City of Austin

Information Security Office

Program Plan and Posture

Table of Contents

1.0 Purpose

The Information Security Office - Program Plan and Posture is a living document that is used throughout the life of the program as a guide and reporting tool, guiding progress toward successfully fulfilling the strategy, identified goals, and objectives while reporting on the associated activities and resulting posture.

The plan is a high-level plan for achieving information security goals and objectives, including short- and mid-term objectives. as well as performance targets specific for each goal and objective. This plan is reviewed at least annually, during all major milestones, and when there is any major change in environment or business drivers.

The posture is a 'current state' report on milestone completion and includes details on how this changes the maturity of the program.

During program build-out, the plan and posture are used as the deployment roadmap and milestone reporting tool, guiding the development and implementation of the City's Information Security Program.

2.0 Scope

This plan and posture apply to the City's Information Security program, including the framework, programs, projects, technology, and the general plan of action.

3.0 Assessment

In determining program development and implementation priority, a general assessment is necessary to determine where the City is, where it needs to be, and the gap between the two. This assessment provides the necessary context and guidelines for the overall roadmap. Current state is based on internal self-assessment activities conducted by the Information Security Office (ISO), the 2019 Nationwide Cybersecurity Review (NCSR), the 2019 Information Security Management Audit conducted by the City Auditor, and post-assessment observations provided by the Department of Homeland Security (DHS) based on an assessment conducted in late 2018.

3.1 Current State

The City is currently focused on IT security within IT operations. Success is due to pockets of excellence within specific City Departments, heroics, and ad hoc processes that are held by a few individuals at the City. Overall, the current approach does not directly address enterprise or business process risk, and only focuses on the technology solutions space.

3.2 Gap Analysis

There is a lack of standardized governance, process, and technology at an enterprise level, creating gaps in organization, business processes, and systems implementation for secure solutions and operations.

3.3 Target State

The City of Austin maintains a documented, standardized, repeatable, and ongoing process of information security- and privacy-related risk management, with established frameworks, programs, and technology to support the City's information security requirements and a risk-based approach for the protection of information and technology. Information security and privacy protection requirements are included by design in all business processes and through the system development life cycle at the organization, business process, and systems implementation levels.

4.0 Roadmap

4.1 Overview

The plan is to establish the Information Security Portfolio in a phased approach. The governance framework is developed, released, implemented, and assessed during each phase until all framework, programs, services, and solutions are in place.

The Center for Internet Security (CIS) Critical Security Controls (CSC), along with consideration of risk and efficiency of risk reduction, are used for sequencing, as well as determining prioritization and scheduling for development, release, implementation, and assessment.

4.2 Critical Success Factors

Success of the deployment strategy relies on the dependencies listed within the phases, as well as the following key factors:

- Executive management sponsorship of policy, program, strategy, and control requirements
- Citywide approval and adoption of framework, programs, and control requirements
- Citywide approval and adoption of assignment of responsibilities as outlined in the framework, programs, and control requirements
- Resources are allotted for process (develop, release, implement, and assess)
- Trained security control assessors develop and adhere to approved security and privacy control assessment plans
- Inventory, configuration, and security categorization for information and systems are identified, documented, and maintained
- System Security and Privacy Officers, Information Owners (IO), System Owners (SO), and Authorizing Officials (AO) are identified and accept responsibilities of the roles

5.0 Measurement

The program is measured by progress toward the Nationwide Cybersecurity Review (NCSR) recommended maturity level. The NCSR is a free, confidential, annual self-assessment survey that is based on the NIST

Cybersecurity Framework (CSF). The NCSR is used to track metrics specific to the City, develop a benchmark to gauge the City's year-to-year progress, and anonymously measure the results against peers.

Measurement of percent increase year-to-year for each CSF Function (program goals) is used as measurement and verification that the program is functioning as expected. As the program matures, more granular measurement would be developed.

6.0 Alignment to City Council Outcomes

6.1 Safety

Being safe in our home, at work, and in our community.

6.1.1 Quality & Reliability of Critical Infrastructure

Strategies:

- Establish information security and risk management programs to provide business impact analysis, business continuity, and disaster recovery information security policy, guidelines, and procedures to effectively manage risk to information and technology that directly and indirectly support critical infrastructure and City operations.
- Establish information security operations and incident management programs to provide computer security incident response to effectively manage information and technology security incidents that directly and indirectly impact critical infrastructure and City operations.

