GLOBAL CITY
TEAMS CHALLENGE

SMART AND SECURE CITIES AND COMMUNITIES CHALLENGE (SC3)

A Risk Management Approach to Smart City Cybersecurity and Privacy

A Guidebook from the
Cybersecurity and Privacy Advisory Committee
(CPAC) Public Working Group

July 2019

Acknowledgements

This publication was developed by the Cybersecurity and Privacy Advisory Committee (CPAC) public working group. The CPAC is a public-private partnership dedicated to promoting built-in cybersecurity and privacy best practices and identifying key considerations for Smart Cities and Communities. This public working group consists of cybersecurity and privacy professionals and practitioners from governments, non-profit organizations, academia, and the private sector. The CPAC acts as a resource to the Global City Teams Challenge (GCTC) and Smart and Secure Cities and Communities Challenge (SC3) effort and the GCTC SuperClusters (e.g., Data, Public Safety, Transportation).

We would like to acknowledge and thank the organizers and hosts of the GCTC-SC3 program for their ongoing support of the CPAC.

In addition, we would like to recognize the following CPAC participants for their contributions to this Guidebook:

- *David Balenson, SRI International*
- *Adnan Baykal, Global Cyber Alliance*
- *Gary Dennis, Booz Allen Hamilton*
- *Wayne Dennis, Accenture*
- *Alex Huppenthal, Aspenworks*
- *Lan Jenson, Adaptable Security*
- *Damon Kachur, Sectigo*
- *Benny Lee, County of San Mateo*
- *Carmen Marsh, Inteligenca*
- *Aleta Nye, J.D., Certified Information Privacy Professional*
- *Carmen Parada, 1CSR, Inc*
- *Renil Paramel, Strategy of Things*
- *Bill Pugh, Smart Connections Consulting LLC*
- *Maryam Rahmani, Maryam Rahmani LLC*
- *Carter Schoenberg, HEMISPHERE Cyber Risk Management LLC*
- *Sushmita Senmajumdar, Adaptable Security*
- *Deborah Shands, SRI International*
- *Dean Skidmore, IoT+LTE Consulting Group*
- *Scott Tousley, Splunk*
- *Ed Walker, City of San Jose*
- *Ruwan Welaratna, Evo, Inc.*
- *Paul Wertz, AT&T*
- *Peter Wong, The Soter Group*

We would especially like to thank those who have read and reviewed this Guidebook throughout its development and provided comments and feedback to help make the Guidebook a better resource for the Smart City community.

We would also like to express our gratitude to all the cities, municipalities, and jurisdictions who have participated in and supported the activities of the CPAC, including San Mateo County, California; San Leandro, California; and San Jose, California.

Finally, we would like to acknowledge the GCTC-SC3 SuperClusters and their leadership for their ongoing support and parallel efforts to elevate cybersecurity and

privacy as priorities in Smart City initiatives.

- *Agriculture and Rural SuperCluster*
- *Data SuperCluster*
- *Education SuperCluster*
- *Public Safety SuperCluster*
- *Smart Building SuperCluster*
- *Transportation SuperCluster*
- *Utility SuperCluster*
- *Wireless SuperCluster*

Intent and Relationship to Existing Risk Management Approaches

The intent of this Guidebook is to promote a risk-managed approach to developing and implementing Smart Cities and Smart City solutions and capabilities, particularly as it pertains to cybersecurity and privacy. While this Guidebook is largely based on the National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF), the Guidebook is not intended to obviate any existing cybersecurity and privacy risk management practices, policies, or processes. Rather, it is intended to supplement existing practices, policies, and processes and provide some Smart City-specific cybersecurity and risk management considerations.

If your organization already uses the NIST RMF or another broadly-adopted risk management framework or standard, such as the ISO/IEC 27000 Information Security Management Systems (ISMS) standards, then this Guidebook can provide some additional critical Smart City-specific cybersecurity and privacy considerations to understand and possibly incorporate into your existing approach.

If your organization uses the NIST Cybersecurity Framework (CSF) as a means to describe and guide cybersecurity activities, this Guidebook can provide additional and more robust cybersecurity and privacy management processes to consider (some aspects of which you may already be doing) and potentially implement to supplement existing practices.

Lastly, if your organization does not have a systematic approach to Smart City cybersecurity and privacy, this Guidebook provides a high-level overview of a risk-based approach to managing Smart City cybersecurity and privacy. In addition, Appendix C includes the “CPAC ‘Top X’ Questions for a Trustworthy Smart City” as a tool for organizations to engage stakeholders and start the conversation around cybersecurity and privacy risk management.

The approach presented in this Guidebook is not prescriptive and will necessarily have to be adapted to meet the specific needs of your organization and environment.

Disclaimer

While the intent of this Guidebook is to promote cybersecurity and privacy for Smart Cities, your municipality or organization should identify the risk management processes and the Smart City products, services, and solutions that best fit your environment and requirements.

The CPAC includes cybersecurity and privacy professionals and practitioners from a variety of public and private sector organizations; however, this Guidebook does not endorse any commercial products or services. Similarly, this Guidebook may present specific approaches or solutions used in individual deployments or jurisdictions; these are included for illustrative purposes only and are not intended to be endorsements of specific products or implementations.

Table of Contents

Chapter 1. Executive Summary

Background

The National Institute of Standards and Technology (NIST) launched the Global City Teams Challenge (GCTC) program in 2014 as a means to encourage collaboration across the global Smart Cities community. The goal of GCTC is to "establish and demonstrate replicable, scalable, and sustainable models for incubation and deployment of interoperable, standards-based solutions using advanced technologies such as IoT and CPS, and demonstrate their measurable benefits in communities and cities."[1]

In 2018, NIST and the Department of Homeland Security Science and Technology Directorate (DHS S&T) partnered to initiate the Smart and Secure Cities and Communities Challenge (SC3) as an effort to build on the GCTC program and demonstrate the "value and return on investment for designed-in trustworthiness for smart city deployments."[2]

In support of the SC3 effort, the Cybersecurity and Privacy Advisory Committee (CPAC) was established as a public working group comprised of cybersecurity and privacy professionals and practitioners across the GCTC community. The CPAC has representation from all levels of government, non-profit organizations, academia, and the private sector.

The CPAC public working group is intended to provide a forum for members to share their expertise, leverage industry best practices, and further collaborate with relevant organizations. The CPAC also serves as a cybersecurity and privacy resource for the GCTC-SC3 SuperClusters and Action Clusters.

This Guidebook has been developed by the CPAC with the primary goal of providing a source document for all entities interested in learning how to manage upcoming Smart City cybersecurity and privacy challenges and risks.

Purpose

Advances in information and communication technologies (ICT) and the advent of Internet of Things (IoT) devices are enabling municipalities' development and deployment of Smart City capabilities and solutions. Municipalities are leveraging these smart solutions to provide enhanced services to their citizens; improve the livability of their communities; and promote economic opportunity.

[1] "About GCTC," *NIST*. https://pages.nist.gov/GCTC/about/the-gctc/
[2] *Smart and Secure Cities and Communities Challenge* presentation by Dr. Douglas Maughan at the 2017 GCTC Expo in Washington, DC.

Ubiquitous connectivity, the proliferation of computing power, and the emerging linkages between cyber and physical infrastructure introduce new and potentially greater cybersecurity and privacy risks than those found in the traditional IT enterprise. Effectively and proactively managing these emerging risks is critical to successfully developing and implementing solutions and to fully realize promised Smart City benefits.

This Guidebook seeks to present an approach to Smart City cybersecurity and privacy risk management that can be adapted to meet the needs of individual municipalities and communities. This Guidebook also provides some key considerations that decision-makers will need to recognize and account for in their risk management approach.

In addition, the appendices of this Guidebook provide additional resources, including a set of use cases to help demonstrate the application of risk management concepts in real-world situations (see Appendix A) and the "CPAC 'Top X' Questions for a Trustworthy Smart City," a discussion tool for initiating the conversation around cybersecurity and privacy risk management (see Appendix C).

