129

SUBMITTAL TO THE BOARD OF SUPERVISORS
COUNTY OF RIVERSIDE, STATE OF CALIFORNIA

FROM: RCIT

SUBMITTAL DATE:
March 26, 2009

SUBJECT: Board Policy A-58

RECOMMENDED MOTION: That the Board of Supervisors approve revised Policy A-58 as part of an upgrade to the County's Information Security System.

BACKGROUND: The Board Policy Manual is a guide for departments on matters that are not otherwise addressed in state codes, county ordinances, and resolutions by the Board of Supervisors. Heretofore Policy A-58 provided significant information security detail that went beyond policy issues. The Information Security Office (ISO) was created and staffed to provide the Board a mechanism to define processes for managing information security risk. The ISO is charged with developing a methodology to define how information security risks are assessed, accepted and/or mitigated. The ISO also works with departments to ensure that each complies with the County's Information Security Standards. The new policy and the Information Security Risk Management Methodology are attached.

:nDepartmental Concurrence

Jack Miller, Chief Information Security Officer

Matt Frymire, Chief Information Officer

FINANCIAL DATA				
	Current F.Y. Total Cost:	$ 0	**In Current Year Budget:**	N/A
	Current F.Y. Net County Cost:	$ 0	**Budget Adjustment:**	N/A
	Annual Net County Cost:	$ 0	**For Fiscal Year:**	

SOURCE OF FUNDS: N/A

Positions To Be Deleted Per A-30 ☐

Requires 4/5 Vote ☐

C.E.O. RECOMMENDATION: APPROVE

APPROVE

County Executive Office Signature

BY: Elizabeth J. Olson

☒ Policy ☐ Consent

☒ Policy ☐ Consent

Dep't Recomm.:

Per Exec. Ofc.:

Prev. Agn. Ref.: 3.7 11/07/06 | **District:** all | **Agenda Number:** 3.33

RIVERSIDE COUNTY, CALIFORNIA
BOARD OF SUPERVISORS POLICY

Subject:	Policy Number	Page
Information Security Policy	**A-58**	**1 of 1**

Policy:

It is the policy of Riverside County to protect Riverside County information in accordance with all applicable laws, governmental regulations and accepted best practices to minimize information security risk; ensuring the right information is available to the right people at the right time.

To achieve this goal, the Riverside County Board of Supervisors authorizes the Riverside County Chief Information Security Officer (CISO) to develop and maintain the Riverside County Information Security Program and requires all Riverside County Departments to comply.

The Information Security Program consists of the Program Framework, the Information Security Risk Management Methodology and Information Security Standards:

- The Program Framework defines the program's Vision, Mission and Roles & Responsibilities.
- The Information Security Risk Management Methodology defines the processes for assessing, accepting and mitigating information security risk.
- The Information Security Standards define the specific controls and processes required to mitigate information security risks. The Information Security Office (ISO) will develop Information Security Standards as necessary.

The Riverside County Chief Information Security Officer is further authorized to assist the state and federal governments in drafting security and privacy legislation to ensure that the best interests of the constituents of Riverside County are represented.

Riverside County
Information Security Office

Jack B. Miller
Chief Information Security Officer

"The Right information to the Right people at the Right time"

RIVERSIDE COUNTY

INFORMATION SECURITY PROGRAM FRAMEWORK

Riverside County Information Security Office
4080 Lemon St • 10th Floor • Riverside, California 92501 • (951) 955-8282 • FAX (951) 955-8070

PURPOSE 3
VISION 3
MISSION 3
SCOPE 3
AUDIENCE 3
TERMINOLOGY 3
ROLES AND RESPONSIBILITIES 4
BOARD OF SUPERVISORS 4
COUNTY EXECUTIVE OFFICER (CEO) 4
CHIEF INFORMATION SECURITY OFFICER (CISO) 4
RIVERSIDE COUNTY DEPARTMENT HEAD 4
DEPARTMENT INFORMATION SECURITY OFFICER (DISO) 4
AUDITOR CONTROLLER 4
REVISION HISTORY 4

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

PURPOSE

The purpose of the Riverside County Information Security Program Framework is to define the Vision, Mission and Roles & Responsibilities for the Information Security Program.

