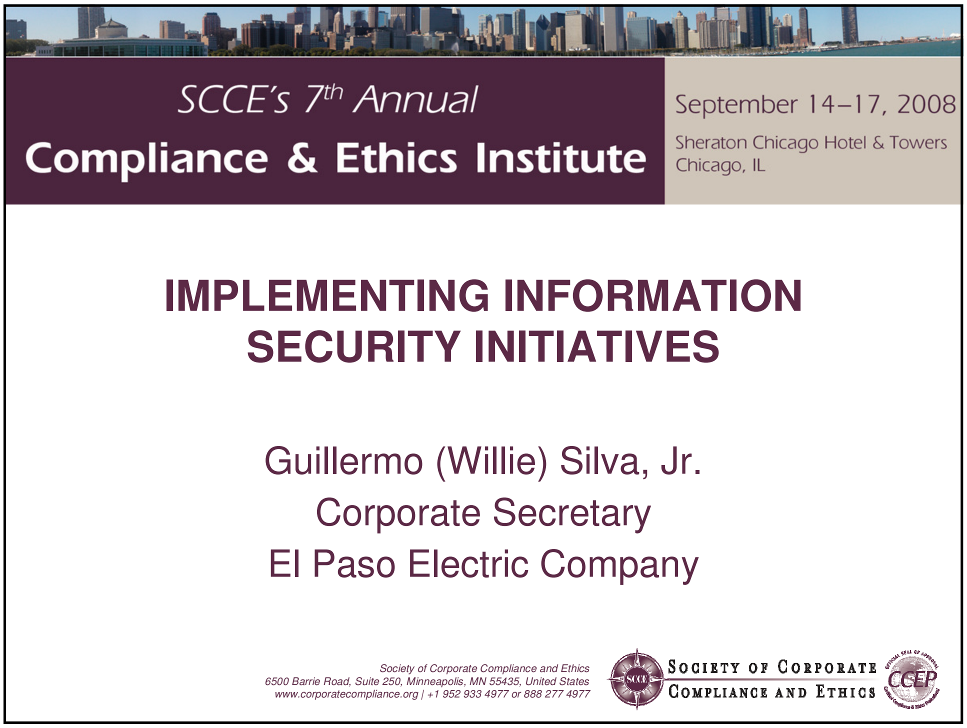


SCCE's 7th Annual

Compliance & Ethics Institute

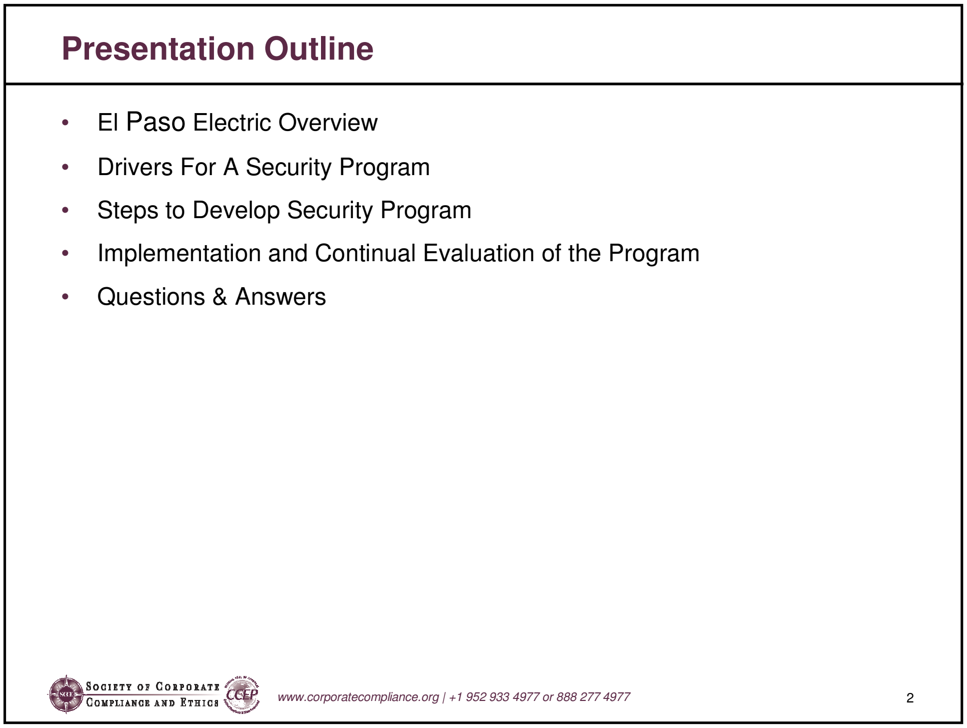
September 14–17, 2008

Sheraton Chicago Hotel & Towers
Chicago, IL

IMPLEMENTING INFORMATION SECURITY INITIATIVES

Guillermo (Willie) Silva, Jr.
Corporate Secretary
El Paso Electric Company

Society of Corporate Compliance and Ethics
6500 Barrie Road, Suite 250, Minneapolis, MN 55435, United States
www.corporatecompliance.org | +1 952 933 4977 or 888 277 4977

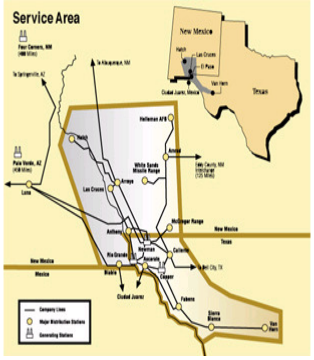


Presentation Outline

- El Paso Electric Overview
- Drivers For A Security Program
- Steps to Develop Security Program
- Implementation and Continual Evaluation of the Program
- Questions & Answers

El Paso Electric Overview

- Regional electric utility serving west Texas and southern New Mexico
- 351,000 retail customers



El Paso Electric Overview (cont.)

- 978 employees
- Above average retail sales growth
- Approximately 1500 MW – gas, coal, and nuclear
- Status of retail competition:
  - Deferred for at least several years in Texas
  - Repealed in New Mexico
- Interconnected with WECC
- Ability to serve load in Mexico

The Electric Company®
EL PASO ELECTRIC

Drivers For An Information and Information Security Program

Information Management Security Programs are often neglected due to resource constraints until one of the following occurs:

- Natural disaster
- Information security breach
- Non-compliance event
- Misinformation provided to the public

Drivers For An Information and Information Security Program (cont.)