Intended Audience

The primary audience for this guidebook is municipal policymakers and leaders (e.g., mayors, council members, city managers, department heads, innovation officers, chief information officers, chief information security officers) actively involved in or considering the development of Smart City capabilities. However, it is also important for all other Smart City stakeholders (including technology/solution implementers and providers) to understand cybersecurity and privacy risk management processes and to be able to prepare and plan accordingly.

Key Takeaways

Readers can take away best practices for a trustworthy Smart City from planning to design to implementation. Specifically, best practices include managing cybersecurity and privacy-related risks for smart solutions, IoT systems, as well as the existing information systems:

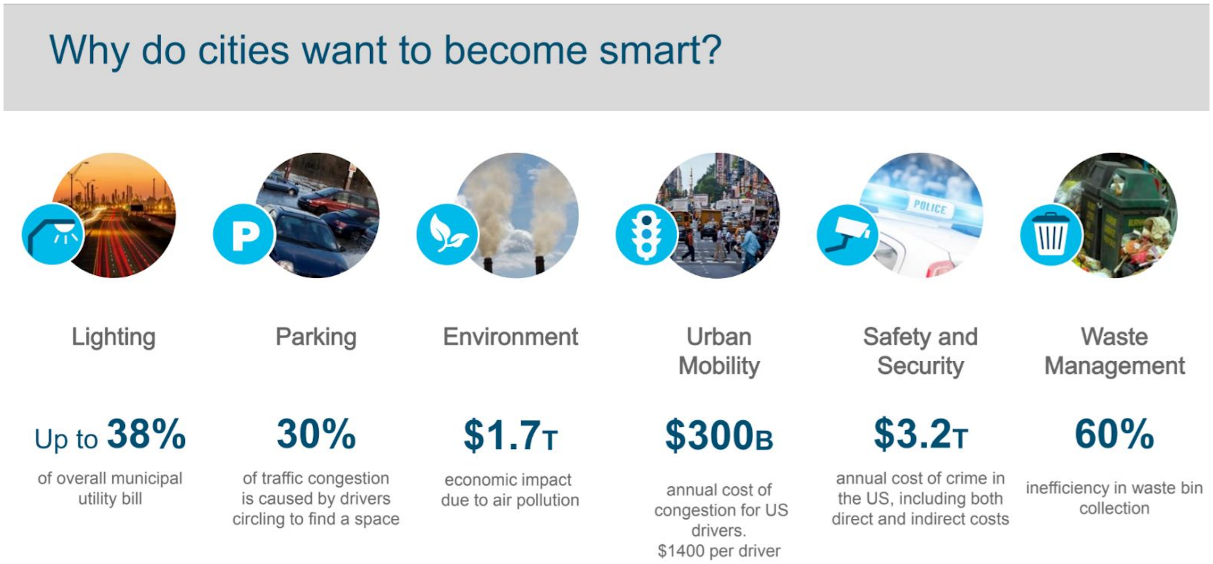
- What is cybersecurity and privacy risk and why is risk management important?
- How might cybersecurity and privacy risk management in a Smart City environment be different from a traditional IT environment?
- How can cybersecurity and privacy risk management practices be operationalized and applied in the Smart City context?

Chapter 2. Smart Cities: Benefits and Cybersecurity and Privacy Risks

Cities and communities stand to harvest unprecedented benefits from advances in information and communications technologies (ICT), in general, and Internet of Things (IoT) and Artificial Intelligence (AI), in particular. Smart cities inevitably introduce new or heighten existing cyber risks, which demand proper consideration in design to ensure the optimal realization of intended Smart City outcomes.

Smart Cities Benefits

Smart cities are associated solutions and capabilities defined by the integration of technology, connectivity, and data to improve the quality of and accessibility to citizen services and to improve the livability of the city and community. Smart cities have the potential to address key challenges, including air and other environmental pollution, traffic congestion, crime, and economic development. Many of these challenges can be directly connected to a direct and/or an indirect fiscal impact (e.g., operational costs, lost economic productivity); conversely, Smart City solutions may have direct benefits in terms of improved services or livability as well as associated benefits of cost savings through enhanced efficiency and a boost in economic productivity, development, and opportunity.



Why do cities want to become smart?

Lighting
Up to 38%
of overall municipal utility bill

Parking
30%
of traffic congestion is caused by drivers circling to find a space

Environment
$1.7T
economic impact due to air pollution

Urban Mobility
$300B
annual cost of congestion for US drivers. $1400 per driver

Safety and Security
$3.2T
annual cost of crime in the US, including both direct and indirect costs

Waste Management
60%
inefficiency in waste bin collection

[3]

While there are many benefits associated with the promise of Smart Cities, there are also many risks and opportunities for unintended consequences. For Smart Cities to truly be successful and reach their full potential, it is important for those designing, developing, and implementing Smart City solutions to properly manage risk. Risk, in the context of Smart Cities, may be found in many common categories such as

[3] National Cybersecurity Center of Excellence research on mitigating IoT-based DDoS as presented by Tim Polk, Russ Gyurek, and Joshua Lawton at CPAC Cybersecurity Symposium for Smart Cities in San Jose, California, on October 3, 2018.

operational, financial, technical, contractual, legal, reputational, and political risk; however, one area of risk that is becoming increasingly important is cybersecurity and privacy risk. Addressing cybersecurity and privacy by design is critical to risk mitigation and enabling the successful development of Smart Cities and its benefits to citizens.

Cybersecurity and Privacy Risk

Risk (R) is commonly considered a function of three factors: vulnerability (V), threat (T), and consequence (C). While there is some contention on what the appropriate formula is, there is a clear, positive relationship between risk and each of its three variables (e.g., as consequence increases, risk increases). A common mathematical expression of risk is that risk is the product of vulnerability, threat, and consequence – or R = V x T x C.

This general notion of risk certainly applies in the cybersecurity and privacy context. With the increasing ubiquity of connectivity, cybersecurity and privacy risk is a concept that must be thoroughly considered in most, if not all, domains, including the Smart City environment. Risk in the Smart City context can be attributed to a wide variety of factors given the nearly infinite permutations of potential Smart City-related vulnerabilities, threats, and consequences.

Example Smart City Cybersecurity and Privacy Vulnerabilities, Threats, and Consequences

Vulnerabilities	Threats	Consequences
● Lack of awareness of all authorized and unauthorized devices/assets ● Poorly-implemented encryption or lack of encryption ● Inability to patch or update software/firmware ● Use of default administrator passwords ● Susceptibility to distributed denial of service (DDoS) attacks ● Lack of security assessment and software code testing ● Inadequate security and privacy awareness and training ● Weak or immature supply chain risk management practices	● National-state and state-sponsored actors ● Organized crime and other criminal groups ● Terrorist groups ● Hacktivists ● Insiders/employees – whether malicious, unintentional, or negligent ● External suppliers, service providers, vendors, and partners (e.g., supply chain risk, interdependence and integration risk) ● Other individual hackers or hacking groups ● Natural and man-made disasters	● Disruption of government services to citizens ● Loss or leakage of citizen personally identifiable information (PII) ● Financial loss or expense (e.g., lawsuits, regulatory penalties, theft of funds, cost of response and remediation) ● Facilitation of terrorist event – whether physical, digital, or combined ● Degradation of trust in government and government services ● Danger to public health or safety

Many of the vulnerabilities and threats that could affect Smart City environments are similar to the cybersecurity vulnerabilities and threats commonly found in the traditional enterprise information technology (IT) environment. Additionally, it is unarguable that the consequences in the Smart City context are potentially more complex and catastrophic given the cyber-physical aspects of Smart Cities as well as the broad reach and expansiveness of Smart City implementations (e.g., citizens, government, the private sector, cross-jurisdictional elements).

Moreover, it is important to recognize that cybersecurity and privacy risks to Smart City environments is not merely hypothetical or notional. Indeed, there have been several high-profile cybersecurity and privacy events (among countless data breaches and attacks around the globe) that have had real, damaging effects on some cities and communities who are leading the Smart City movement.

The following four tangible examples of Smart City cybersecurity and privacy risk are based on publicly-available information.