VISION

The vision of the Information Security Program is that through appropriate information security risk management, Riverside County will reduce the chances of having an information security incident impact the delivery of service to its constituents.

MISSION

The mission of the Information Security Program is to ensure the right information is available to the right people at the right time.

SCOPE

The scope of the Information Security Program includes all Riverside County information assets.

AUDIENCE

The audience for this document includes all Riverside County personnel with roles listed herein.

TERMINOLOGY

Information Security Incident – The unauthorized modification of, denial of access to or disclosure of an information asset.

Information Asset - Information in any form, created or collected to support Riverside County operations.

Information Security Risk – The combination of the probability of an information security incident occurring and its impact to county finances or constituent confidence.

Information Security Risk Management – The assessment, acceptance and mitigation of information security risk.

Riverside County Department – Any clearly defined functional body governed by the Riverside County Board of Supervisors. This includes but is not limited to Departments, Agencies and Commissions.

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

ROLES AND RESPONSIBILITIES

BOARD OF SUPERVISORS
The Board of Supervisors is responsible for reviewing and ratifying the Information Security Policy (A-58).

COUNTY EXECUTIVE OFFICER (CEO)
The County Executive Officer acts as an agent of the Board of Supervisors to ensure that administrative policies and programs are carried out by departments.

CHIEF INFORMATION SECURITY OFFICER (CISO)
The Chief Information Security Officer is responsible for managing the Information Security Program.

RIVERSIDE COUNTY DEPARTMENT HEAD
Department Heads are responsible for ensuring Departmental participation in the Information Security Program and designating a Department Information Security Officer.

DEPARTMENT INFORMATION SECURITY OFFICER (DISO)
Department Information Security Officers are responsible for ensuring that processes and standards developed by the Information Security Program are communicated and implemented within their Department. The Department Information Security Officer must report directly to either the Department Head or a Deputy Department Head. This title is a designation not an human resources classification.

AUDITOR CONTROLLER
The Auditor Controller is responsible for including information security as a component of their audit plan. The Auditor Controller will collaborate with the Information Security Office on issues related to compliance with the Information Security Program.

REVISION HISTORY

Change Date	Changed by (Name)	Revision	Description of Changes	Approved By	Approval Date
03/16/09	Sebron	1.0	Published Document	Jack B. Miller	03/17/09

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

Riverside County
Information Security Office

Jack B. Miller
Chief Information Security Officer

"The Right information to the Right people at the Right time"

RIVERSIDE COUNTY

INFORMATION SECURITY RISK MANAGEMENT METHODOLOGY

Riverside County Information Security Office
4080 Lemon St • 10th Floor • Riverside, California 92501 • (951) 955-8282 • FAX (951) 955-8070

PURPOSE 3
SCOPE 3
AUDIENCE 3
TERMINOLOGY 3
ROLES AND RESPONSIBILITIES 5
COUNTY EXECUTIVE OFFICER (CEO) 5
CHIEF INFORMATION SECURITY OFFICER (CISO) 5
INFORMATION SECURITY OFFICE (ISO) 5
DEPARTMENT HEAD 5
DEPARTMENT INFORMATION SECURITY OFFICER (DISO) 5
PROCESSES 6
RISK MITIGATION 6
RISK ASSESSMENT 8
RISK ACCEPTANCE 12
REFERENCE SECTION 13
REVISION HISTORY 13

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

PURPOSE

The Riverside County Information Security Risk Management Methodology supports the Riverside County Information Security Program by defining processes for managing information security risk. This methodology defines how information security risks are assessed, accepted and/or mitigated.

SCOPE

The scope of the Information Security Risk Management Methodology includes all Riverside County information assets.

