CITY OF
ROSEVILLE
CALIFORNIA

Enterprise Security Strategic Plan for 2012-2015

Prepared
for

Enterprise Security Committee

Prepared
by

Enterprise Security Steering Committee

May 2012

Table of Contents

Enterprise Security Strategic Plan for *2012-2015*

City of Roseville / Enterprise Security Committee – May 2012

INTRODUCTION

In February of 2012 the City of Roseville moved forward with the implementation of the Enterprise Security Committee for the purpose of:

- Work to reduce threats to physical and information security, while looking for solutions that make efficient use of resources.
- Protect customer's private/personal information.
- Prevent loss of property.
- Development, oversight, and monitoring of Compliance Program.

In order to achieve the above mentioned goals or desired state, the Steering Committee's initial efforts focused on staffing the subcommittees, developing a Charter (Appendix A), and Guiding Principles (Appendix B). The Charter and Guiding Principles provide the foundation for the committee to develop the Strategic Plan.

METHODOLOGY

This Security Strategic Plan was developed following the methodology shown on Figure-1 below. That is:

1) Identify **Actual State** of security
2) Identify **Desired State**
3) Identify **Objectives.** These objectives must be aligned with the organization's strategic objectives.
4) Define a **Strategy** that will give the highest probability of success in achieving the Objectives. Cost, risk, duration, available resources, etc., will help define the Strategy.
5) Identify steps / **Projects** needed to achieve Objectives. The collection of these projects constitutes the Security Program.
6) Projects within the Security Program are identified as Short-term, Mid-term, and Long-term. Normally the **classification** in terms of duration is less than 3 months for Short-term, 3 to 6 months for Mid-term, and over 6 months for Long-term projects.
7) Finally, projects identified in step 5, are **prioritized** in terms of risk and cost.

Although the **Guiding Principles** are not a specific step in formulating the Strategic Plan, they guide the decision making process at each step.

It is important to note that the Strategic Plan should be revised periodically to adjust to the changing needs of the organization.

