

PALM BEACH STATE COLLEGE

ADMINISTRATIVE PROCEDURE

Policy: 6Hx-18-1.XX	Category: Information Technology	Version Date: 0001
Title: Risk Assessment		Effective Date: 11-01-09
Originating Unit: Information Technology Security Office		Last Review: TBD
Review Officer: Chief Information Officer, Anthony Parziale		Next Review: TBD

Overview:

Risk assessment is a methodology for determining the likelihood and severity of loss of information confidentiality, integrity and confidentiality. It is the basis of compliance with most information-based regulations and standards; in fact, it is the basis of all information security.

The principal goal of an organization's risk management process should be to protect the *organization and its ability to perform their mission*, not just its IT assets. Therefore, the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization.

Purpose:

A basic requirement of an effective Information Assurance program is to identify and classify the assets to be secured. A well-defined and auditable risk assessment process significantly assists the planning and selection of security controls used to protect assets. Risk assessment is the process of identifying threats to, and vulnerabilities of, information assets, the value of those assets and determining the potential business impact of a loss caused by the identified threats and vulnerabilities. Controls can then be applied to mitigate the risks of loss. Not all risks can be offset at a cost commensurate with the asset to be protected; however, it is not only legitimate, but also prudent, for management to accept certain levels of risk as a "cost of doing business."

The objective of the risk management process is to enable the organization to accomplish its mission(s) (1) by better securing the IT systems and business processes that store, process, or transmit electronic information; (2) by enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.

Scope:

All of the Information Assurance controls of Palm Beach State College that specify the use of a risk assessment process are covered by this policy. The information assets and individuals covered by this policy include, but are not limited to:

Risk Assessment Policy

- The information assets stored and managed by Palm Beach State, whether in electronic or printed form
- Computers, networking infrastructure (routers, switches, firewalls, etc.), and other electronic equipment associated with the storage, processing, or transmission of information
- Software and program source code
- Electronic services (such as electronic messaging, fax, etc.) provided by Palm Beach State
- All users

Policy:

Enterprise Security Risk Assessment

Each year the Information Technology Security Office (ITSO) in conjunction with Information Technology (IT) must conduct, or manage an independent party who conducts, an organization-wide security risk assessment.

Business Unit Risk Assessment

Each critical organizational or business unit within Palm Beach State that manages its own computers or networks must also perform, at least annually, a security-related risk analysis of these same systems, coordinated through the ITSO, and then certify that adequate security measures have been implemented to mitigate the risks.

Risk Assessment Methodology

Palm Beach State requires, where appropriate, that a risk assessment process be used where specified by Information Security policies and procedures, or by laws or regulations. The Facilitated Risk Assessment process is the recommended standard (cf. Risk Management Guide for Information Technology Systems, NIST SP 800-30.)

Palm Beach State risk assessments are to be conducted using the Facilitated Risk Assessment process (FRA).

Specific instances requiring risk assessments include:

Production System Risk Assessments

1. All systems being implemented (COTS) or constructed will be assessed for risk by a project-oriented FRA team during the preliminary design phase, before funding has been finalized. (Industry experience shows that security remediations not implemented until the actual construction phase cost 4 times as much, and those not implemented until after implementation cost 10 times (a whole order of magnitude) as much.)

Risk Assessment Policy

2. All production computer information systems must be reevaluated for risk when they are to be significantly modified or enhanced.
3. All production information systems that are being considered for development or deployed by external third parties.

Annual Information Technology Risk Report

For IT to properly perform its risk management role, IT management must produce a special annual report. This report is to include a description of all material Palm Beach State information technology-related risks, as well as an assessment of how these risks are currently being managed.

Material\Significant Information Security Risks

For every material\significant information systems security risk identified -- whether through a formal risk assessment or not -- management must make a specific decision about the degree to which Palm Beach State will be self-insured and accept the risk, seek external insurance, or adjust controls to reduce expected losses to an acceptable cost of conducting business.