AUDIENCE

The audience for this document includes all Riverside County personnel with roles listed herein.

TERMINOLOGY

Information Security Risk – The combination of the probability of an information security incident occurring and its impact to county finances or constituent confidence.
Information Asset - Information in any form, created or collected to support Riverside County operations.

Information Security Incident - The unauthorized modification of, denial of access to or disclosure of an information asset.

Gap Analysis – A gap analysis is a differential comparison between the required information security processes and standards and the actual implementation of controls. The gap analysis includes remediation plans for all identified gaps.

Vulnerability – An exposure that could result in an information security incident.

Threat – The intent and ability to cause an information security incident.

Mitigating Control - Other controls that reduce the ISIP associated with this particular gap.

Previously Accepted Risk - Other accepted risks that may increase the overall risk associated with this particular gap.

Potential Scenarios - Situations resulting from an information security incident arising from this particular gap.

Information Security Incident Probability (ISIP) – The likelihood of the occurrence of an information security incident. The ISIP is a combination of vulnerability and threat and is classified based on the following parameters.

	High	Medium	Low
Probability	Highly Likely	Probable	Not Likely

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

Operational State – The operating state of the County when an incident occurs. For purposes of quantifying business impact the ISO has defined the following two categories:

- Business As Usual – standard day to day operating paradigm
- Regional Disaster – circumstance where a significant number of business processes are impacted due to a regional event

Business Impact – The repercussions to the County's finances and/or constituent confidence if an information security incident occurs.

Business Impact Rating (BIR) – Logical grouping of business impacts based on the following parameters.

Constituent Confidence		
Severe	**Moderate**	**Minor**
Extensive Dissatisfaction	Moderate Dissatisfaction	Limited Dissatisfaction

County Finances		
Severe	**Moderate**	**Minor**
Monetary Loss greater than $5,000,000	Monetary Loss between $1,000,000 and $5,000,000	Monetary Loss less than $1,000,000

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

ROLES AND RESPONSIBILITIES

COUNTY EXECUTIVE OFFICER (CEO)

The County Executive Officer will escalate Information Security Risks to the Board of Supervisors as necessary.

CHIEF INFORMATION SECURITY OFFICER (CISO)

All risk assessments must be submitted to the Chief Information Security Officer for validation and approval. CISO signatory approval is required for acceptance of all critical, high and medium level information security risks.

INFORMATION SECURITY OFFICE (ISO)

The Information Security Office will develop Information Security Standards to ensure Riverside County's Information Security Risk is appropriately mitigated and assist departments with implementing the Riverside County Risk Management Methodology.

DEPARTMENT HEAD

Department Heads are responsible for ensuring their departments comply with Riverside County's Information Security Risk Management Methodology. Requests to the CISO for acceptance of critical, high and medium information security risks must be submitted by the Department Head.

DEPARTMENT INFORMATION SECURITY OFFICER (DISO)

The Department Information Security Officer is responsible for ensuring that a gap analysis is completed within 90 days of the release of new Information Security Standards. While the ISO is the only organization authorized to document formal information security risk assessments, the DISO is responsible for ensuring Risk Assessments are completed whenever there is or will be non-conformance with an Information Security Standard.

Riverside County Information Security Office
4080 Lemon St • 10th Floor • Riverside, California 92501 • (951) 955-8282 • FAX (951) 955-8070