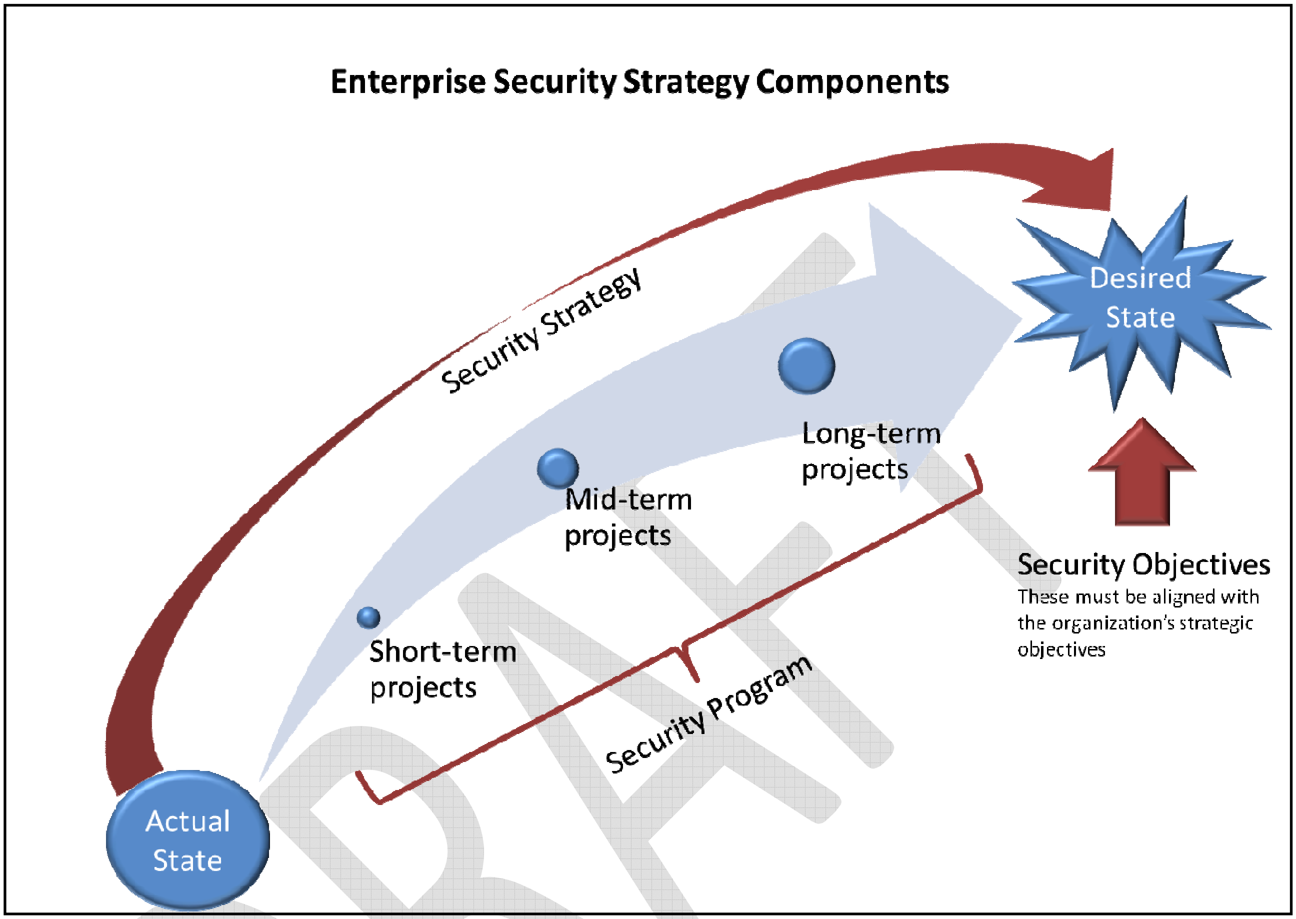


Figure - 1

A very simplistic example of how this methodology could be applied follows:

Actual State: We are at war

Desire State: Peace

Objective: Win the war

Strategy: Divide and conquer

Program: Infiltrate enemy lines, Intercept enemy communications, and disseminate false information. These will be classified as long, mid, or short-term, and prioritize in terms of risk.

Guiding principles: We will adhere to Geneva Convention rules of warfare, we will not attack civilians, we will work to reduce casualties on both sides, etc.

STRATEGIC PLAN

1) Actual State

Over that last 12 months, the City of Roseville has engaged in several efforts that provide clarity regarding the Actual State of security in both Information Security and Physical Security. In no particular order these efforts include:

- Department of Homeland Security, 2011 Nationwide Cyber Security Review (Annual).
- Payment Card Industry (PCI) Data Security Standard Self-Assessment (Annual).
- Gap Analysis of Critical Infrastructure Protection. Audit by Encari, LLC (April 2011)
- Security Risk Assessment by Threat Analysis Group (May 2011). This physical security assessment included three sites: Electric Corp Yard, Corporation Yard, Civic Center, and Alternative Transportation.
- Information Systems Review by Maze & Associates (Annual)
- Security Compliance Assessment by Moss Adams LLP (2011)

There are a few observations to be made based on the information provided by these efforts. First, there is no one assessment that covers the depth and breadth of all these combined. A detailed and more narrowly focused assessment is not needed in every case. This is because there are areas of greater risk, or areas specific to compliance mandates. Some assessments, such as the PCI self-assessment, are specific to a single application (credit card payment processing) while others are specific to an entire department and services the department provides such is the case of Electric Utility (NERC). Second, although these efforts vary in scope, the result is a clearer picture of the current state of security. Third, some of these assessments, such as PCI-DSS Self-Assessment, are required recurring efforts. Fourth, it should be noted that in addition to the above sited efforts, future assessments such as the Criminal Justice Information Services (CJIS) audit review are already planned for this year. These may reveal areas of further improvement.

2) Desired State

The Desired State of the City of Roseville as it relates to Information/Cyber and Physical Security must have:

- An environment that reduces threats to physical and information/cyber security, with solutions that make efficient use of resources.
- An environment that protects customer’s private/personal information.
- An environment that prevents loss of property.
- A Security Compliance Program with oversight and monitoring.

3) Objectives

The Objectives of the Enterprise Information/Cyber and Physical Security Committee and for this Strategic Plan are:

- Establish a uniform approach for maintaining, developing, and implementing a Citywide Security Program.
- Ensure the availability, confidentiality, and integrity of the information systems of the City, by providing leadership, guidance and overall strategy for Cyber and Physical Security.
- Establish a Security Awareness and Training Program.
- Ensure regulatory compliance, maintaining a risk management program (including but not limited to policies), establishing incident/emergency response teams, as well as other security-related responsibilities.
- Periodic risk assessments and audits.