<table>
<tr><td colspan="2"><em>Atlanta Ransomware (March 2018)</em>[4]</td></tr>
<tr><td colspan="2">In March 2018, the City of Atlanta, Georgia, fell victim to a SamSam ransomware attack. Government agencies were locked out of their systems, and applications and services were forced offline - in some cases for months. The attackers were asking for approximately $51,000 in Bitcoin as a ransom payment. Similar attacks were allegedly conducted in ten U.S. states and Canada - including Newark, New Jersey; the Port of San Diego; and the Colorado Department of Transportation.</td></tr>
<tr><td>Vulnerability</td><td>Likely weak access control measures, which allowed a successful brute force attack (i.e., attackers guessed credentials to access system). In addition, a January 2018 audit of Atlanta’s IT systems identified 1,500-2,000 vulnerabilities in the city’s IT systems, which may have facilitated initial access to or the eventual lateral movement with the city’s infrastructure.</td></tr>
<tr><td>Threat</td><td>In November 2018, two Iranian nationals were charged with executing the SamSam ransomware attack; they are not considered to be associated with a nation-state actor.</td></tr>
</table>

[4] “Georgia Charges Iranians in Ransomware Attack on Atlanta, *NPR*. https://www.npr.org/2018/12/05/673958138/georgia-charges-iranians-in-ransomware-attack-on-atlanta; https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWlMcXS0K/; “Atlanta Officials Reveal Worsening Effects of Cyber Attack,” *Reuters*. https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M?feedType=RSS&feedName=technologyNews; https://www.wired.com/story/doj-indicts-hackers-samsam-ransomware/

Consequence	Hundreds of municipal online applications and services (e.g., court systems, bill payment, law enforcement ticketing) were disabled, and many data records were lost, including police dash camera recordings and legal records. Many of these functions were considered "mission critical." Nearly 4,000 computers were locked by the ransomware. The financial cost of response, remediation, and recovery has increased from early estimates of $2.7 million to $17 million (including $6 million in contracts for security services and software updates and $1.1 million in new IT equipment).

SingHealth (Singapore) Breach (June-July 2018)[5]	
For about a week during the summer of 2018, hackers actively targeted a SingHealth database and were successful in exfiltrating health-related data on 1.5 million patients.	
Vulnerability	A vulnerable workstation/endpoint provided the hackers with initial access. They were able to exploit privileged account credentials to access the database.
Threat	Singapore's government has attributed the breach to an advanced persistent threat (APT) group from a nation-state actor. After the SingHealth breach, they determined that the hackers had been in their systems for at least 10 months.
Consequence	Personally-identifiable information, including demographic data, identification numbers, and some prescription medication history, was stolen. This data could be leveraged for further nefarious purposes, such as identity theft, fraud, or black market pharmaceuticals. Singapore paused all Smart Nation efforts in order to review cybersecurity and privacy practices. In January 2019, Singapore's Personal Data Protection Commission announced fines totaling S$1M (approximately US$740,000) against SingHealth and its IT vendor.

---

[5] Choudhury, Amit Roy. "SingHealth Breach a Wake-Up Call for Smart Nation Singapore," *GovInsider*. https://govinsider.asia/innovation/singhealth-breach-wake-call-smart-nation-singapore/

<table>
<tr><td colspan="2"><em>District of Columbia Surveillance Camera Ransomware (January 2017)</em>[6]</td></tr>
<tr><td colspan="2">Shortly prior to the 2017 Presidential Inauguration, Washington, DC's Metropolitan Police Department (MPD) discovered that nearly 70% of their surveillance cameras were malfunctioning or not operational.</td></tr>
<tr><td>Vulnerability</td><td>Most likely, poor access control measures managing access to internet-connected computers/devices across the District of Columbia, each of which controlled an MPD surveillance camera, were exploited. It appears that the perpetrators had valid credentials for the compromised machines.</td></tr>
<tr><td>Threat</td><td>Two Romanian hackers used Cerber and Dharma ransomware to shutdown the police camera systems for four days and demanded $60,000 in Bitcoin ransom. However, it appears that they were unaware they were targeting an MPD system.</td></tr>
<tr><td>Consequence</td><td>123 of 187 MPD surveillance cameras went offline just prior to the Presidential Inauguration. These hijacked government computers were used to launch and hide the source of a subsequent ransomware attack against a list of approximately 180,000 email addresses. While the actual consequence of this attack was relatively limited, this brought up concerns of potential national security concerns.</td></tr>
</table>

<table>
<tr><td colspan="2"><em>ForeScout Building Automation Systems (January 2019)</em>[7]</td></tr>
<tr><td colspan="2">In January 2019, ForeScout released research on the vulnerability of building automation systems. While these may not all necessarily be "smart" buildings, it is easy to imagine how similar risks exist across all types of buildings with building automation systems and related technologies</td></tr>
<tr><td>Vulnerability</td><td>Poorly implemented (digital) access control measures and software code weaknesses (e.g., cross-site scripting bugs, buffer overflow) are the primary vulnerabilities that could be exploited. Despite notifying the relevant vendors, more than 11,000 devices</td></tr>
</table>

[6] Thomson, Iain. "Guilty: The Romanian Ransomware Mastermind Who Infected Trump Inauguration CCTV Cams," *The Register*. https://www.theregister.co.uk/2018/09/21/cctv_ransomware_trump_washington_dc/

[7] Higgins, Kelly Jackson. "Malware Built to Hack Building Automation Systems," *DarkReading*. https://www.darkreading.com/vulnerabilities---threats/malware-built-to-hack-building-automation-systems/d/d-id/1333671?

	remain exposed and vulnerable. Many of these vulnerable devices are reported to be in schools and medical facilities.
Threat	The ForeScout researchers were able to develop proof-of-concept malware capable of exploiting these building automation systems for about $12,000 - showing that it does not require a well-resourced adversary to pose a credible threat.
Consequence	Potential consequences could include overheating and causing damage to data centers or providing/denying physical access to restricted/secure areas. Building automation systems have been successfully exploited in other non-experimental scenarios.

Enabling Trustworthy Smart Cities through Risk Management

Municipal governments have a responsibility to administer their respective municipalities and to provide services to their constituents. The key value propositions of “Smart Cities” emphasize the primary municipal missions and demonstrate how they can be improved through the use of data, digital technology, and connectivity:

- Improve quality of life and livability of the community
- Foster economic opportunity, growth, and development
- Ensure public safety, security, and resilience
- Bolster community health and wellness
- Promote equitable access and opportunity

In other words, Smart Cities are intended to conduct the mission of “traditional” cities, but in an enhanced manner through the implementation of “smart” capabilities.

In leveraging data and technology to enhance government services and to ultimately mature as a Smart City, municipalities also have a responsibility to address - and build in, where appropriate - cybersecurity and privacy risk management measures. Cybersecurity and privacy risk management should be viewed not only as a requirement but also as a key enabler of Smart Cities and the municipal mission.

Addressing and implementing cybersecurity and privacy risk management in a proactive manner - and communicating those risk management practices, processes, and measures - can help demonstrate municipal responsibility and build public trust. Building trust can help increase public support for Smart City programs and projects and can promote citizen participation - a requisite for the viability of many Smart City solutions and capabilities. In turn, earned trust can help expedite the development and deployment of Smart City capabilities.

Indeed, the failure to proactively manage cybersecurity and privacy risks can be a detriment to Smart City efforts and can negatively impact the very systems intended to improve city services and citizens' livelihoods. In the example of SingHealth, a data breach and data exposure was the catalyst for Singapore to temporarily suspend its Smart Nation activities and conduct a holistic review of its cybersecurity and privacy practices. SingHealth suffered deep monetary fines. It is certainly plausible to see how data breaches or leakages could erode public support for Smart City implementations that require the collection, processing, and storage of citizen- or community-related data. Proactively managing cybersecurity and privacy risks can prove to be more effective and cost-efficient, especially when considering the total cost of ownership and including potential costs of breach response and remediation.

Ultimately, municipalities should continue to focus on the primary mission of improving the livability of their communities; however, cybersecurity and privacy risk management should be viewed as essential supporting functions. Smart city solutions should be developed and deployed in a risk-aware manner, and cybersecurity and privacy should be included as areas of risk (alongside others, such as fiscal, environmental, legal, or contractual).