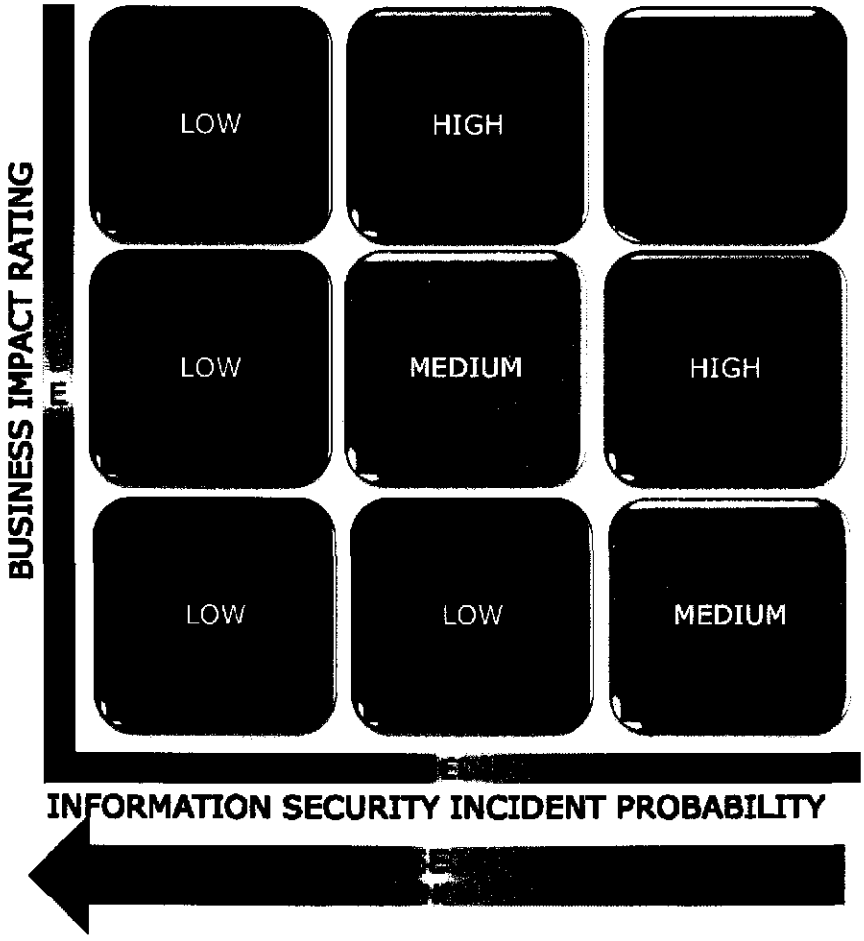
PROCESSES

RISK MITIGATION

Process Overview

The Risk Mitigation Process reduces Riverside County's information security risk to low through the development and implementation of Information Security Standards. Information Security Standards establish the minimum set of controls necessary to reduce the Information Security Incident Probability (ISIP) thereby reducing information security risk. If the controls required by an Information Security Standard will not be implemented, the Risk Assessment Process must be followed to accurately classify the level of risk and the Risk Acceptance Process must be followed to appropriately accept the risk.