Alignment of Strategic Objectives

It is important to note that the above sited objectives are aligned and in support of:

a) **City of Roseville's goals:** "A Complete and Well-Managed Community Infrastructure" and "A Healthy, Safe and Secure Community"

b) **City Council Priorities:** "Maintain City Infrastructure"

c) **Vision and Mission of the City:** "One City" because the Enterprise Security Committee is the result of a collaboration effort by multiple departments looking for a synergistic approach. "Open for Business" because it focuses on continuity of normal business operation. "Urban to Metropolitan" because it brings the City of Roseville to a higher level of organizational maturity, in regards to security, which will allow the City to adjust to a changing environment as it grows.

4) Strategy

Although the City of Roseville has been affected by the economic downturn, it remains committed to the overall security of the organization. At the same time given the limited resources, there is recognition that in order to achieve the City's objectives a sensible strategy must be implemented. The Steering Committee recommends a multi-step approach. These are:

A) Based on efforts identified in Section 1 (Actual State) develop two comprehensive lists of action items in the areas of Physical Security and Information/Cyber Security. It is expected that these lists will represent a significant number of items aimed at closing gaps between Actual State and Desire State.

B) Although there is more than one methodology available to prioritize these efforts, the Steering Committee recommends the utilization of a Risk Probability/Impact Matrix (see Figure-2 below). This will provide each project a Risk Assessment Code (RAC) of between 1 and 5.

C) Once items are prioritized in terms of Risk Probability/Impact further analysis may be needed to prioritize even further in case of multiple projects with the same RAC score. The Steering Committee recommends the use of Weights and Counts methodology: Using this approach, a weight is assigned to each aspect. For example, Regulatory Compliance and Audit findings may be weighed more heavily than Other benefits. Next, the count is determined by simply counting the number of audit findings that are remedied by the project. In the end, the quantitative score is expressed as follows:

Project Quantitative Score (PQS) = C_{reg} x W_{reg} + C_{audit} x W_{audit} + C_{OT} x W_{OT}

C_{reg}= Count of regulatory compliance that will be met by the project

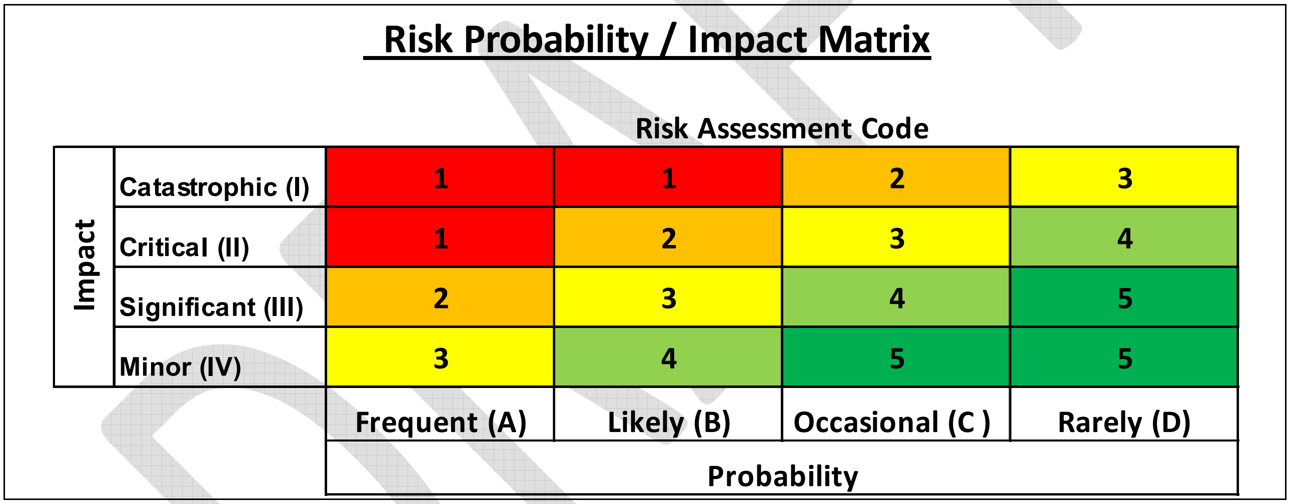
W_{reg}= Weight for regulatory compliance

C_{audit} = Count of audit findings remedied by the project

W_{audit} = Weight for audit findings

C_{OT}= Count of other benefits from the project

W_{OT}= Weight for other benefits



Risk Probability / Impact Matrix

		Risk Assessment Code			
Impact	Catastrophic (I)	1	1	2	3
	Critical (II)	1	2	3	4
	Significant (III)	2	3	4	5
	Minor (IV)	3	4	5	5
		Frequent (A)	Likely (B)	Occasional (C)	Rarely (D)
		Probability			

Figure – 2

D) Finally projects with the lowest RAC score and the highest PQS score should be targeted first.