Examples:

- Business Impact Analysis
- Information System Contingency Planning

Relevant Metrics:

- #1, Percentage of departments that have documented critical infrastructure following sector-specific guidance.
- #2, Percentage of departments that have completed performance and vulnerability audits of documented critical infrastructure following sector-specific guidance.
- #3, Percentage of our critical infrastructure for which vulnerabilities have been assessed and addressed via protective and/or mitigation strategies.
- #4, Number and percentage of our critical infrastructure assets with current, accredited, or non-accredited disaster recovery and Continuity of Operations Plans (COOP). Indicate accreditation details where applicable.

Relevant Challenge Statements:

- #3, How might we strengthen local and regional partnerships to prevent, prepare for, and respond to natural and human-caused hazards, including digital security breaches?
- #5, How might we proactively identify, assess, and manage risks related to the quality, reliability, and access to critical infrastructure, given the challenges of an aging infrastructure, greater climate impacts, and population growth?

Supporting Technologies:

- Awareness and Training Course Development Solution
- Consolidated Log Management Solution
- Governance, Risk, and Compliance (GRC) Solution
- Identity and Access Management (IAM) Solution
- Malware Protection Solution
- Network Segmentation and Security Zoning
- Patch Management Solution
- Vulnerability Management Solution

6.2 Government That Works for All

Believing that city government works effectively and collaboratively for all of us, and is equitable, ethical, and innovative.

6.2.1 Condition/Quality of City Facilities and Infrastructure and Effective Adoption of Technology

Strategies:

- Establish information security, risk management, and assessment and authorization programs to provide oversight and guidance, ensuring protection and sustainment of City information, technology infrastructure, and operations when adopting new technology.
- Establish standards for secure data collection and sharing while leveraging open source technologies, mobile-ready web applications, and proven, agile project methodologies to improve how we manage projects and information. (Established as the proposed strategy in current Council Strategy from outcomes workshops.)

Examples:

- Business Impact Analysis
- Information and Operational Risk Assessment
- Assessment and Authorization of Systems

Relevant Metrics:

- #1, Percentage of time that City-owned infrastructure is operational.
- #3, Total time critical city services were unavailable due to information security risk.

Relevant Challenge Statements:

- #1, How might we build a more trusting, collaborative decision-making process amongst Council, City Management, and our Community to increase productivity and transparency?
- #5, How might we mature the City's data and technology capabilities to provide secure and scalable solutions that enable staff to deliver accessible, modern, and impactful services to all residents?

Supporting Technologies:

- Asset Management Solution
- Consolidated Log Management Solution
- Governance, Risk, and Compliance (GRC) Solution
- Identity and Access Management (IAM) Solution
- Malware Protection Solution
- Network Segmentation and Security Zoning
- Patch Management Solution
- Vulnerability Management Solution

6.2.2 Transparency and Ethical Practices

Strategy:

- Establish information security and privacy programs to ensure proper data collection and monitoring is in place to provide evidence of ethics violations and transparency of process while balancing the protection of employee and resident privacy.

Example:

- Protection of resident information that is given for fulfilment of City services.

Relevant Metrics:

- #1, Percentage of residents who report employees of the City of Austin are ethical in the way they conduct City business.
- #2, Number of findings of fraud, waste, and abuse by employees, officials, and contractors.
- #3, Percentage of employees who report that those in their work group generally behave ethically in the workplace.

- #5, Number of findings of unethical behavior as determined by the Ethics Review Commission.
- #6, Percentage of residents who report that they are satisfied with their ability to engage the City in a fair and transparent manner.

Relevant Challenge Statements:

- #1, How might we build a more trusting, collaborative decision-making process amongst Council, City Management, and our Community to increase productivity and transparency?
- #5, How might we mature the City's data and technology capabilities to provide secure and scalable solutions that enable staff to deliver accessible, modern, and impactful services to all residents?
- #7, How might we improve engagement to include voices of our most vulnerable communities, demonstrate the impact of public input, and generate meaningful outcomes for the community?