In the event of a natural disaster/service interruption - information management is heightened:

- Protection of information systems
  - Computer systems
  - Communication systems
- Procedures for external communications to the public – reliable source issues

Drivers For An Information and Information Systems Security Program

- Corporate Governance
- Sarbanes – Oxley Compliance
- NERC CIP SubStandards (Critical Infrastructure Protection)
- FERC Order 2004 Standard of Conduct Compliance
- Post 9/11 Heightened Awareness
- Company Internal Code of Conduct and Code of Ethics
- HIPAA

Common Thread – **Compliance**

Drivers For An Information and Information Systems Security Program (cont.)

Internal Drivers:

- Risk Management Programs assign a level of risk tolerance to contingency planning, or strategies and procedures, to maintain and resume critical business functions in the event of a business disruption.
- Corporate Audit Committees polled by KPMG International's Audit Committee Institute ranked the following as 2007 priorities:

Risk Management	-	61%
Internal Controls	-	61%
Accounting Judgments and Estimates	-	50%
Legal/Regulatory Compliance	-	36%

- Information Security ranked top of the KPMG International's Audit Committee Institute survey at 78% in 2006.

Steps to Develop a Security Program

Step 1 – Conduct a security audit

Audits to identify vulnerabilities with security and overall compliance with internal policies and procedures.

Steps to Develop a Security Program (cont.)

Step 2 – Evaluated audit findings and implemented recommendations

- Ratification of the Company's Information and Information Systems Security Plan and Policies
- Technical Enhancements
- Creation / Update of Policies and Procedures
- Roll-out plan for Information Management and Information Systems Security Program
- Definition of Continuing Education Plan
- Definition of Continuing Assessment Program

Steps to Develop a Security Program (cont.)

Step 3 – IT Executive Council Role

– Nomenclature of the Council is not important

The Council's mission is to ensure that:

- Technology projects are aligned with corporate goals;
- Project proposals are evaluated, weighted and prioritized against all other IT projects;
- Corporate budget considerations are evaluated for each project
- Each project proposal includes a formal business case.

Steps to Develop a Security Program (cont.)

Step 3 – IT Executive Council Role (cont.)

Members of the IT Council include:

VP – Information Services, Chair

VP – Power Generation

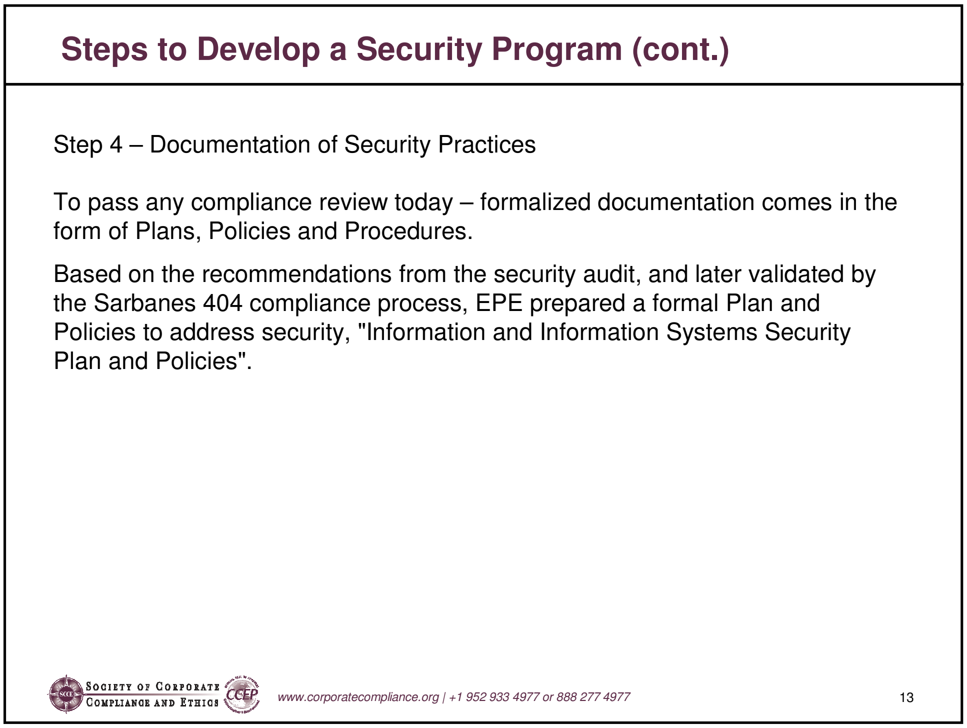
VP – Transmission and Distribution

VP – Corporate Planning and Controller

VP – Administration

VP – Power Marketing and International Business

VP – Regulatory Affairs and Treasurer

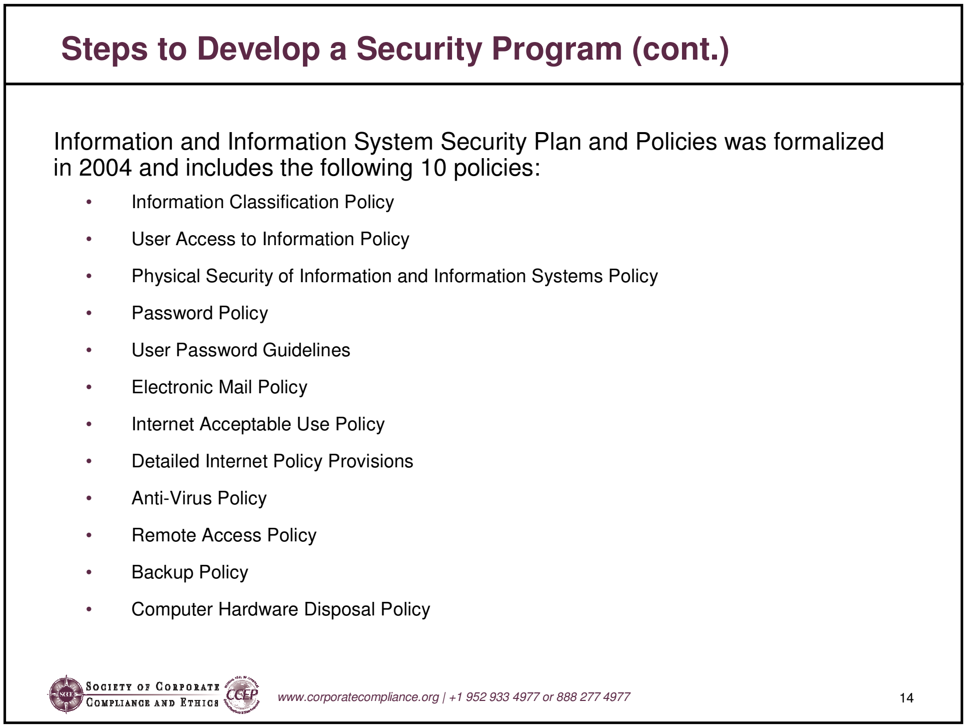


Steps to Develop a Security Program (cont.)

Step 4 – Documentation of Security Practices

To pass any compliance review today – formalized documentation comes in the form of Plans, Policies and Procedures.

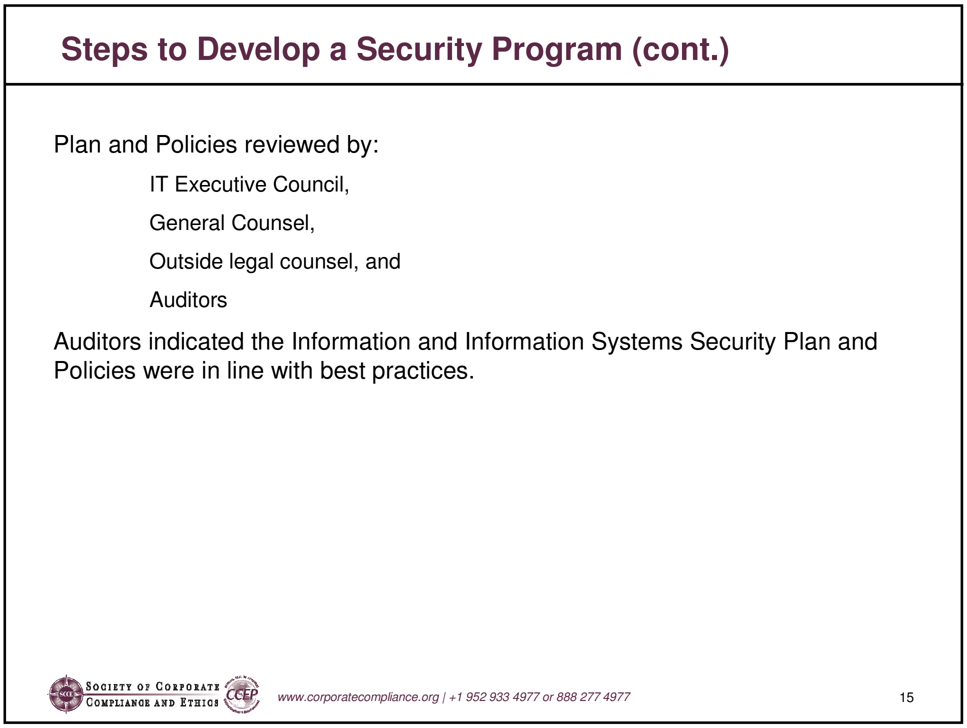
Based on the recommendations from the security audit, and later validated by the Sarbanes 404 compliance process, EPE prepared a formal Plan and Policies to address security, "Information and Information Systems Security Plan and Policies".



Steps to Develop a Security Program (cont.)

Information and Information System Security Plan and Policies was formalized in 2004 and includes the following 10 policies:

- Information Classification Policy
- User Access to Information Policy
- Physical Security of Information and Information Systems Policy
- Password Policy
- User Password Guidelines
- Electronic Mail Policy
- Internet Acceptable Use Policy
- Detailed Internet Policy Provisions
- Anti-Virus Policy
- Remote Access Policy
- Backup Policy
- Computer Hardware Disposal Policy



Steps to Develop a Security Program (cont.)

Plan and Policies reviewed by:

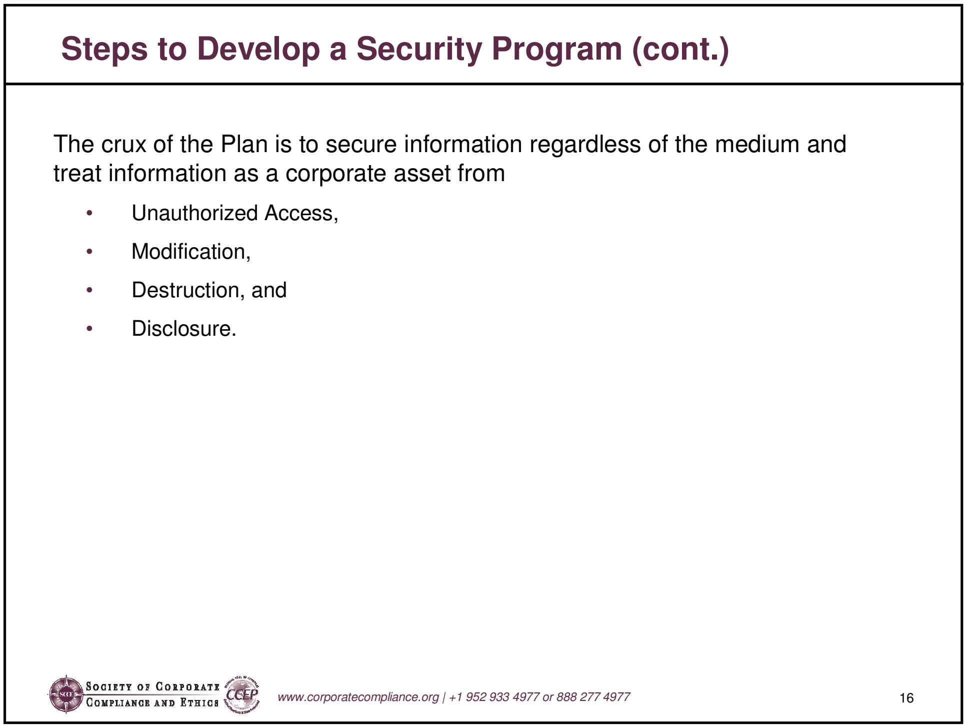
IT Executive Council,

General Counsel,

Outside legal counsel, and

Auditors

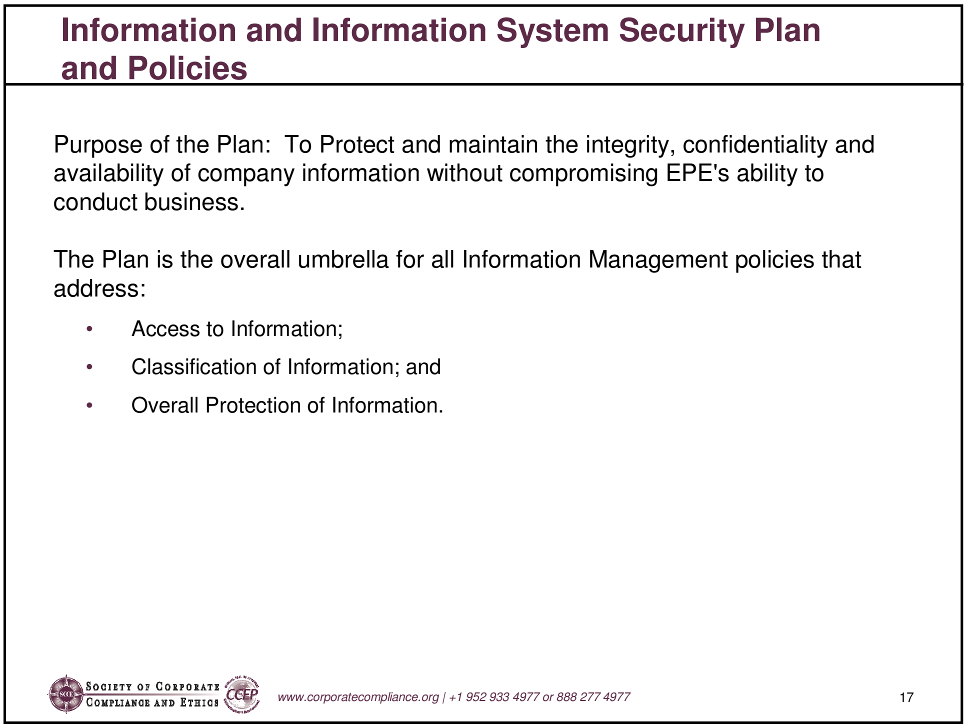
Auditors indicated the Information and Information Systems Security Plan and Policies were in line with best practices.



Steps to Develop a Security Program (cont.)

The crux of the Plan is to secure information regardless of the medium and treat information as a corporate asset from

- Unauthorized Access,
- Modification,
- Destruction, and
- Disclosure.

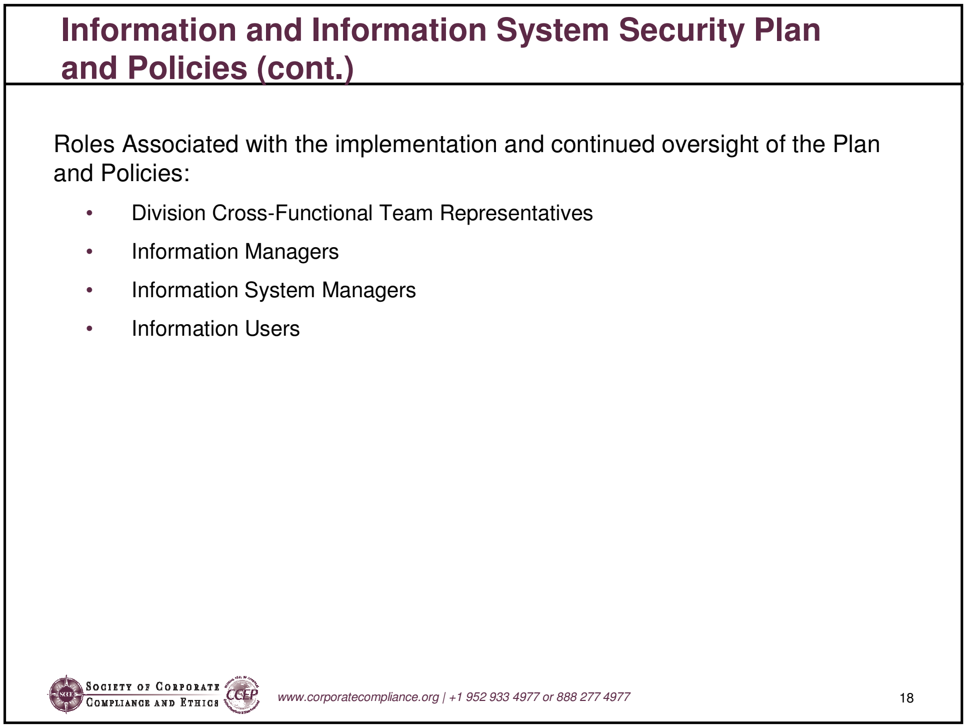


Information and Information System Security Plan and Policies

Purpose of the Plan: To Protect and maintain the integrity, confidentiality and availability of company information without compromising EPE's ability to conduct business.