The following chapter and the supporting appendices focus on describing the key elements of a cybersecurity and privacy risk management process or program. There is no one-size-fits-all approach to cybersecurity and privacy risk management. Municipalities and Smart City stakeholders will need to determine what risk management processes and functions fit their needs the best, with the understanding that the approach to risk management will necessarily adapt and mature over time as requirements and risks change.

Chapter 3. Trustworthy Smart Cities through Risk Management

Organizations participating in the Smart City environment – whether as municipalities, critical infrastructure operators, product or service providers, or citizens – already consider at least some aspects of risk (e.g., business risk, reputational risk) in the development and deployment of Smart City capabilities and solutions. And one growing area of risk is cybersecurity and privacy risk.

Many of the cybersecurity- and privacy-related vulnerabilities and threats that could affect Smart City environments are similar to those commonly found in the traditional enterprise IT environment. The cyber-physical aspects of Smart Cities as well as the interconnections and interdependencies that are characteristic of Smart City solutions could potentially result in more complex and catastrophic consequences (e.g., disruption of government services to citizens; terrorist event; danger to public health or safety). The recognition of these vulnerabilities, threats, and consequences necessitates the consideration and adoption of risk management processes and practices that can help Smart City organizations make risk-based business decisions, such as identifying what levels of risk are acceptable and where investments need to be made to mitigate risk.

Cybersecurity and privacy risk management does not have to be an undue burden. In fact, there are a variety of tools that can make it easier to integrate risk management; and risk management, in turn, will be an enabler for Smart City solutions and capabilities.

- There is an abundance of existing guidelines, standards, and references to inform and improve risk management processes
- Risk management can be a tool and enabler for Smart City solutions by establishing and increasing trust in government and trust in systems
- Leveraging existing relationships (e.g., inter-/intra-governmental, public-private partnerships, new and existing suppliers) to collaborate on risk management objectives can increase effectiveness and efficiency in a limited-resource environment

While the need for cybersecurity and privacy risk management is clear, a successful risk management program will require coordination and commitment from all levels of government and from all Smart City participants.

Organizations will need to adopt processes and practices that are appropriate for their specific needs. The NIST Risk Management Framework (RMF) is one tool, of many, that can help organizations supplement and refine existing risk management practices or establish new risk management processes. At the most generic level, the RMF consists of seven iterative steps - an initial preparatory step to ensure readiness to execute the process followed by the six main steps - that can be more strategic or tactical as needed.

0. Prepare for risk management at all organizational levels
1. Categorize information and information systems
2. Select and tailor security and privacy controls
3. Implement security and privacy controls
4. Assess (independently) security and privacy controls for proper and intended implementation, operation, and risk outcomes
5. Authorize system operation
6. Monitor (continuously) to adjust to system and environment changes and to maintain awareness of organization risk posture

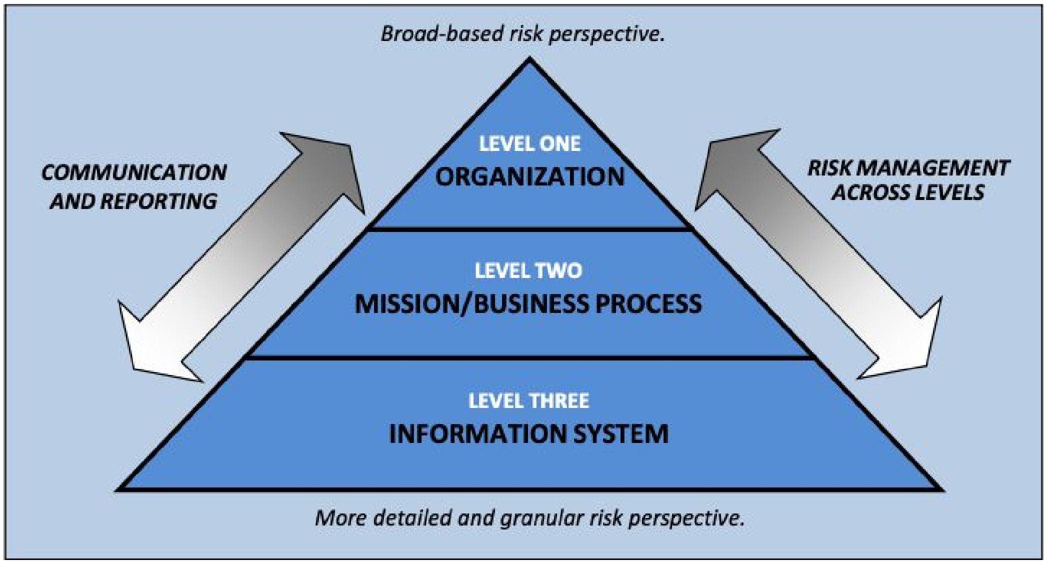
Operationalizing, standardizing and coordinating risk management across an organization is critical for minimizing cybersecurity and privacy risks during the development and operation of Smart City solutions. Cities – and all other participants in the Smart City environment – must determine the appropriate policies and processes to adopt and implement based on their current risk management practices, risk posture, and their risk management strategy.

What is Cybersecurity and Privacy Risk Management?

Risk management is a critical practice that not only assists in mitigating potential catastrophic consequences but also enables the success of Smart City systems, projects, and programs by enhancing trust. The risk management process ultimately helps organizations make risk-based business decisions, such as identifying what levels of risk are acceptable to the organization and where investment needs to be made to mitigate risk, namely by reducing vulnerabilities (e.g., implementing security or privacy controls) or limiting consequences (e.g., developing continuity of operations capabilities, purchasing cyber insurance to minimize financial loss).[8] That said, risk management is more substantial than simply implementing more cybersecurity and privacy controls.

[8] Organizations can make decisions and investments to reduce vulnerabilities and consequences. The third component of risk – threat – is external to the organization and typically cannot be directly controlled. However, organizations need to understand their sector, industry, or regional threat environment to inform their risk management processes and decisions.

NIST's Approach to Organization-Wide Risk Management


Broad-based risk perspective.
COMMUNICATION AND REPORTING
LEVEL ONE
ORGANIZATION
RISK MANAGEMENT ACROSS LEVELS
LEVEL TWO
MISSION/BUSINESS PROCESS
LEVEL THREE
INFORMATION SYSTEM
More detailed and granular risk perspective.
[9]

Risk management can be viewed as a process and practice that requires participation from, and engagement of, all levels of a given organization. The risk management functions at each level are interconnected and inform the risk decisions made at the other levels. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) proposes a three-level approach to risk management: (1) organization level; (2) mission/business process level; and (3) information system or system component level.

At the top of the pyramid, the organization establishes the risk management strategy, communicates risk management guidance, identifies missions and business processes, and provides oversight of the organization's risk posture. The risk guidance developed at the strategic levels determines the risk management activities performed at the lower, tactical levels – e.g., the information system and system component level.

The security and privacy risk management practices ultimately implemented at the information system level directly reflect the risk management principles defined by the organization. Reporting of system risk posture up to the organization level is intended to provide an aggregate view of risk across the organization, allowing the organization to adjust and achieve the desired risk posture.

In the Smart City context, the organization level may include entities such as the mayor's office and key risk-related offices such as those of the chief risk officer, chief information officer, chief information security officer, or chief privacy officer.

[9] NIST SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations*, December 2018.

Underneath this level may be a transportation mission area or an acquisition management business process area. These areas would naturally involve a wider array of stakeholders; for example, the transportation mission area may include a wide variety of transportation-related agencies, including the departments of transportation and public works as well as emergency management and law enforcement entities.

At the most tactical level – the information system level – the risk management process may focus on a single system, solution, or capability. Example systems of interest could be defined as a smart parking meter system or a system comprised of traffic sensors and the back-end traffic analytics capability. It should be noted that the depiction in the pyramid does not explicitly address the relationships with external organizations (e.g., county, state, private sector); however, supply chain risk management is certainly a critical part of the RMF.

Cybersecurity and Privacy: Differences and Overlap

The risk management process can apply to both cybersecurity and privacy. Indeed, many privacy risks and the management of those risks can be viewed as identical to or synonymous with cybersecurity risks. However, there are instances when privacy may deviate from the traditional notion of cybersecurity. Nonetheless, cybersecurity and privacy are undoubtedly interrelated and complementary and coordination between those two areas of risk is necessary.