Supporting Technologies:

- Asset Management Solution
- Consolidated Log Management Solution
- Governance, Risk, and Compliance (GRC) Solution
- Identity and Access Management (IAM) Solution
- Malware Protection Solution
- Network Segmentation and Security Zoning
- Patch Management Solution
- Vulnerability Management Solution

7.0 Alignment to the City's IT Strategic Plan

7.1 Modernize the Core (a Smart Cities Foundation)

Update and improve foundational systems.

Strategies:

- Establish the Information Security and Risk Management Programs to provide business impact analysis, business continuity, and disaster recovery information security policy, guidelines, and procedures to effectively manage risk to information and technology that directly and indirectly support critical infrastructure and critical City operations.
- Establish information security operations and incident management programs to provide computer security incident response to effectively manage information and technology security incidents that directly and indirectly impact critical infrastructure and critical City operations.

- Establish information security, risk management, and assessment and authorization programs to provide oversight and guidance, ensuring protection and sustainment of City information, technology infrastructure, and operations when adopting new technology.
- Establish standards for secure data collection and sharing while leveraging open source technologies, mobile-ready web applications, and proven, agile project methodologies to improve how we manage projects and information. (Established as the proposed strategy in current Council Strategy from outcomes workshops.)

Examples:

- Business Impact Analysis
- Information and Operational Risk Assessment
- Information System Contingency Planning
- Assessment and Authorization of Systems

Relevant Implications:

- Establish funding models for core citywide, multi-department, and department-specific systems (e.g., Finance, Human Capital Management, Asset, Computer-Aided Dispatching)
- Establish asset lifecycle management for IT assets
- Establish system governance to support entire city rather than one department
- Leverage governing boards for roadmaps for key systems
- Create a single source of information on citywide solutions

Supporting Technologies:

- Asset Management Solution
- Consolidated Log Management Solution
- Identity and Access Management (IAM) Solution
- Network Segmentation and Security Zoning

7.2 Make Data Accessible, Safe, & Useful to City Staff

Provide robust City technology infrastructure.

Strategies:

- Establish standards for secure data collection and sharing while leveraging open source technologies, mobile-ready web applications, and proven, agile project methodologies to improve how we manage projects and information. (Established as the proposed strategy in current Council Strategy from outcomes workshops.)

Examples:

- Business Impact Analysis
- Information and Operational Risk Assessment
- Assessment and Authorization of Systems

Relevant Implications:

- Insist on common security and business policies, practices, and processes.
- Build infrastructure to support analytics and access safely, anywhere, and anytime.
- Establish Master Data Management to identify data sources, ownership, and classification.

Supporting Technologies:

- Asset Management Solution
- Awareness and Training Course Development Solution
- Consolidated Log Management Solution
- Governance, Risk, and Compliance (GRC) Solution
- Identity and Access Management (IAM) Solution
- Malware Protection Solution
- Network Segmentation and Security Zoning
- Patch Management Solution
- Vulnerability Management Solution

7.3 Make Doing Business Easy

Provide residents with seamless access to City services.

Strategies:

- Establish information security and risk management programs to provide business impact analysis, business continuity, and disaster recovery information security policy, guidelines, and procedures to effectively manage risk to information and technology that directly and indirectly support critical infrastructure and critical City operations.
- Establish information security operations and incident management programs to provide computer security incident response to effectively manage information and technology security incidents that directly and indirectly impact critical infrastructure and critical City operations.

Examples:

- Business Impact Analysis
- Information and Operational Risk Assessment

- Information System Contingency Planning
- Assessment and Authorization of Systems

Relevant Implications:

- Insist on common business policies, practices, and processes.
- Integrate civic/democratic participation and support equity to ensure all users can access City services.
- Offer paperless options for current paper-based transactions for external and internal customers.
- Define "Civic Moments", and ensure all residents have access to technology and the adequate technology literacy skills to participate in a digital society. Cross the digital divide so all parts of the community can participate.

Supporting Technologies:

- Consolidated Log Management Solution
- Governance, Risk, and Compliance (GRC) Solution
- Identity and Access Management (IAM) Solution
- Malware Protection Solution
- Network Segmentation and Security Zoning
- Patch Management Solution
- Vulnerability Management Solution