The Plan is the overall umbrella for all Information Management policies that address:

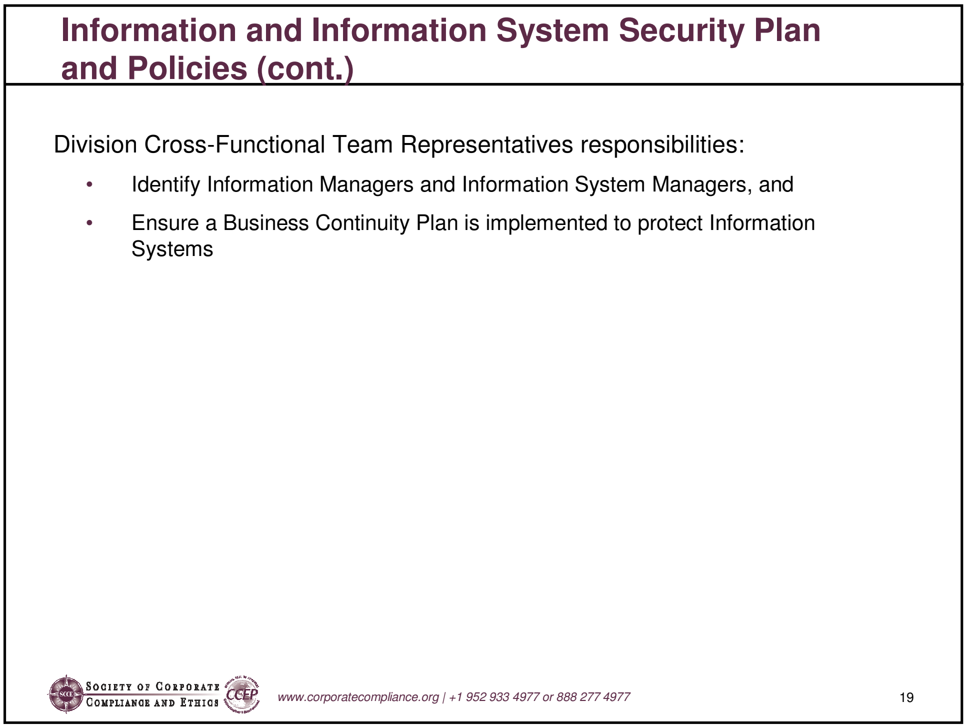
- Access to Information;
- Classification of Information; and
- Overall Protection of Information.



Information and Information System Security Plan and Policies (cont.)

Roles Associated with the implementation and continued oversight of the Plan and Policies:

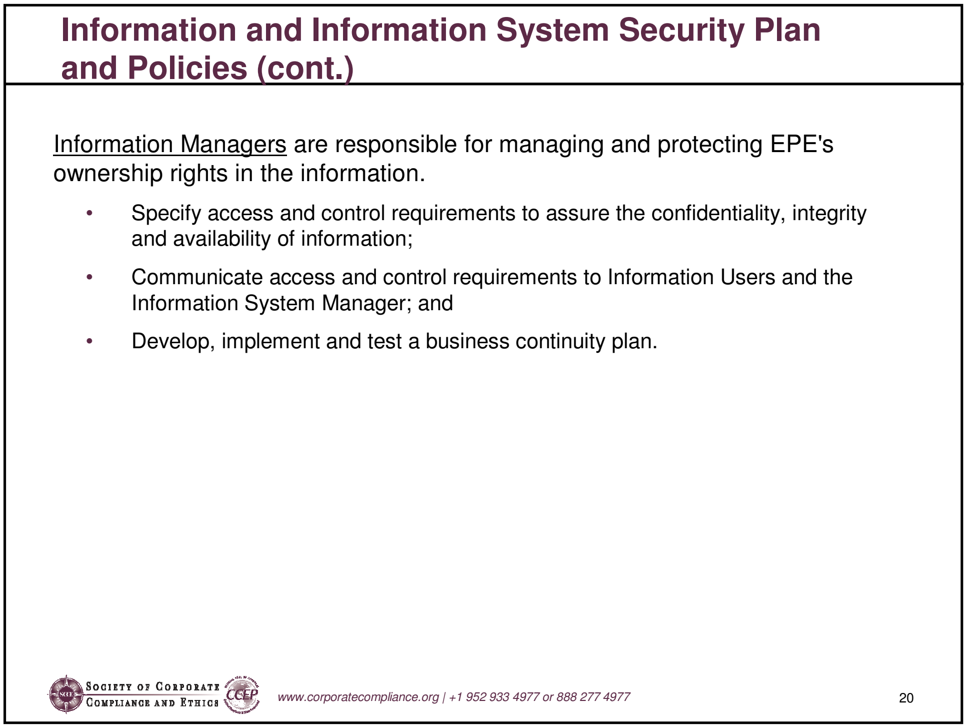
- Division Cross-Functional Team Representatives
- Information Managers
- Information System Managers
- Information Users



Information and Information System Security Plan and Policies (cont.)

Division Cross-Functional Team Representatives responsibilities:

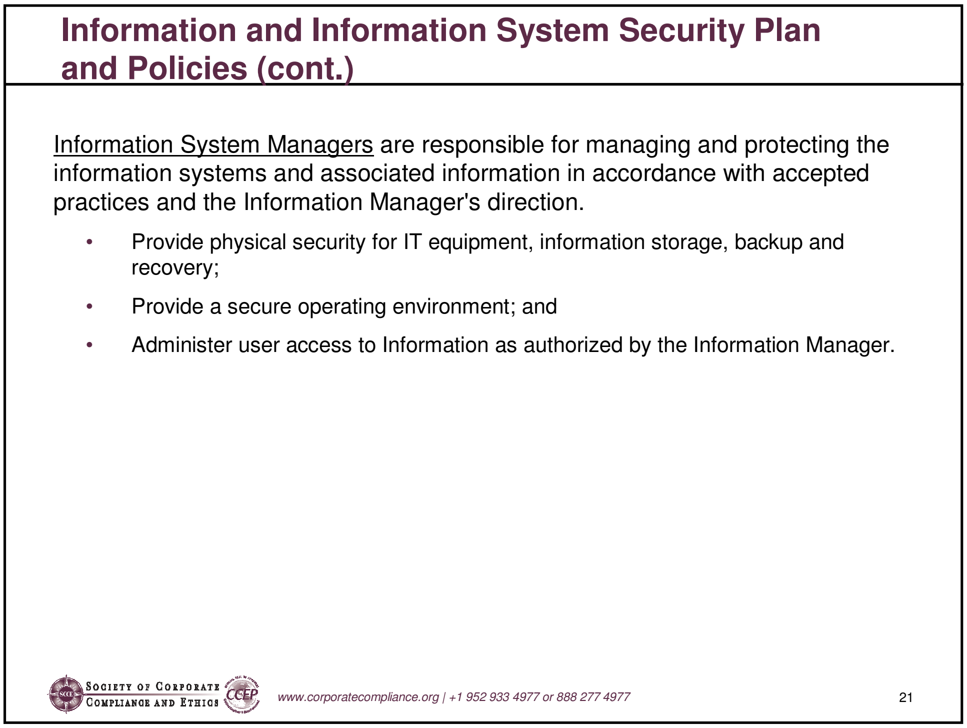
- Identify Information Managers and Information System Managers, and
- Ensure a Business Continuity Plan is implemented to protect Information Systems



Information and Information System Security Plan and Policies (cont.)

