

CTA INFORMATION SECURITY CASE STUDY:

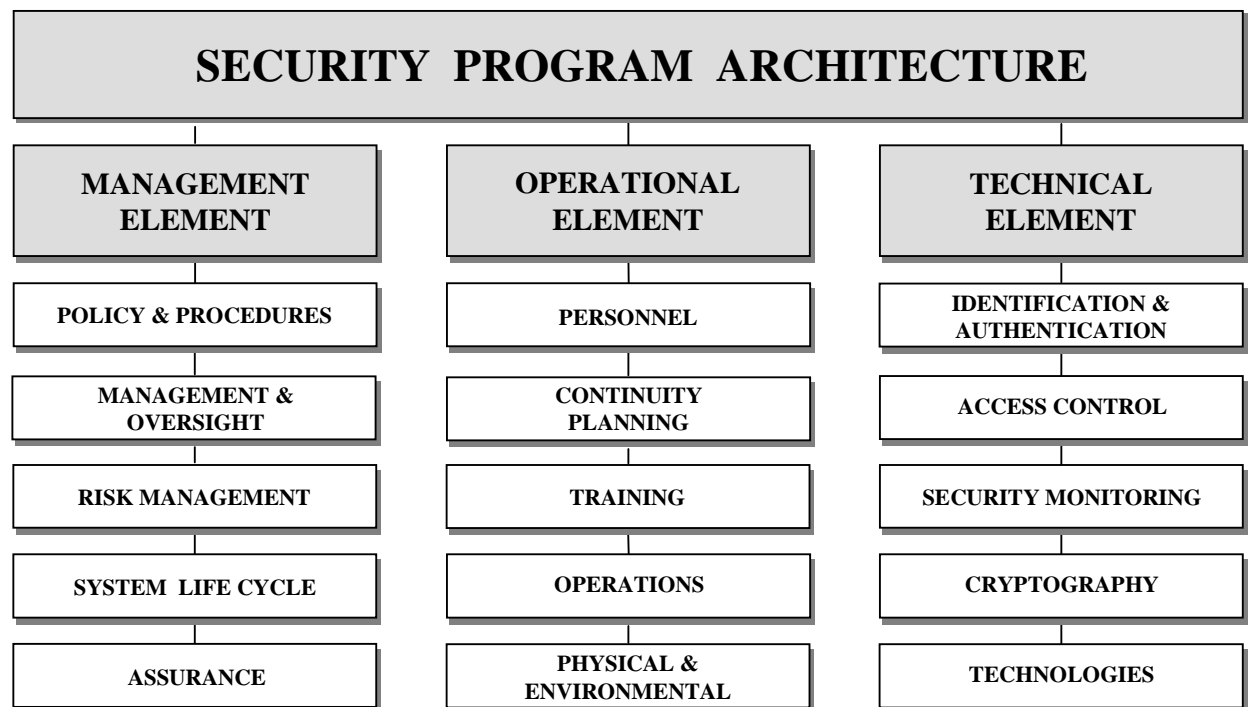
SECURING STATE GOVERNMENT INFORMATION NETWORKS

CLIENT DESCRIPTION:

The State's Information Technology Services (ITS) organization, which along with the State's Communications Network, provides connectivity and IT Services to all State organizations, departments, and regions.

PROJECT DESCRIPTION:.

Develop an Enterprise-level information protection program. It first developed an overall security program architecture, followed by a general design (Phase II), and a finally a detailed design. The project identified three areas of focus, management, operational, and technical.