Cybersecurity traditionally focuses on the confidentiality, integrity, and availability of data and data systems. Privacy generally pertains to specific types of data - such as personally identifiable information (PII), protected health information (PHI)[10] - and goes beyond the three core attributes of cybersecurity. Privacy necessarily requires cybersecurity (in particular confidentiality), but privacy also involves the protection of data over its entire lifecycle, including determining how it is created; how it is collected; how and where it is processed and stored; how it is used and by whom; how it is disseminated or disclosed; and how it is disposed.

While there are often shared goals between cybersecurity and privacy, it is worth noting that cybersecurity and privacy could potentially conflict at times. For example, a cybersecurity capability may require the decryption of data, thereby creating the potential for exposure or misuse. At a broader level, cybersecurity is often associated with mass collection of data and surveillance, which can raise many privacy questions. There are certainly mitigations and controls to address such conflicts (e.g., technical and administrative controls, such as data de-identification and data minimization) but ultimately, coordination between the two disciplines is necessary to ensure desired cybersecurity, privacy, and shared outcomes are achieved.

[10] It is important to note that there are varying definitions of privacy. While some definitions of privacy may be more focused on the individual citizen and associated personal data (e.g., PII, PHI), privacy principles can also pertain to intellectual property or other corporate or government data, for example.

Cybersecurity and privacy provide a means for building and establishing trust in Smart City environments. The burden, however, is on the municipality or relevant Smart City capability providers to offer adequate levels of cybersecurity and privacy. The expectation cannot be on the individual or citizen to manage and control the cybersecurity and privacy of their own data within the Smart City environment.

This document is intended to present cybersecurity and privacy risk management as a combined process. In the context of Smart Cities, cybersecurity and privacy cannot and should not be disaggregated.

Existing Risk Management Guidelines, Standards, and References

The NIST RMF is not a single standard or checklist that instructs how to perform risk management. Rather, the RMF is really a suggested approach to risk management and is supported by a collection of more detailed and specific guidelines that address specific aspects of risk management (e.g., selection of security and privacy controls). The RMF and any of the associated guidance can be used as the foundation for or as a supplement to new and existing organizational risk management processes. Furthermore, there is also a variety of risk management guidelines, standards, and references developed by organizations other than NIST that may be appropriate for some organizations.

Example U.S. Risk Management-Related Guidelines, Standards, and References

U.S. Publications	Title
NIST Special Publication (SP) 800-37 Rev. 2	Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
NIST SP 800-39	Managing Information Security Risk: Organization, Mission, and Information System View
Federal Information Processing Standard (FIPS) 199	Standards for Security Categorization of Federal Information and Information Systems
SP 800-60 Rev. 1	Guide for Mapping Types of Information and Information Systems to Security Categories
FIPS 200	Minimum Security Requirements for Federal Information and Information Systems
SP 800-53 Rev. 5 (Draft)	Security and Privacy Controls for Information Systems and Organizations
SP 800-128	Guide for Security-Focused Configuration Management of Information Systems
SP 800-34 Rev. 1	Contingency Planning Guide for Federal Information Systems
SP 800-61 Rev. 2	Computer Security Incident Handling Guide

SP 800-53A Rev. 4	Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans
SP 800-137	Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations
NIST Internal Report (NISTIR) 8062	An Introduction to Privacy Engineering and Risk Management in Federal Systems
NIST Cybersecurity Framework v1.1	Framework for Improving Critical Infrastructure Cybersecurity
NISTIR 8170 (Draft)	The Cybersecurity Framework: Implementation Guidance for Federal Agencies

Example International Risk Management-Related Guidelines, Standards, and References

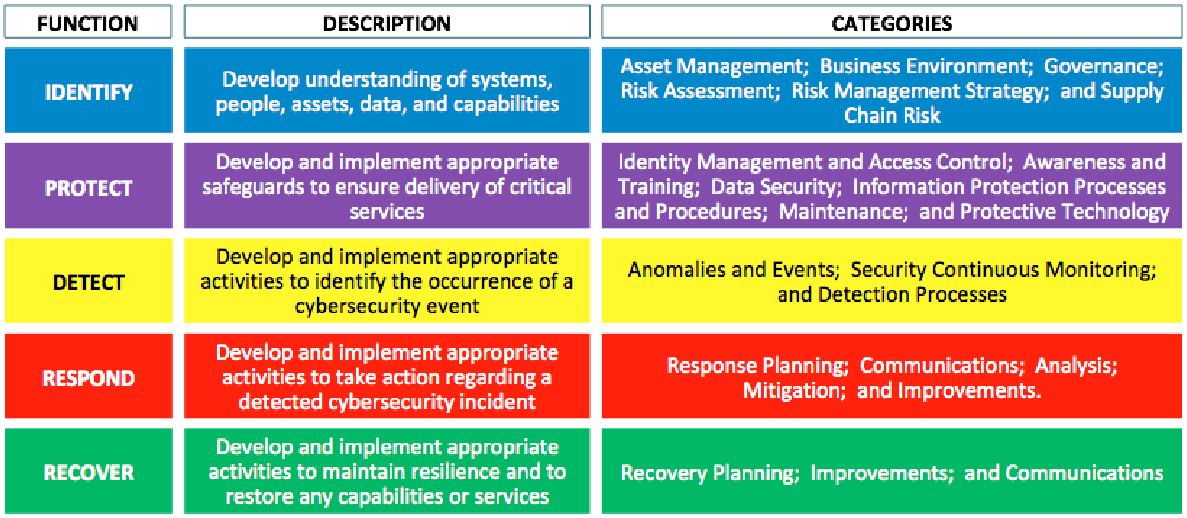
International Publications	Title
ISO 31000:2018	Risk Management – Guidelines
ISO/IEC 27000	Information Security Management Systems (ISMS) Standards
Institute of Risk Management (IRM)/The Public Risk Management Association (Alarm)/The Association of Insurance and Risk Managers (AIRMIC) 2002	Risk Management Standard
Committee of Sponsoring Organizations of the Treadway Commission (COSO) 2004	Enterprise Risk Management – Integrated Framework
OCEG Red Book	Governance, Risk, and Compliance (GRC) Capability Model
ISACA COBIT 5	A Business Framework for the Governance and Management of Enterprise IT

Given the information/data- and technology-centric nature of Smart Cities, the remainder of this risk management section focuses on the NIST RMF as a starting point for addressing Smart City cybersecurity and privacy risk management. While this summary of the NIST RMF is not intended to be prescriptive, the RMF (as well as the other existing documents) can be used as a tool to inform new risk management practices and to supplement existing risk management processes. Ultimately, organizations will have to determine which practices to implement and what the appropriate references and guidelines for those practices are.

Relationship Between the Cybersecurity Framework (CSF) and the Risk Management Framework (RMF)

The NIST Cybersecurity Framework (CSF) has received a lot of attention in the last several years as a voluntary and flexible framework for critical infrastructure organizations to improve their cybersecurity risk management practices. It is meant to be complementary to existing risk management and information security programs, and help strengthen them. The processes and taxonomies (e.g., functions, categories, subcategories) presented by CSF can generate inputs for the RMF (e.g., establishing and standardizing cybersecurity requirements, establishing tailored control baselines, or developing baseline and target profiles) and also facilitate the communication and reporting of cybersecurity and privacy risk information across the organization. The bulk of the direct alignment between the CSF and the RMF is in the RMF "Prepare" step, which is further discussed later in this document. The alignment between CSF and the other RMF steps varies considerably and can be dependent on the framework user's interpretation. The latest version of the RMF (SP 800-37 Rev. 2) was explicitly updated to provide references that indicate the alignment between the CSF and specific RMF steps and tasks.

