLC Guidelines into future system modifications.</b>	<b>9</b>
	Background Checks for Critical Positions	<b>Require background checks for all critical positions at Jamcracker before access to sensitive systems is permitted.</b>	<b>5</b>
	Expand Contingency Plans	<b>Expand contingency plans to incorporate all possible types of incidents.</b>	<b>8</b>
	Separate Hot and Cold Facilities	<b>Physically separate “Hot” and “Cold” production environments to allow immediate backup operations in the “Cold” environment.</b>	<b>3</b>
	Continue Documenting all Security Procedures	<b>Finish documentation of remaining Jamcracker security procedures.</b>	<b>7</b>
	Change SFA Password Expiration Period	<b>Increase expiration period for SFA user passwords from 30 days to 60-90 days.</b>	<b>6</b>