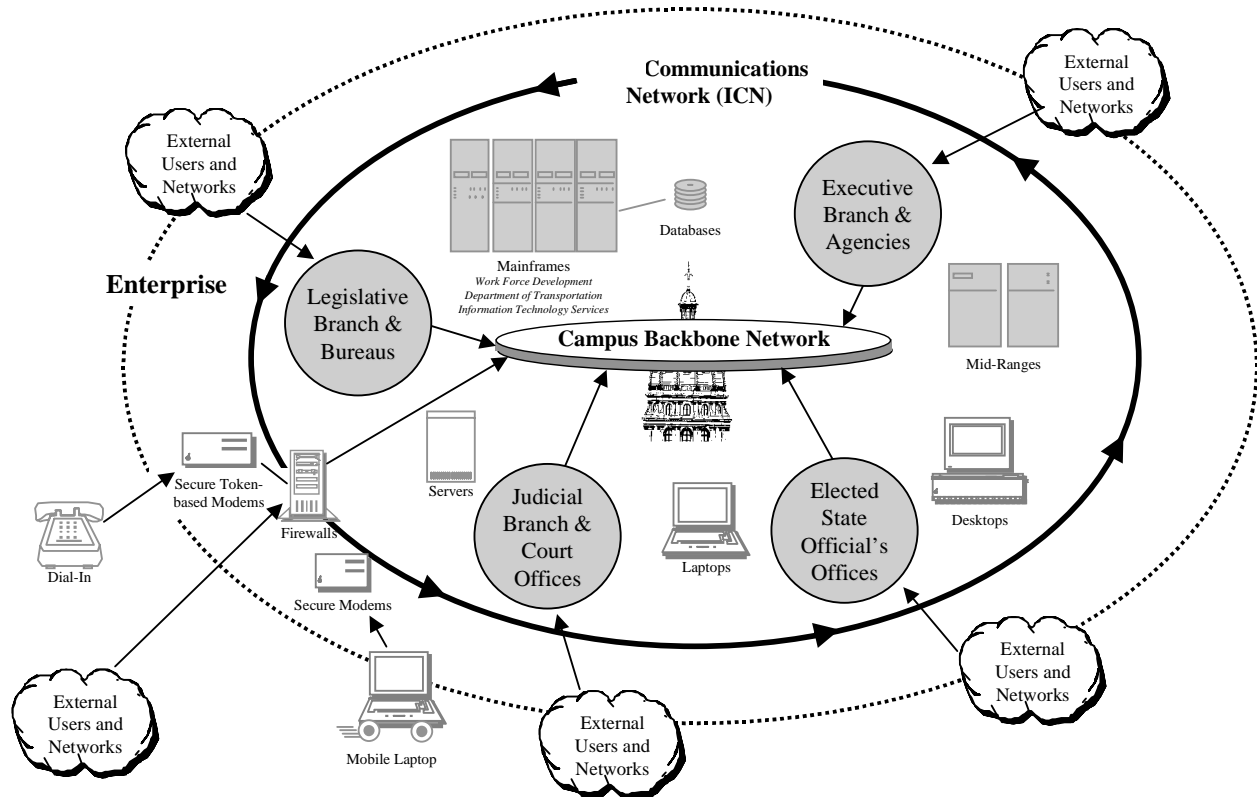
Management controls dealt with policies regulating the information infrastructure, inter-agency communication, identification of security needs, and providing connectivity for the Enterprise. Operational controls dealt with issues such as a citizen's right of public access, continuity planning, training, backup tapes, off-site storage, environmental issues such as climatic, structural, and configuration of different information assets. Technical controls addressed issues such as standard hardware configurations, testing, verification, single-sign on, vulnerability identification, reporting, isolation, and removal.

CTA PROJECT REQUIREMENTS:

Develop an overall information system security architecture and implementation approach for the State's information processing system and organizations that are responsible for them.

SYSTEM ARCHITECTURE:

The system architecture consists of the following platforms; Unix, NOVELL, Windows NT, and IBM mainframes.



The architecture is divided into the Communications Network (ICN) and Campus Backbone Network (BCN). The ICN is a statewide, state-administered fiber optics network responsible for the transmission of high quality full-motion, two-way, interactive video; data transport; and long distance voice communications. Authorized users include:

- a. All accredited K-12 school districts and private schools.
- b. All accredited public and private colleges and technical educational institutions.
- c. State agencies.
- d. Federal agencies.
- e. United States Post Office.
- f. Hospitals and physician clinics (video and data services only).

g. Public libraries.

The ICN was constructed as a tool to provide authorized users throughout the state, telecommunications capability for voice, data, and two-way, interactive, full motion video. The ICN has accomplished this by equitable pricing for sites throughout the state. Sites are not punished financially by their geographical location. Currently the ICN serves all 99 counties in the State and has a node within 15 miles of every citizen.

The Campus Backbone Network (CBN) provides connectivity to various organizational entities, to the ICN, and to the Internet. It is implemented as a token ring network at 16 Mbs. State Governmental organizations use the CBN to obtain connectivity to the mainframe systems, mail hub, and access to another organization's LAN. External users on field assignments are supposed to connect to the organization's LAN through the ICN via the CBN to that organization's LAN. However, several organizations provide direct dial-in capability to their LANs.

WORK ACCOMPLISHED:

Developed an overall information security program and architecture that identifies tasks, responsibilities, milestones, and required resources.

BENEFITS TO CLIENT:

Completion of the first phase of this program has provided the customer with a strategic roadmap and plan for the identification and implementation of an information protection program to greatly reduce the current information security threats and risks.