RISK CLASSIFICATION MATRIX

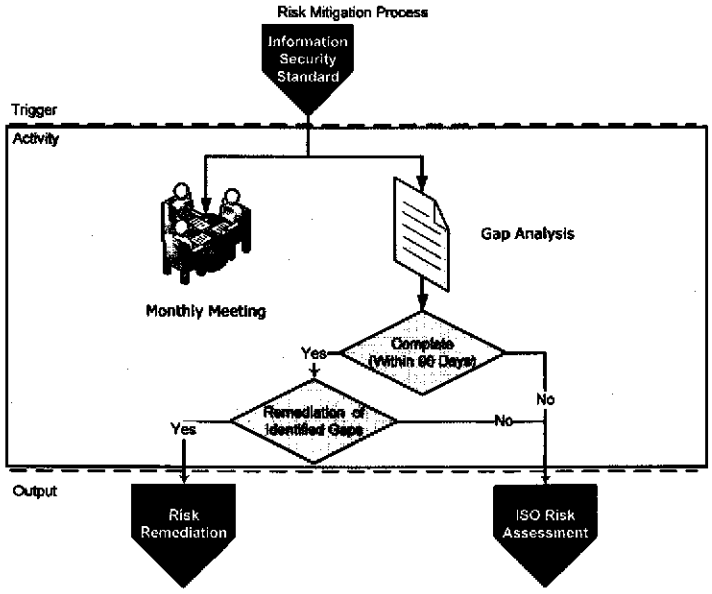


Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

Process Activity

1. ISO will develop Information Security Standards based on information security best practices and regulatory requirements
2. Departments must complete a gap analysis within 90 days of the release of an Information Security Standard
3. ISO will provide Departments with gap analysis templates
4. Departments will provide the ISO with monthly status updates
5. Copies of the completed gap analysis must be provided to the ISO
6. Departments must engage the ISO to complete the Risk Assessment and Acceptance Processes for all identified gaps that will not be remediated
7. Departments must immediately contact the ISO if they determine that they will not be able to complete the gap analysis within the required 90 day timeframe
8. The Risk Assessment and Acceptance Processes must be followed if the gap analysis is going to exceed the 90 day timeframe

Process Flow



Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

RISK ASSESSMENT

Process Overview

The Risk Assessment Process provides a consistent, systematic process to identify, analyze and classify risk. This systematic process must provide comparable and reproducible results. This process is triggered by the identification of a gap or the annual re-evaluation of accepted risk. The output of this process is classified risk. If classified risk will not be mitigated, the Risk Acceptance Process must be followed to ensure the risk is appropriately accepted. Only the ISO is authorized to document formal information security risk assessments.

Process Activity

1. Identify information assets

2. Identify vulnerabilities associated with the area of non-conformance

3. Identify threats that could exploit identified vulnerabilities

4. Identify mitigating controls

5. Identify previously accepted risks
   - Review all currently accepted risks for the identified information assets in order to understand what, if any, relationship this risk may have with any accepted risks.

6. Identify Information Security Incident Probability (ISIP)
   - ISIP will be classified using the following criteria:

	High	Medium	Low
Probability	Highly Likely	Probable	Not Likely

- The ISIP is based on a combination of the following factors:
  - Frequency of attempt – How often is this attack attempted?
  - Ease of exploit – How sophisticated is the attack? Do likely attackers have the skills to execute the attacks?
  - Strength of controls – How vulnerable is the information asset? To what extent do the existing controls mitigate the risk?
  - Are there any currently accepted risks that:
    - Increase the frequency of attempt?
    - Increase the ease of exploit?
    - Reduce the strength of existing controls?
  - Would accepting this risk:
    - Increase the overall level of risk to the department or county?
    - Increase the risk of another currently accepted risk?
    - Increase the reliance on a specific control or set of controls?

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

7. Identify operational state
   - Business as usual
   - Regional disaster

8. Identify potential scenarios

9. Quantify business impact
   - Financial
   - Constituent confidence

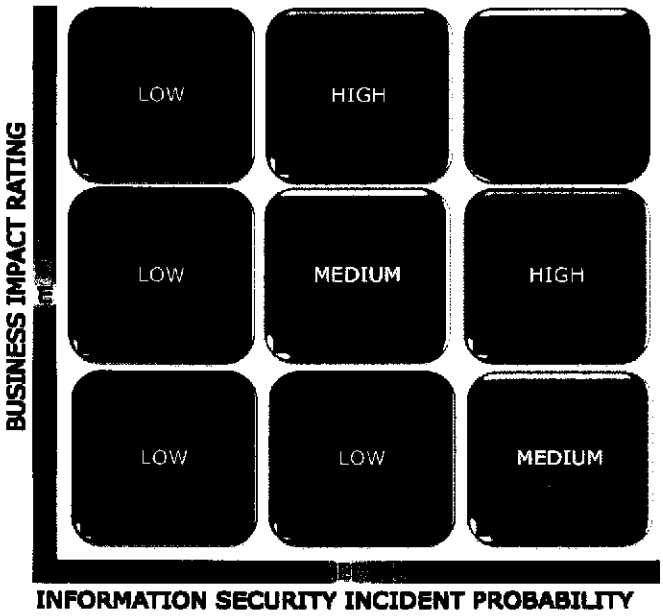
10. Identify Business Impact Rating (BIR)
    - Identify the BIR of an incident. The highest level of identified business impacts must be used for this assessment. BIR is classified based on the following parameters.