Information Managers are responsible for managing and protecting EPE's ownership rights in the information.

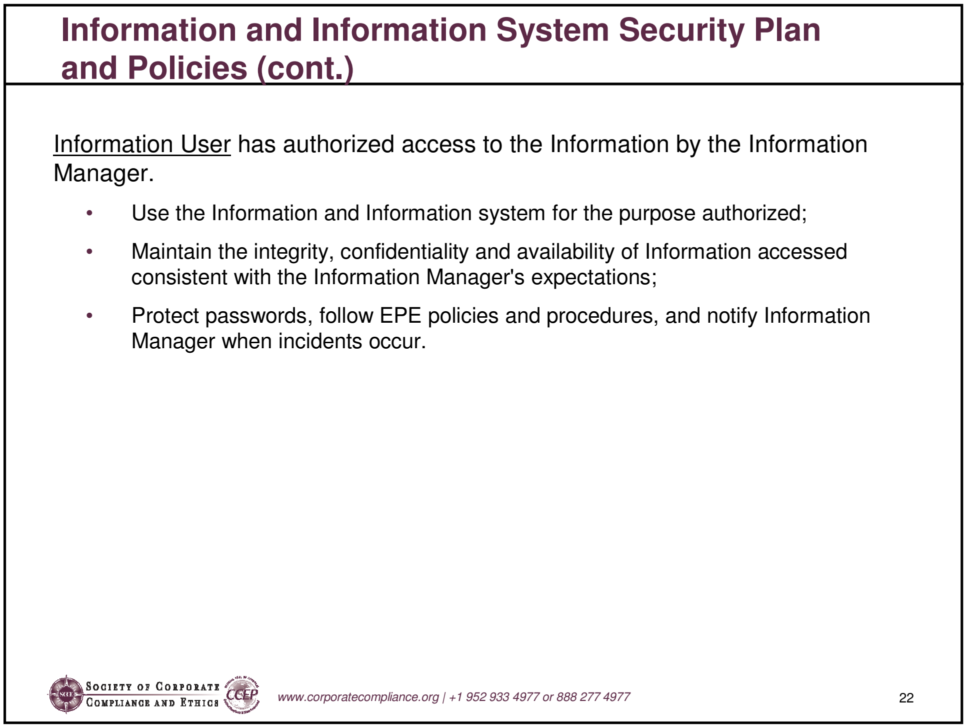
- Specify access and control requirements to assure the confidentiality, integrity and availability of information;
- Communicate access and control requirements to Information Users and the Information System Manager; and
- Develop, implement and test a business continuity plan.



Information and Information System Security Plan and Policies (cont.)

Information System Managers are responsible for managing and protecting the information systems and associated information in accordance with accepted practices and the Information Manager's direction.

- Provide physical security for IT equipment, information storage, backup and recovery;
- Provide a secure operating environment; and
- Administer user access to Information as authorized by the Information Manager.



Information and Information System Security Plan and Policies (cont.)

Information User has authorized access to the Information by the Information Manager.

- Use the Information and Information system for the purpose authorized;
- Maintain the integrity, confidentiality and availability of Information accessed consistent with the Information Manager's expectations;
- Protect passwords, follow EPE policies and procedures, and notify Information Manager when incidents occur.

Implementation and Continual Evaluation of the Program

Heightening employee awareness to security concerns was gradual, yet has been continuous since the inception of the Security Program.

- All desktop monitors are set to "lock-out" to a screen saver when there has been 15 minutes of inactivity on the desktop. Employees are required to enter a password in order to access the desktop.

1st security measure that had a visible / direct impact on employees.

Implementation and Continual Evaluation of the Program (cont.)

Roll-out of the "Information and Information systems Security Plan and Policies" was a **key** component of the Security Program. This involved:

- Production of the Plan and Policies in booklet form with a letter from the CFO encouraging employee support and compliance.
- Posted Plan and Policies on the EPE intranet site.
- Conducted Mandatory employee training:
  - Management Team (Officers, Directors, Managers and Supervisors) – conducted in 4 meetings in groups of 25 with a Power Point Presentation
  - Online interactive employee training (developed in-house)
- Established cross functional team to assist with the Implementation of the Plan

Implementation and Continual Evaluation of the Program (cont.)

Maintaining employee awareness to security of information and information systems comes in many forms:

- Communications through the employee newsletter in the form of cartoons and articles
- Reminders posted online to the intranet site about specific polices – i.e., 12 character requirement for passwords
- Provide refresher training

Implementation and Continual Evaluation of the Program (cont.)

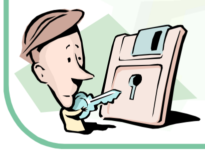
SPEAKING ABOUT INFORMATION SYSTEMS

Question:

Who is responsible for monitoring access to all the different information systems of EPE?

