

TITLE:	IT RISK MANAGEMENT		
POLICY #:	P-CCSP-003	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



State of Colorado Cyber Security Policies

IT Risk Management

Overview

This policy document is part of the State of Colorado Cyber Security Policies, created to support the State of Colorado Chief Information Security Officer (CISO) in achieving the goals of the Colorado Information Security Act (C.R.S. 24-37.5, Part 4). All Agencies within the scope of this Policy must support and comply with the Requirements section of this document. Additional best-practice guidance is outlined in the Guidelines Section which has been designed to help an Agency achieve the objective of this Policy.

For the purposes of this document, an “Agency” includes organizations as defined in C.R.S. 24-37.5-102(5).

Information Technology security methodologies are the primary vehicle to protect sensitive and critical information resources. Most Information Technology groups or divisions are not fully versed in the value the system provides the organization that relies on the system for achieving operational goals. Thus, a process of assessing the level of impact resulting from a breach of confidentiality, integrity or availability is vital to ensure the party that is ultimately responsible or reliant on the system understands and supports security controls appropriate for the system and accepts the residual risk remaining after the application of these controls.

Authority

C.R.S. 24-37.5-401(1), C.R.S. 24-37.5-403(2)(e).

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.

TITLE:	IT RISK MANAGEMENT		
POLICY #:	P-CCSP-003	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Scope

This policy document applies to every State agency ("Agency") as defined in C.R.S. 24-37.5-102(5). "State agency" means every state office, whether legislative, executive, or judicial, and all of its respective officers, departments, divisions, commissions, boards, bureaus, and institutions. "State agency" does not include state-supported institutions of higher education, the department of higher education, the Colorado commission on higher education, or other instrumentality thereof.

Policy

All Agencies shall develop, maintain, and operate under an IT Risk Management Plan (RMP) and perform an Agency-wide IT Risk Assessment annually.

Definitions

Formal Risk Assessment – A formal Risk Assessment is documented and presented to Executive Management for Risk Acceptance. A formal Risk Assessment must have a statement of Risk Acceptance or Rejection and be approved by Executive Management to indicate their approval or disapproval of the residual risk.

Informal Risk Assessment – An Informal Risk Assessment is the result of deliberations between subject matter experts regarding Cyber Security risk factors and estimated impact. An Informal Risk Assessment is typically performed in the Requirements Analysis or Feasibility Study phases and results in a recommendation for specific security controls. To qualify as a Risk Assessment, an Informal Risk Assessment must have the results documented in some form.

For the purposes of this document, refer to C.R.S. 24-37.5-102, C.R.S. 24-37.5-402, and the Colorado Cyber Security Program Policy Glossary for any terms not specifically defined herein.

Roles and Responsibilities

Executive Director – is responsible for acceptance of residual risk identified in the agency-wide IT risk assessment.

State Chief Information Security Officer (CISO) – is responsible for review and approval of Agency risk management plan as part of the Agency's Cyber Security Program Plan approval process.

Agency Chief Information Officer (CIO) – is responsible for:

- Leading the development of the Agency risk management plan.
- Leading the performance of an agency-wide IT risk assessment.

Agency Information Security Officer (ISO) – is responsible for:

- Monitoring the effectiveness of controls deployed as a result of the agency-wide risk assessment.
- Performing system-level risk assessments where appropriate with the assistance of System Owners.

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.

TITLE:	IT RISK MANAGEMENT		
POLICY #:	P-CCSP-003	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



Agency Staff – is responsible for participation as required in the risk management process.

Requirements

IT Risk Management Plan

Agencies shall develop, disseminate, and periodically review a formal, documented, risk management plan that addresses scope, roles, responsibilities, management commitment, coordination among organizational entities, compliance criteria, and methodology for performing risk assessments. The plan is to include all systems providing State of Colorado services as well as those services contracted to vendors or other third parties.

The Agency risk management plan is to include a characterization of the agency’s systems based on their function, the data stored or processed, and their overall criticality to the organization.

The Agency risk management plan is to include a requirement for a formal annual agency-level Cyber Security Risk Assessment that is submitted to the CISO as part of the Agency Cyber Security Program Plan approval process.

The Agency is to update the risk management plan whenever there are significant changes to the agency’s information systems, the facilities where the systems reside, or other conditions that may impact the risk status of the Agency.

The Agency’s risk management plan is to support vulnerability scans conducted in accordance with the National Institute of Standards and Technology Special Publication (NIST) 800-26.

Agency-Wide Risk Assessment Methodology

The risk assessment methodology leverages industry standards and best practices and includes an assessment of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. For guidance on performing Risk Assessments, see the National Institute of Standards and Technology Special Publication (SP) 800-30, “Risk Management Guide for Information Technology Systems.”

Agencies are to categorize identified risks in terms of likeliness of occurrence and potential impacts using the following definitions:

Likelihood of Occurrence

High - A threat is highly motivated and sufficiently capable, and controls to prevent a vulnerability from being exercised are ineffective.

Medium - A threat is motivated and capable, but controls are in place that may impede successful exercise of a vulnerability.

Low – A threat lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, a vulnerability from being exercised.

Magnitude of Impact

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.

TITLE:	IT RISK MANAGEMENT		
POLICY #:	P-CCSP-003	EFFECTIVE DATE:	DECEMBER 20, 2006
SCOPE:	ALL DEPARTMENTS	SUPERCEDES:	FIRST RELEASE



High – Exploitation of a vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an agency’s mission, reputation, or interest; or (3) may result in human death or serious injury.

Medium – Exploitation of a vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization’s mission, reputation, or interest; or (3) may result in human injury.

Low – Exploitation of a vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization’s mission, reputation, or interest.

The Colorado Cyber Security Plan (CCSP) Policies identify various required minimum controls. In the event that a Risk Assessment identifies a system which cannot meet the required minimum controls, mitigating compensating controls may be selected if they in fact reduce risk to a level acceptable by the Agency. However, any compensating controls that are implemented **MUST** be identified in the formal Agency-wide Risk Assessment, to include the policy non-compliance risk they are addressing and the level of residual risk remaining after implementation of the compensating controls.

Guidelines

This section describes best practices for meeting the objective of this policy.

Granularity of Risk Assessment

The risk assessment plan includes the periodic, at least annual, risk assessment of critical systems.

The risk assessment plan includes the periodic risk assessment of all Agency systems.

System Level risk assessments may be executed formally, with documentation and executive approval or informally by consensus-building activities among IT staff and section managers.

References

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, “Risk Management Guide for Information Technology Systems”
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, “Security Self-Assessment Guide for Information Technology Systems”
- Federal Information Processing Standard (FIPS) 199,
- “Standards For Security Categorization Of Federal Information And Information Systems”
- International Standard For Information Security (ISO)
- “The International Standard Code Of Practice For Information Security Management 17799/27002” Section 4: Risk assessment and treatment

THE ENCLOSED POLICIES AND PROCEDURES ARE FOR OFFICIAL USE ONLY WITHIN THE STATE OF COLORADO. THE MATERIAL MAY NOT BE COPIED OR REDISTRIBUTED WITHOUT THE PERMISSION OF THE CISO FOR THE STATE OF COLORADO.