Constituent Confidence		
Severe	**Moderate**	**Minor**
Extensive Dissatisfaction	Moderate Dissatisfaction	Limited Dissatisfaction

County Finances		
Severe	**Moderate**	**Minor**
Monetary Loss greater than $5,000,000	Monetary Loss between $1,000,000 and $5,000,000	Monetary Loss less than $1,000,000

11. Classify the risk according to the Risk Classification matrix.

RISK CLASSIFICATION MATRIX



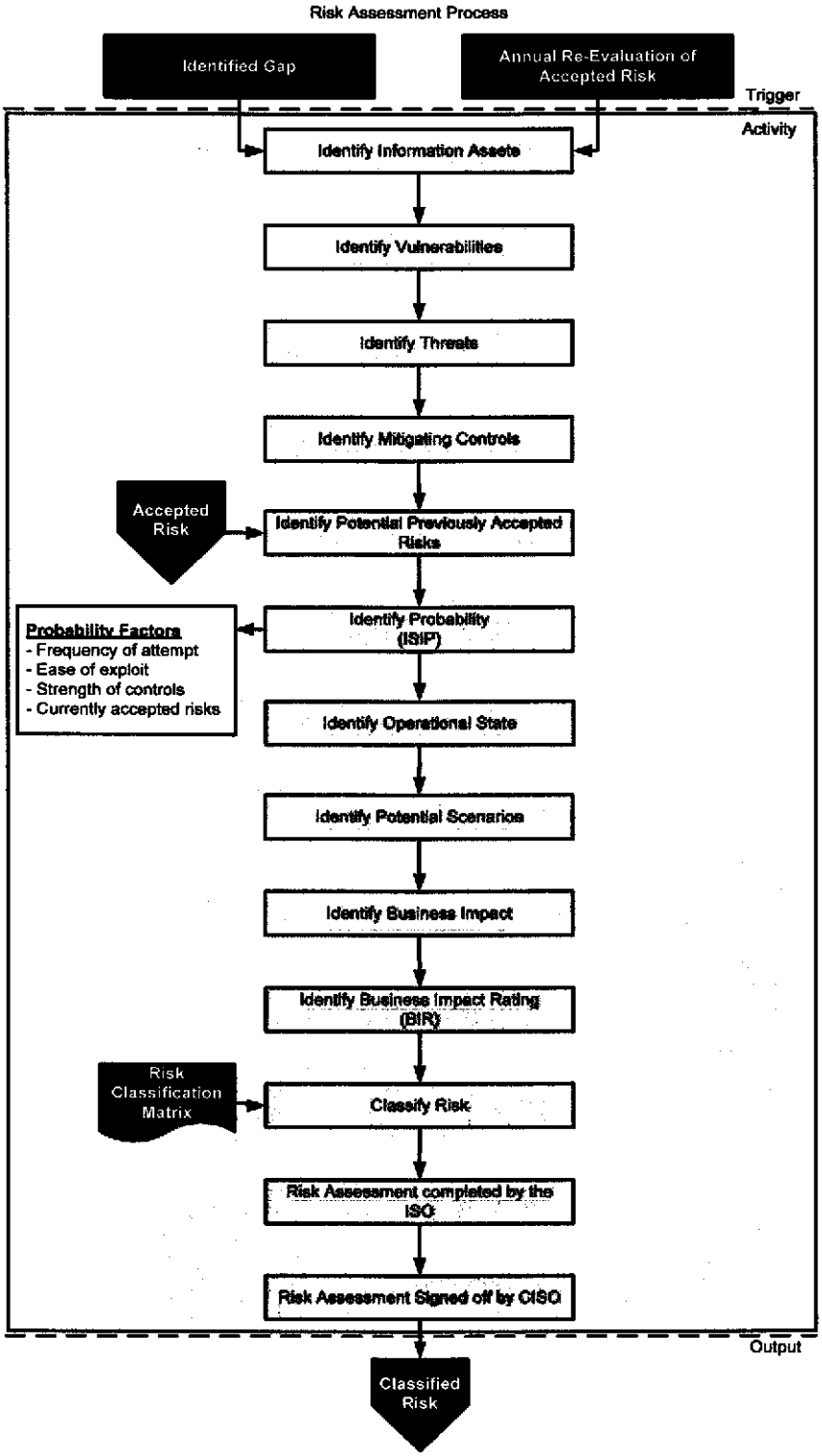
Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