NIST Cybersecurity Framework Core[11]



FUNCTION	DESCRIPTION	CATEGORIES
IDENTIFY	Develop understanding of systems, people, assets, data, and capabilities	Asset Management; Business Environment; Governance; Risk Assessment; Risk Management Strategy; and Supply Chain Risk
PROTECT	Develop and implement appropriate safeguards to ensure delivery of critical services	Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology
DETECT	Develop and implement appropriate activities to identify the occurrence of a cybersecurity event	Anomalies and Events; Security Continuous Monitoring; and Detection Processes
RESPOND	Develop and implement appropriate activities to take action regarding a detected cybersecurity incident	Response Planning; Communications; Analysis; Mitigation; and Improvements.
RECOVER	Develop and implement appropriate activities to maintain resilience and to restore any capabilities or services	Recovery Planning; Improvements; and Communications

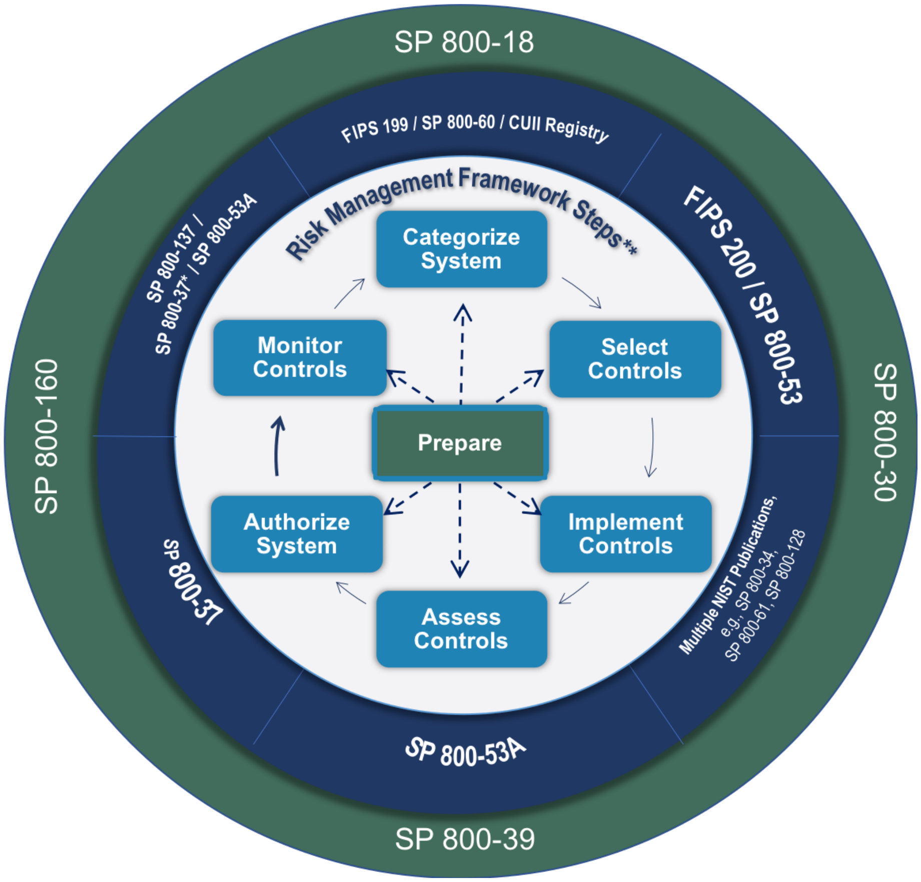
NIST Risk Management Framework

The latest version of the NIST RMF (Revision 2) describes a seven-step risk management process where the original six steps are preceded by a foundational preparation phase (i.e., Prepare). This process as a whole, as well as each step in the process, is iterative in nature and is continuously applied to information systems and information flows across the organization. Risk management should be performed in this continuous manner to account for changes in organization risk management

[11] *NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.*

strategy, evolution of the threat landscape, adoption of new technology, and other anticipated and unanticipated developments.

NIST Risk Management Framework Diagram and Corresponding NIST Guidance[12]



Step 0: Prepare

Organizational preparation is essential to attaining the risk reduction benefits of following the steps in the NIST RMF. The preparation step focuses on necessary communication and consensus-building among organizational leaders. Identifying high-impact and/or high-value systems, reaching consensus on protection and privacy priorities, risk tolerance, and allocating resources to implement and monitor controls are key issues to be addressed in preparation for executing the remaining steps in the RMF in a cost-effective and consistent manner.

Preparation is also necessary at the lower, tactical levels – i.e., system level. These activities are similar in nature and scope to the organizational preparation tasks. This includes identifying key system stakeholders, identifying and prioritizing assets

[12] "Risk Management," *NIST*. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview

and information types, and in general, determining the risk management status quo (i.e., the current state of risk management practices and posture) and intended risk objectives for the system of interest.

Key Organizational/Strategic "Prepare" Tasks and Steps

- Identify and assign key risk management roles and responsibilities[13]
- Establish and communicate organization risk management strategy
- Conduct or update organization-wide risk assessment[14]
- Determine and communicate organization-wide control baselines[15]
- Identify and document common controls[16]
- Prioritize information systems[17]
- Develop, communicate, and implement organization continuous monitoring strategy

Key System-/Tactical-Level "Prepare" Tasks and Steps

- Identify system's alignment with missions and business processes
- Identify key stakeholders
- Identify and prioritize assets
- Determine authorization boundary of system of interest
- Identify information types processed, stored, and transmitted by the system
- Determine information lifecycle
- Conduct or update system risk assessment
- Determine security and privacy requirements
- Determine system alignment with enterprise architecture
- Register system for management and oversight purposes

A more detailed and succinct description and resource for this step of the RMF is available in the form of a Quick Start Guide on the NIST website.[18]

Step 1: Categorize

The security categorization step of the NIST RMF is critical for informing the subsequent steps of the RMF process. The primary focus is for organizations and

[13] See NIST Special Publication 800-37 Rev. 2, "Risk Management Framework for Information Systems and Organizations: Appendix D" for descriptions of example roles and responsibilities that may be important for a risk management process.

[14] Reference Appendix A and B for an example of a risk assessment process and template. Another example of a risk assessment tool is the Center for Internet Security's (CIS) Nationwide Cybersecurity Review (NCSR).

[15] More detail on control baselines can be found in Step 2: Select.

[16] More detail on common controls can be found in Step 2: Select.

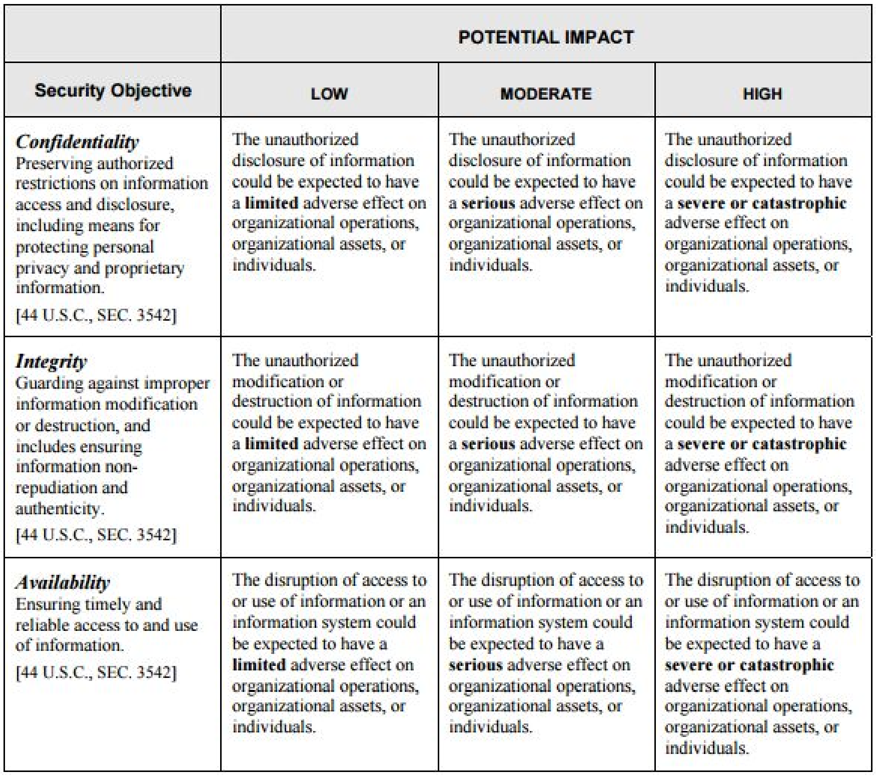
[17] More detail on prioritizing information systems can be found in *Step 1: Categorize*.