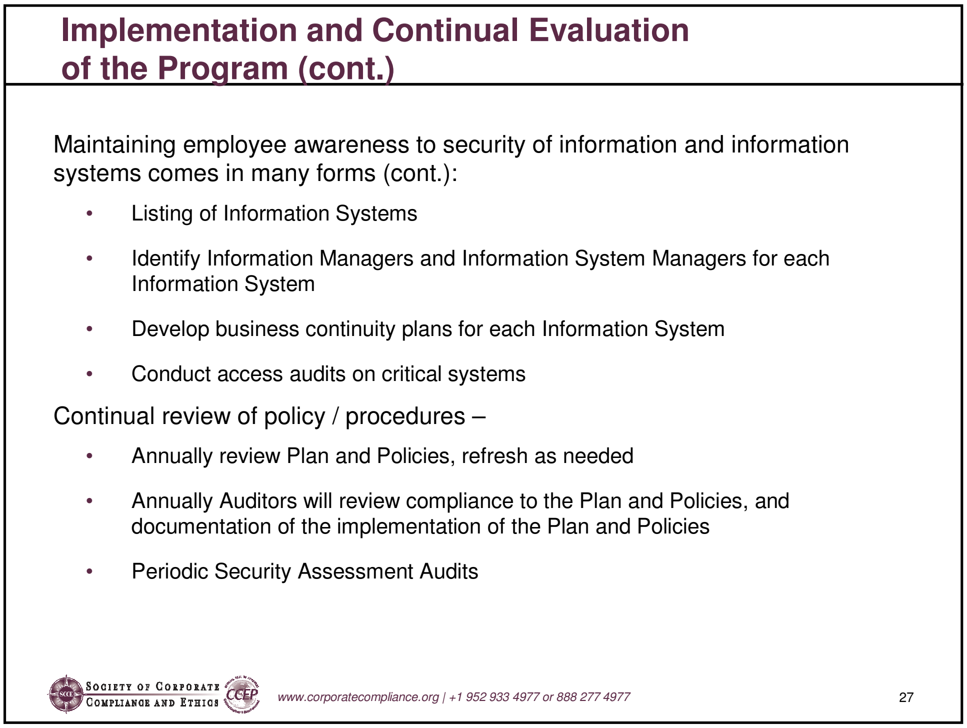
Answer:

The Information Manager of the System authorizes both access and the level of access to be granted to each user, in writing to IT. Upon receipt of the written notice, IT will enable access for the user as instructed.



Reference:

EPE Information and Information Systems Security Plan and Policies, User Access to Information Policy, Page 11.



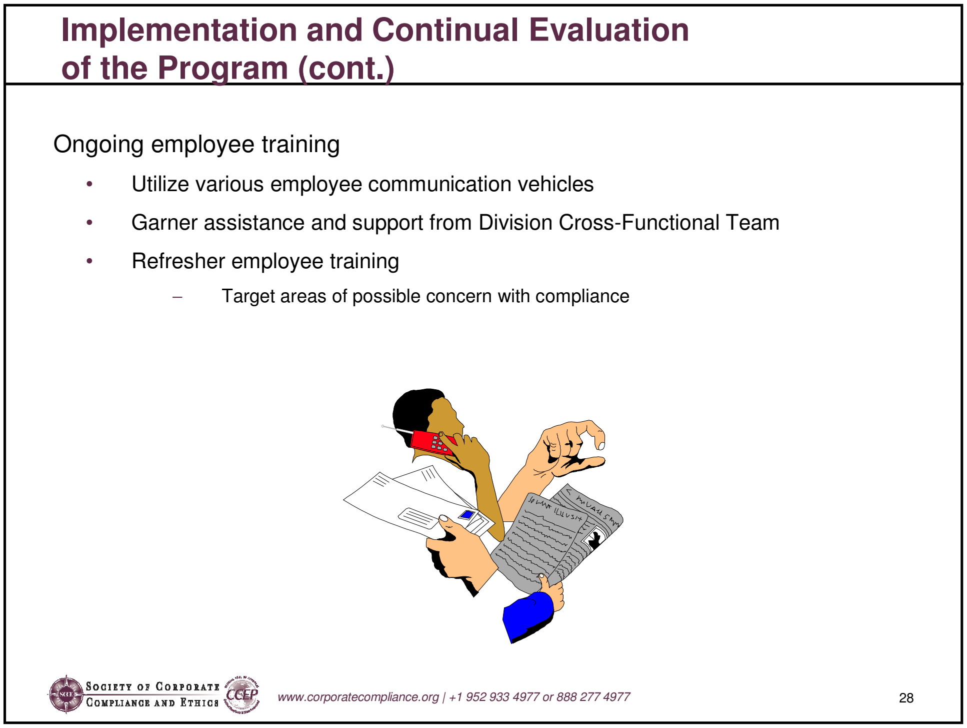
Implementation and Continual Evaluation of the Program (cont.)

Maintaining employee awareness to security of information and information systems comes in many forms (cont.):

- Listing of Information Systems
- Identify Information Managers and Information System Managers for each Information System
- Develop business continuity plans for each Information System
- Conduct access audits on critical systems

Continual review of policy / procedures –

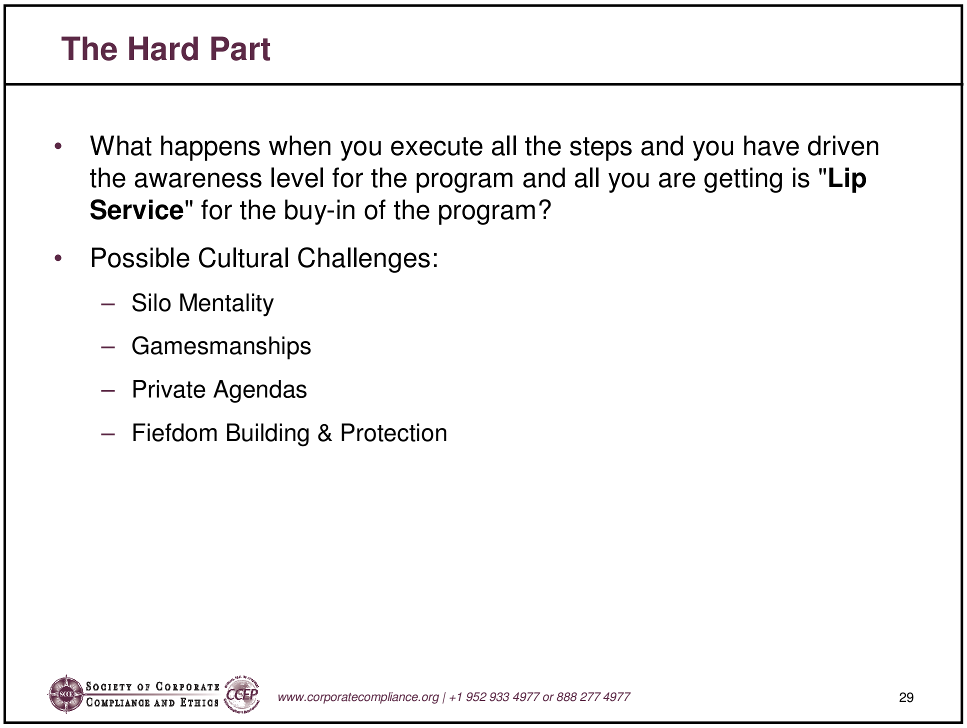
- Annually review Plan and Policies, refresh as needed
- Annually Auditors will review compliance to the Plan and Policies, and documentation of the implementation of the Plan and Policies
- Periodic Security Assessment Audits



Implementation and Continual Evaluation of the Program (cont.)