12. Risk Assessment completed by Departmental ISO Representative, reviewed with DISO and submitted to the CISO for signoff.

13. Risk assessment signoff to be completed by the Chief Information Security Officer

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

Process Flow



Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

RISK ACCEPTANCE

Process Overview

The Risk Acceptance Process provides a consistent, structured process to objectively accept information security risk in accordance with Riverside County's risk acceptance criteria. If the Chief Information Security Officer is unwilling to accept the classified risk, the Department will remediate the gap or implement other mitigating controls to reduce the risk to an acceptable level.

Process Activity

1. Acceptance requests submitted to the CISO by the Department Head on the Risk Acceptance Form.

2. ISO to validate the business impact as appropriate (Executive Office, Public Information Officer, Risk Management, County Counsel etc.)

3. Risk accepted
   - CISO will generate and distribute an executive report to the informed parties as identified in the Operational Risk Acceptance Table
   - All risk acceptances for critical and high risks will expire, by default, on an annual basis
   - At time of expiration, each risk must be re-assessed and re-accepted.

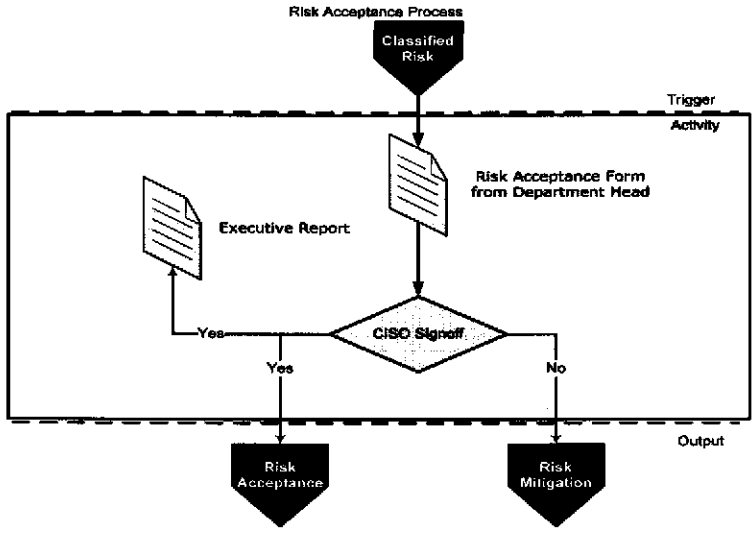
4. Risk not accepted
   - Department will remediate gap or implement other mitigating controls to reduce the risk to a level that Riverside County is willing to accept

Operational Risk Acceptance Table

Risk Classification	Authorized Acceptor(s)	Informed Parties
CRITICAL RISK	CISO	Executive Office
HIGH RISK	CISO	Executive Office
MEDIUM RISK	CISO	Executive Office
LOW RISK	DEFAULT ACCEPTANCE	Not Applicable

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070

Process Flow



REFERENCE SECTION

N/A

REVISION HISTORY

Change Date	Changed by (Name)	Revision	Description of Changes	Approved By	Approval Date
03/16/09	Sebron	1.0	Published Document	Jack B. Miller	03/17/09

Riverside County Information Security Office
4080 Lemon St ● 10th Floor ● Riverside, California 92501 ● (951) 955-8282 ● FAX (951) 955-8070