[18] "NIST Prepare Quick Start Guide," https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides/Step-0-Prepare, February 2019.

system owners to determine the potential consequences (e.g., mission, legal, continuity of operations) associated with each information type (e.g., personally identifiable information (PII), accounting data, traffic information, energy production data) processed, stored, or transmitted by an information system in a systematic and consistent manner across the organization. This provides a structured process for prioritizing assets.

For each system, information types will need to be identified and categorized. The information types can be categorized based on potential impact values (i.e., low, moderate, high) for each security objective (i.e., confidentiality, integrity, availability). For example, the *confidentiality* impact value of PII is generally considered to be *moderate* by NIST. The figure below depicts NIST's approach, which results in each information type being assigned one of nine possible "security objective-potential impact" combinations.

FIPS 199 Potential Impact Definitions for Security Objectives



	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

[19]

The highest potential impact identified for a given system can then be used to determine the security impact level of the information system as a whole (e.g., a system that processes a high-impact information type should be categorized as a high-impact information system). The system security category can prescribe, at a

[19] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

minimum, a predetermined security control baseline (e.g., baseline for high-impact information systems). Adjustments to information type impact values and system security categories may be necessary to account for specific risk considerations that are not evident in standard organizational guidance and security control baselines.

Key "Categorize" Tasks and Steps

- Prepare for system categorization[20]
- Identify information types
- Select the provisional impact values for each type of information
- Adjust the information type's provisional impact values and system security category based on organization risk management strategy and guidance
- Determine, approve, and maintain the system security impact level (e.g., low/moderate/high)

A more detailed and succinct description and resource for this step of the RMF is available in the form of a Quick Start Guide on the NIST website.[21]

Step 2: Select

The selection of security controls[22] – including, but not limited to, management, operational, and technical risk mitigations – is essential for protecting an organization's systems and information and enables the execution of the organizational mission. Selection of security controls involves identifying the set of controls that can appropriately and adequately mitigate risk in a cost effective manner while also maintaining compliance with any applicable policies, standards, laws, or regulations. The security categorization process determines the set of baseline security controls from which the selection process begins (e.g., high-impact systems start with the high-impact baseline). The standardization of sets of baseline security controls can also enable organizations to convey security requirements to external vendors and service providers. Organizations and information system owners will need to make adjustments to the security controls to account for considerations such as organization-specific requirements; operating environment needs; targeted threats; and legal and regulatory compliance standards.

It is also important to note that there are three types of security controls that differ based on their scope and applicability: system-specific; common; and hybrid.

1) System-specific: security capability for a specific information system

[20] Note that there is some overlap between these "Categorize" steps and the system-level steps delineated in the "Prepare" phase.

[21] "NIST Categorize Quick Start Guide," https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/step-1-categorize, February 2019.

[22] Refer to Appendix A. Smart Cities Use Cases for more detailed examples of selection and implementation of specific security and privacy controls.

2) Common: security capabilities for multiple information systems (or organization-wide)
3) Hybrid: security capabilities that have both system-specific and common attributes

Taking a holistic view of an organization’s information systems, their security categories, and the organization’s risk profile can enable organizations to select a set of common controls to protect multiple information systems. This practice can prove to be more cost effective and can result in more consistency in technology, architecture, and process across the organization.

Key “Select” Tasks and Steps

- Choose a set of baseline security controls
- Tailor and supplement the baseline security controls to meet organization-, environment-, and system-specific needs
- Specify minimum assurance requirements, as necessary, to determine proper implementation and efficacy of security and privacy controls
- Complete system security and privacy plans
- Develop continuous monitoring strategy
- Review and approve system security and privacy plans

There is a multitude of existing reference material for selecting security and privacy controls and for establishing baseline sets of controls. The following are examples of existing resources:

- NIST SP 800-53 Rev. 5 – *Security and Privacy Controls for Information Systems and Organizations*
- Center for Internet Security (CIS) [“Top 20”] Controls V7.1 and the CIS Controls Internet of Things Companion Guide
- NIST SP 800-66 Rev. 1 – *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*[23]
- NIST Cybersecurity Framework v1.1 - *Framework for Improving Critical Infrastructure Cybersecurity*
- NISTIR 8170 – *The Cybersecurity Framework: Implementation Guidance for Federal Agencies* and supplemental materials
- ISO/IEC 27002:2013 – *Code of Practice for Information Security Controls*
- CTIA Cybersecurity Certification Test Plan for IoT Devices, August 2018

Establishing and communicating the security and privacy control baselines is an important task in the “Prepare” phase of the RMF, and these baselines will need to be updated and re-disseminated to reflect changes in the risk and technology environment.

[23] This guidance can help organizations subject to HIPAA map NIST SP 800-53 security controls to HIPAA rule requirements.

A more detailed and succinct description and resource for this step of the RMF is available in the form of a Quick Start Guide on the NIST website.[24]

Step 3: Implement

Conceptually, the implement step of the RMF may be the most straightforward. The focus of this step is to implement the controls specified in the select step and to document the baseline configurations of these security controls. In circumstances where organizations or system owners may not be able to directly affect the implementation of a control – for example, in an external system or a specific COTS component – it may be necessary to test, evaluate, and validate prior to implementation to ascertain the presence and efficacy of an embedded security control.

Key "Implement" Tasks and Steps

- Implement controls specified in approved system security and privacy plans
- Establish baseline configurations for security and privacy controls
- Update system security and privacy plans to reflect control implementation outcomes

---

Step 4: Assess

The assessment step of the RMF focuses on assuring that implemented security controls – including system-specific, common, and hybrid – are implemented in a correct manner; operating as intended; and producing the intended security, privacy, or risk mitigation outcome. This generally requires identifying an experienced assessor or assessor team with the appropriate levels of technical and policy expertise as well as independence from the organization and system owners. This step – similar to the other steps and the entire RMF process – must be iterated as systems mature and as the organization's risk posture evolves.

Key "Assess" Tasks and Steps

- Select independent assessor or assessor team
- Develop assessment plan
- Conduct security and privacy control assessment
- Report findings and recommendations
- Implement initial remediation actions, reassess remediated controls, and update system security and privacy plans
- Develop a plan of action and milestones (POA&M) for remediation of remaining deficiencies

[24] NIST Select Quick Start Guide, https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/step-2-select, August 2018.

Step 5: Authorize

The authorize step of the RMF evaluates whether the level of cybersecurity and privacy risk of operating an information system is acceptable to the organization and the mission. This determination takes into account the outputs from the previous steps of the RMF process, including system security and privacy plans; the system-specific, common, and hybrid controls specified therein; and the findings from the assessment step (i.e., step 4). The authorization decision is typically made by a senior management official internal to the organization. This authorizing official, in collaboration with other security, privacy, and risk personnel, takes the available information (e.g., system security and privacy plans, assessment reports, organizational risk management strategy) to analyze and determine the amount of risk associated with operating a given system. This step ultimately determines whether systems are authorized to operate or not authorized to operate, along with the associated terms and conditions (e.g., authorization duration).

<u>Key “Authorize” Tasks and Steps</u>

- Generate authorization package, including outputs from previous steps such as system security and privacy plans, supply chain risk management plans, security and privacy assessment reports, and POA&Ms
- Conduct risk analysis and risk determination (by authorizing official)
- Provide risk response (e.g., risk acceptance, risk mitigation)
- Approve or deny system authorization
- Report authorization to the organization for purposes of aggregated organization-wide security and privacy risk awareness

Step 6: Monitor

Continuous monitoring enables organizations to conduct the risk management process in a continuous, near real-time manner rather than as a rigid process with a pre-determined schedule. Changes in system configurations, hardware, software, interdependent systems and connections, threat environment, etc. are inevitable over the life of the system. As such changes occur, organizations need to be able to continuously evaluate system-specific and organizational risk posture and to adjust accordingly (e.g., re-categorize systems, select and implement additional controls, remove obsolete controls). While system owners may initially need to designate a frequency at which these monitoring tasks are performed, the objective is to continually mature to a more frequent, more continuous risk management process, especially for prioritized and high-impact systems and controls. For example, common controls may be of higher priority to be continuously monitored due to their broad application across enterprise information systems. The transition from periodic monitoring to more continuous monitoring can also be facilitated through the use of automated tools.