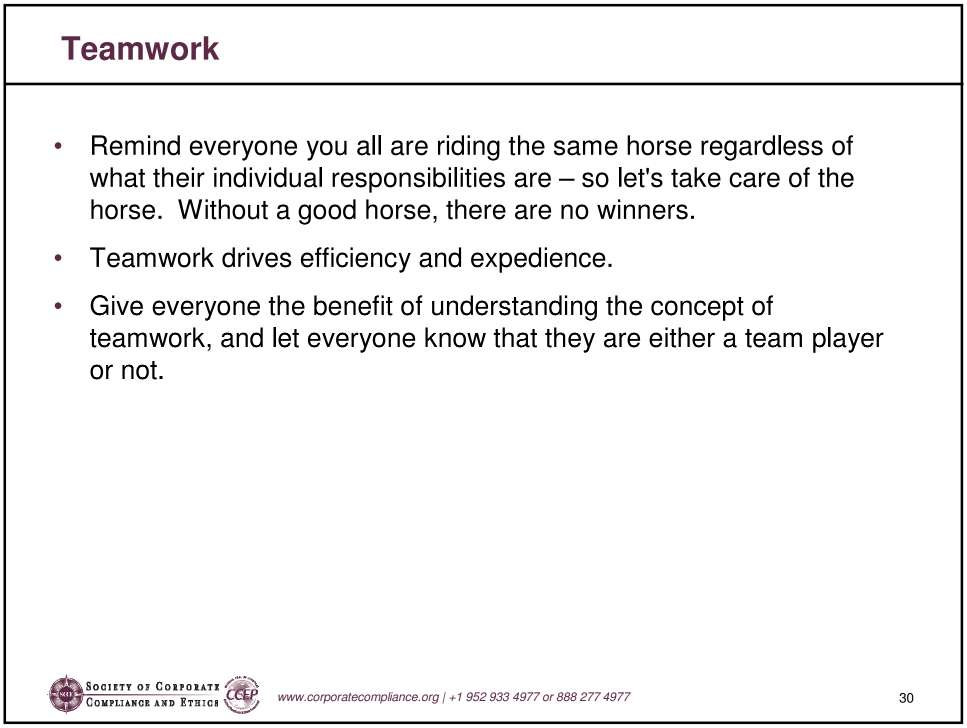
Ongoing employee training

- Utilize various employee communication vehicles
- Garner assistance and support from Division Cross-Functional Team
- Refresher employee training
  - Target areas of possible concern with compliance



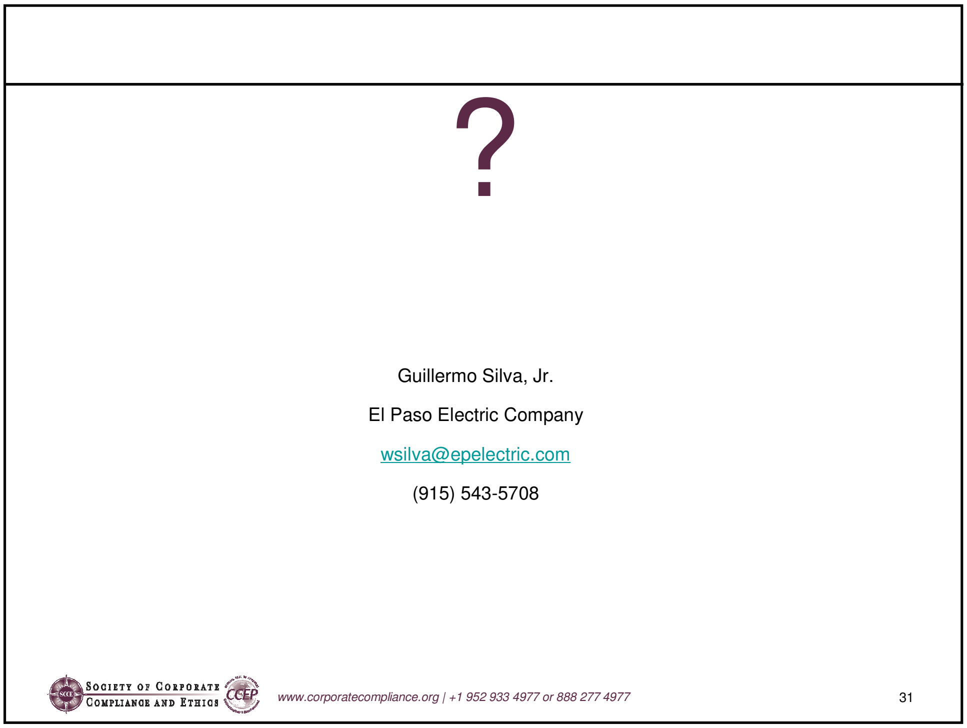
The Hard Part

- What happens when you execute all the steps and you have driven the awareness level for the program and all you are getting is "**Lip Service**" for the buy-in of the program?
- Possible Cultural Challenges:
  - Silo Mentality
  - Gamesmanships
  - Private Agendas
  - Fiefdom Building & Protection



Teamwork

- Remind everyone you all are riding the same horse regardless of what their individual responsibilities are – so let's take care of the horse. Without a good horse, there are no winners.
- Teamwork drives efficiency and expedience.
- Give everyone the benefit of understanding the concept of teamwork, and let everyone know that they are either a team player or not.



?

Guillermo Silva, Jr.

El Paso Electric Company

wsilva@epelectric.com

(915) 543-5708