

# ITS Strategic Roadmap – FY20 Planning

## Information Security Management

Author: *John Griffey*

Date last updated: *December 27, 2018*

### Background

The Information Security Management program, established by Mayor Barry's Executive Order 34 and reconfirmed under Mayor Briley, strives to provide the policy and guidance to safeguard the confidentiality, availability and integrity of the Metropolitan Government's information assets and infrastructure.

Program activities include policy creation, distribution, review and assistance with compliance; guidance on compliance with targeted Federal and State regulations, including HIPAA; information security awareness and training; and identification and remediation of information security risks.


The Information Security Management program exists to serve to all Metropolitan Government employees and third party users except those agencies specifically outlined in Executive Order 34. Those agencies, however, are requested to consider adopting policies and practices put forth through this program.

Stakeholders are all Departments and Agencies of the Metropolitan Government; government vendors and partners; the members of the Mayoral Information Security Advisory Board; and the citizens of Nashville and Davidson County.

### Current Strategic Drivers

1. **Customer Demand: Secure Government Systems** (High) – Proliferation of mobile devices, rise of hacktivism, reliance on any time connectivity to Metro network, etc. has increased the need to ensure the security of the Metro network. The complexities of digital business combined with an emerging "hacker industry," significantly increase the threat surface for Metro. Relying on perimeter defense and rule-based security is inadequate, especially as organizations exploit more cloud based services.
2. **Customer Demand: Efficient, Timely Solutions** (High) – Customer departments and agencies want to implement technology that efficiently meets their business needs. IT Security can be seen as an impediment to timely or efficient solutions. Additionally, departments are embracing "mobility" (access to everything, all the time, from any device, from anywhere) as a way to meet their business goals. These solutions require a more robust approach to enterprise security.
3. **Industry Trend: Increasing Security Threats** (High) – Social Engineering (Phishing, Spear Phishing), Advanced Persistent Threats (APTs), Hacktivist Groups (Anonymous, LulzSec), threats against elections and the rise of ransomware and cryptomining will continue to require attention with proper controls through well-constructed and implemented policies, procedures, and standards.



4. **Regulation: Regulatory Compliance Obligations** (High) – Regulations and standards such as HIPAA/HITECH, PCI-DSS, TCA 47-18-2107, and FERPA have specific information security control needs that must be addressed to realize appropriate levels of compliance with applicable laws, standards, and regulations.
5. **Regulation: Mayoral Executive Orders** (High) – Executive order 34 addresses specific information security areas to include governance, training, acceptable use, and policy development and implementation.
6. **Customer Need: Metro Employee Awareness** (High) – People will continue to be the weak link in the information chain without a constant and evolving information security awareness program. This awareness includes the roles and responsibilities each position has in Metro’s information security management program.
7. **Customer Desire: Cloud Computing** (High) – The widespread public acceptance of cloud for services that employees and citizens use every day, along with the potential for positive financial impact and increasingly effective cloud vendor security stance make a hybrid model a potential direction. Due to these economies of scale and potential cost savings, a growing number of Metro agencies have investigated and/or migrated certain to cloud-based systems.
8. **Industry Trend: Privacy** (High) – Over the past years, the need to protect privacy in the private sector has become more important, with the expansion of new technology based solutions (behavior analysis, big data analytics, location based analytics, etc.). New services and solutions in the public sector will involve collection of citizen data that will make privacy an important consideration moving forward.
9. **Industry Trend: Continued Integration of Cyber and Physical Systems**  (High) – “Smart Cities” solutions, such as the ones in Metro’s Connected Nashville initiatives, promise to deliver many valuable time- and resource-saving conveniences, these services require sophisticated cybersecurity. Every device or sensor that connects to the network broadens the attack surface, creating a potential entry point for cybercriminals to hack to or hack through.
10. **Industry Trend: Data Access** (Medium) – Increasing desire for access to more data, such as with open government data portals, require effective information governance, privacy, confidentiality and security protocols, as well as intuitive analytics and visualization tools to build public trust and confidence in the quality and value of open data.



## On the Horizon Strategic Drivers

1. **Administration Change** (High) – An election for Metro Government in the fall of 2019 has the potential to replace our current mayor, vice mayor and members of the Metro Council. With this election comes the potential to disrupt the planned direction of systems, funding and personnel related to prior administrations.
2. **New Legislation** (Medium) – Increasing legislation at the state level, specifically around privacy, and the international level (EU GDPR) might push the creation of additional Tennessee state legislation or even Federal legislation. If passed and enacted, these and other laws may have information security implications for Metro Government.
3. **New Controls and Standards** (Low) – Standards that Metro information security policies and procedures are based on, such as NIST and ISO, are constantly being updated.

## Short Term Goals (0-6 months) 7/1/19 – 12/31/19

#	Goal/Objective	Est. Start	Est. Duration
1	Continue to evaluate Information Security Management program and address any findings.	11/19	Ongoing
2	Continue to plan and coordinate activities of the outsourced HIPAA Privacy and Security offices for Metro’s identified Covered Entities.	7/19	Ongoing
3	Plan and coordinate activities for October 2019 Cyber Security Awareness month.	7/19	3 months
4	Develop processes for conducting “privacy impact assessments” as part of project implementations.	7/19	6 months
5	Evaluate the use of Cloud Access Security Broker (CASB) to further interject enterprise security controls as cloud based resources are accessed. Provide report of findings to CIO.	7/19	3 months
6	Continue to track risk using previously developed risk management tools (risk assessment and risk register).	7/19	Ongoing

## Medium Term Goals (6-18 months) 1/1/20– 12/31/20

#	Goal/Objective	Est. Start	Est. Duration
1	Develop business case for policy/risk management automation. Research industry reports. Provide report on findings to CIO.	1/20	2 months
2	Research and provide report to CIO on possibility of implementing GRC (governance, risk management and compliance) solution. (Capital Funding Required)	3/20	6 months

## Long Term Goals (18-36 months) 1/1/21 – 6/30/22

#	Goal/Objective	Est. Start	Est. Duration
1	Implementation of GRC (governance, risk management and compliance) solution. (Capital Funding Required)	6/21	12 months



## Related Roadmaps

- Information Security Program
- Identity and Access Management
- System Lifecycle Management
- Open Data

## Related Resources

- Mayoral Executive Orders 34 at <http://www.nashville.gov/Metro-Clerk/Legal-Resources/Executive-Orders.aspx>
- Metro Government Information Security Policy at <http://www.nashville.gov/Information-Technology-Services/Information-Security/Information-Security-Policies.aspx>
- [Connected Nashville](#)
- [PCI Security Standards](#)
- [Gartner Top 6 Security and Risk Management Trends For 2018](#)
- [The top cyber security trends of 2018 so far](#)
- [Microsoft's Identity Life Cycle Management Strategy And Roadmap](#)
- [Privacy Tracker - iapp](#)
- [Top 10 Digital Transformation Trends For 2019](#)