It should be noted that there may be situations in which regardless of the score, and based on resources and cost, a project may need to be postponed. In these cases, the subcommittees will be asked to provide options for compensating controls.

Note: For a list definition of terms used in Figure – 2 impact levels please refer to Appendix – A.

5) Program

The completion of step 4 above will produce a deliverable that will define a number of projects. The collection of these projects will form the City’s Security Program. It is important to note that establishing a Security Program is not a onetime event, but an ongoing venture that follows a cyclical process. The implementation phases (see Figure – 3 below) are not cleanly separated processes, but instead represent a flow of activities that yield an ever maturing Program. The implementation cycle involves establishing security requirements, educating people about their responsibilities under those requirements, building governance structures to ensure Program compliance, and monitoring and reporting of progress.

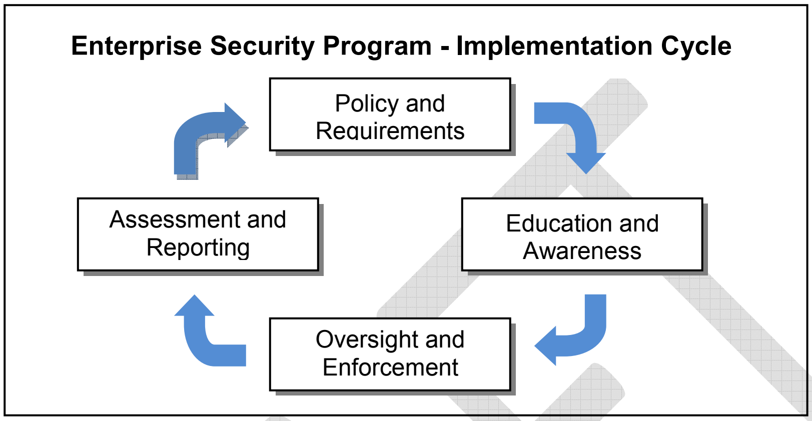

Enterprise Security Program - Implementation Cycle
Policy and Requirements
Education and Awareness
Oversight and Enforcement
Assessment and Reporting

Figure - 3

6) Guiding Principles

A) Governance: Security is the responsibility of everyone in the organization.

B) Accountability: Security responsibilities should be made explicit.
The responsibilities and accountability of City assets and information should be explicit.

C) Awareness: Personnel need to have an effective level of security awareness.
Senior management is committed to ensure security awareness is achieved agency-wide.

D) Aligned: Information and physical security supports the mission of the organization.
Security rules and procedures do not exist for their own sake but are put in place to protect important assets and support the overall City mission. Security is intended to improve the service provided to all customers.

E) Proportionate: Security should be cost effective and proportionate.
City security policies, practices, procedures, standards, security levels and costs should be appropriate and proportionate. Security measures will vary among systems and programs. A business analysis will be performed considering the severity, probability and extent of potential harm to determine the level of security applied.

F) Integration: Security requires a “One City”, comprehensive and integrated approach.
Effective information security requires a comprehensive approach that considers a variety of areas throughout the entire enterprise. City policies, standards, practices and procedures for the security should be coordinated and comprehensive to create a

coherent system of security. This considers other practices and procedures of the organization.

G) Timeliness: Security actions should be timely.
City personnel and business partners should act in a timely and coordinated manner to prevent and respond to breaches in security.

H) Reassessment: Security should be periodically reassessed.
The security of City resources and these policies should be reassessed at least annually.

Appendix A

Risk Impact Level - Definitions

Catastrophic	Greater than $1 million	Cyber	Complete breach of sensitive or classified information, sabotage, or closure of business. Loss of confidentiality, integrity, or availability leads to a **catastrophic** effect on the organization.
		Physical	Total loss of property; irreversible environmental damage, or business closure
Critical	$200,000 – $1 million	Cyber	Long term loss of one or more primary mission capabilities. Loss of confidentiality, integrity, or availability leads to a **critical** effect on the organization.
		Physical	Severe damage, major loss, reversible environmental damage, or violation of law/regulation
Significant	$10,000 – $200,000	Cyber	Long term loss of one or more minor or temporary loss of one or more primary mission capabilities. Loss of confidentiality, integrity, or availability leads to a **significant** effect on the organization.
		Physical	Minor damage, minor loss, or mitigatable environmental damage where restoration activities can be done
Minor	$2,000 – $10,000	Cyber	Temporary loss of one or more minor mission capabilities. Loss of confidentiality, integrity, or availability leads to a **minor** effect on the organization.
		Physical	Less than minor injury/illness, less than minor mission loss, or minimal environmental damage