Roles and Responsibilities

Risk management is a management responsibility. The following describes the key roles of the personnel who should support and participate in this process (See NIST SP 800-30.)

One of the major strengths of FRA lies in the way that it composes the team to perform the Risk Assessment. Drawing together the process owners, stakeholders, and Subject Matter Experts (SME's) from the spectrum of disciplines involved, builds a formidable brain trust to conduct the FRA itself --- and ultimately builds ownership of the resulting methods and processes to better assure protection of the business assets involved.

FRA Team – The FRA Team defines the specific scope of the risk assessment then identifies threats, assets, vulnerabilities, and risks to the Network processing environment. Additionally, the team identifies risks mediation by controls already in place. Remaining residual risks are categorized as either major or minor, and are included in the analysis of the effectiveness of the security protection on the environment in the scope of the specific FRA.

Senior Management – Senior management, under the standard of due care and ultimate responsibility for mission accomplishment, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks requires the support and involvement of senior

management.

Chief Information Officer (CIO) – The CIO is responsible for the enterprise's IT planning, budgeting, and performance including its information security components. Decisions made in these areas should be based on an effective risk management program.

System and Information Owners – The system and information owners are responsible for ensuring that proper controls are in place to address integrity, confidentiality, and availability of the IT systems and data they own. Typically the system and information owners are responsible for changes to their IT systems. Thus, they usually have to approve and sign off on changes to their IT systems (e.g., system enhancement, major changes to the software and hardware). The system and information owners must therefore understand their role in the risk management process and fully support this process.

Business and Functional Managers – The managers responsible for business operations and IT procurement process must take an active role in the risk management process. These managers are the individuals with the authority and responsibility for making the trade-off decisions essential to mission accomplishment. They are responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk (that which remains) before authorizing the IT system in question for operation. Their involvement in the risk management process enables the achievement of proper security for the IT systems, which, if managed properly, will provide mission effectiveness with a minimal expenditure of resources.

Information Security Manager (ISM) –The ISM is tasked with providing internal expertise and training to management on how to conduct an effective risk assessment. The ISM is to provide assurance that risk assessments are performed when required and that they adequately consider and determine the threats, vulnerabilities, assets, controls, risks and residual risks involved.

IT Security Practitioners – IT security practitioners (e.g., network, system, application, and database administrators; computer specialists; security analysts; security consultants) are responsible for proper implementation of security requirements in their respective IT systems. As changes occur in the existing IT system environment (e.g., expansion in network connectivity, changes to the existing infrastructure and organizational policies, and introduction of new technologies), the IT security practitioners must support or use the risk management process to identify and assess new potential risks and implement new security controls as needed to safeguard their IT systems.

Risk Assessment Policy

Security/Subject Matter Professionals – The organization’s personnel are the users of the IT systems. Use of the IT systems and data according to an organization’s policies, guidelines, and rules of behavior is critical to mitigating risk and protecting the organization’s IT resources. To minimize risk to the IT systems, it is essential that system and application users be provided with security awareness training. Therefore, the IT security trainers or security/subject matter professionals must understand the risk management process so that they can develop appropriate training materials and incorporate risk assessment into training programs to educate the end users.

Enforcement:

As those holding a position of trust, the Management of Palm Beach State is to protect the information assets of, and therefore, the best interests of Palm Beach State. To intentionally avoid performing risk assessments in their area of business responsibility is a breach of that trust and poses serious potential impact on the health and viability of Palm Beach State. The penalties for such violation of trust should be commensurate with the potential consequences to Palm Beach State.

Exceptions:

Exceptions to this policy must be made in writing by the designated Owner of the system or information that will be out of compliance with this policy and approved by a member of the ITSO.

Contact Information:

Questions, concerns or comments concerning this guideline should be directed to:
 Tony Parziale
 CIO
 Palm Beach State College
 4200 Congress Avenue, ITB 103
 Lake Worth, Florida 33461
 Tel: 561.868.3262
 Fax: 561.868.3259

Revision History:

Version	Revision Date	Review Date	Description
1.0	06/30/2009		