Key Organizational/Strategic "Monitor" Tasks and Steps

- Monitor system and environment changes
- Conduct ongoing assessment of security and privacy control effectiveness and ongoing risk analysis and response
- Update authorization status and related documents
- Report security and privacy posture
- Conduct ongoing system authorizations
- Dispose of systems, as necessary (i.e., when systems are removed from operation)

Key System-/Tactical-Level "Monitor" Tasks and Steps

- Prepare and develop a continuous monitoring plan
- Document changes to system or environment and determine potential impact
- Assess a subset of security and privacy controls
- Conduct remediation activities
- Update selected security and privacy controls and related documentation
- Report security status to organization
- Conduct risk analysis and determination
- Implement decommissioning plan, as necessary

A more detailed and succinct description and resource for this step of the RMF is available in the form of a Quick Start Guide on the NIST website.[25]

[25] NIST Monitor Quick Start Guide, https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/risk-management-framework-(rmf)-step-6-monitor, August 2018.

Chapter 4. Key Smart City Risk Management Considerations

Operationalizing and standardizing risk management across the organization is critical for minimizing cybersecurity and privacy risks during the development and operation of Smart City capabilities and solutions. It will be up to cities and their partners to determine the appropriate risk management policies and processes to adopt and implement based on their current risk management practices, risk posture, and their risk management strategy. While aspects of risk management may seem daunting and challenging, there are certainly opportunities that cities can leverage to their advantage.

The following considerations are things that Smart City organizations should keep in mind as they pursue the development, adaptation and maturation of their risk management programs.

Strategic Considerations

- ***Risk management as a Smart City enabler -*** Proper risk management practices and communication of those risk management practices can actually help enable the development, deployment, and operation of Smart City capabilities. Risk management should not be viewed as an encumbrance. Proper cybersecurity and privacy controls can help gain public trust and buy-in and promote requisite participation in Smart City functions.

- ***Adapt perspective to look beyond traditional IT enterprise -*** IoT projects introduce devices with connectivity and computational power at the network edge. Previously, devices with these capabilities were generally contained within data centers or other network segments that could be configured for limited ingress/egress and monitored. Existing threat models and risk management strategies and practices may need to be adapted and extended to cover these new system components.

- ***Identifying, understanding, and assessing interdependencies -*** Smart city functionality may introduce new dependencies (e.g., data dependencies), and risk management decisions will need to consider the nature of these interdependencies. While an information system or an information type may be low impact for some stakeholders, the system or data may be high impact in another stakeholder's context. Organizations need to consider these differences in classification for such systems and data and ensure that they are protected at the appropriate level. Additionally, it is worth noting that interdependencies between traditionally “cyber” and traditionally “physical” systems is fundamental to Smart Cities. Identifying these interdependencies and understanding and assessing how cybersecurity and privacy risks can potentially translate into, for example, safety-related risks is critical.[26]

Coordination and Communication Considerations

- ***Intra-governmental coordination and collaboration -*** Given the interconnectedness and multi-stakeholder nature of Smart City capabilities and solutions, successful risk management will require significant communication, collaboration, and coordination between city departments and agencies. This necessitates the development of consensus, modification of existing structures and processes, and consideration of new shared resource and service models.

- ***Public-private and intergovernmental coordination -*** Smart city systems often involve a mix of assets that are inherently multi-party and multi-jurisdictional (e.g., city-owned and operated; regional; commercially-owned and operated). Implementations involve numerous government, private sector, and quasi-governmental organizations and their associated products, services, capabilities, oversight, etc. Successful risk management will require sharing of information (including potentially business-sensitive information), coordination of risk management and governance practices, and alignment of organizational and system boundaries. Increasingly complex interconnectivity and interdependency will necessitate particular attention to IT and data stewardship. Understanding and clearly delineating system, data, risk, and liability ownership - and ultimately, accountability - will be essential to managing cybersecurity and privacy risk in an effective manner. As Smart City projects have the unprecedented potential to impact residents either positively or negatively, special care needs to be given to engage the residents throughout the project lifecycle.

- ***External communication of risk management strategy and policies -*** It is important for organizations to adequately communicate risk management strategies, policies, and guidance not only to internal departments and agencies but also to existing and prospective external partners, service providers, vendors, and constituents. This enables external parties to understand the risk management environment in which they are expected to participate and also enables providers to develop capabilities based on well-established risk management practices (e.g., security and privacy control

[26] *NIST SP 1190GB-5: Guide Brief 5 - Assessing Energy System Dependencies,* provides an example of how system and organizational interdependencies can be identified and evaluated. This publication is specific for energy systems but could be extended for use in other domains.

baselines). Additionally, capability providers will be better enabled to collaborate with other capability providers and ensure that potential integrations of their offerings are compatible and do not create unmanageable risks.

Resource Planning Considerations

- ***Evaluate costs and benefits of cybersecurity and privacy upfront -*** Cybersecurity and privacy risk mitigations must be considered as part of the overall budget of any IoT project. Some costs may be upfront (e.g., system design reviews, pre-deployment comprehensive penetration testing) and others might be ongoing (e.g., active network traffic monitoring, insurance). Additionally, the potential technical, contractual, and legal costs associated with remediation and recovery from a breach or attack also need to be considered and factored into the risk calculus. Investing in cybersecurity and privacy risk management capabilities upfront can have the benefit of mitigating or minimizing these potential costs (i.e., paying down risk).

- ***Account for and provide resources for capability sustainment and maturation -*** Risk management and the implementation of cybersecurity and privacy controls is not a one-time, compliance-based effort. It is a repetitive process that will compel updates as technology advances, risk profiles adjust, and the organization's risk management program matures. Organizations will need to ensure that risk management capabilities and processes can be sustained and allowed to improve and mature as required.

- ***Leverage existing IT/system assessment and auditing functions -*** If a city already has an independent assessor or auditor (whether a government organization or a contractor) for their enterprise IT systems, the scope of work could be expanded to include Smart City systems. However, the city will need to consider whether the assessor or auditor has the requisite, specialized expertise to evaluate the diverse set of Smart City technologies and systems.

Procurement, Contractual, and Supply Chain Considerations[27]

- ***Consider both insourcing and outsourcing for risk management functions* - ** The decision to insource or outsource certain capabilities, services, or functions is particularly important from the cybersecurity and privacy risk management perspective. These decisions should also consider initial implementation and ongoing operation and maintenance of capabilities. Some municipalities, particularly those who may be smaller or less mature,

[27] An in-depth discussion of supply chain risk management practices, considerations, and controls can be found in *NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

may not have the capacity to build out suitable in-house staffs and associated infrastructure. With proper guidance and procurement processes, vendors should be able to build in or provide certain cybersecurity or privacy functions, thereby decreasing the burden on in-house resources. However, a risk decision of whether to trust vendor attestations or to evaluate and validate outsourced cybersecurity and privacy functions in-house or through a third-party will come into play.

- ***Leverage acquisition and procurement mechanisms -*** Risk management needs to include acquisition and procurement offices and personnel – both in the establishment and implementation of risk management strategies and practices. Smart city solutions' dependence on external services and COTS products provides an opportunity for Smart City buyers to dictate risk management requirements in contractual agreements, service level agreements, product certifications, etc. This is a means for Smart Cities to have some level of control over the security and privacy of systems and products that would otherwise be out of their control and ultimately assist in mitigating enterprise risk. However, procurement strategies and practices need to be flexible and be able to adapt to changing threat environments and corresponding cybersecurity and privacy requirements.

- ***Understand supply chain to truly determine risk profile -*** Smart cities are inherently dependent on industry partners to support new development and capabilities in a variety of dynamic areas - e.g., distributed energy production/management, telecommunications, traffic and facilities management, supporting infrastructure and services and cloud providers. Simply evaluating the cyber hygiene of the Smart City is not enough. To fully understand what exposure to harm (legal or cost related) exists, Smart Cities must carefully evaluate how business partners support or directly interact with Smart City resources. Independent studies show an alarming increase in successful compromises as a result of third parties. Municipalities should solicit assistance from regulatory, legal, and cyber subject matter experts as to how to ensure a lower risk profile by requiring enhanced security posture of the Smart City's supply chain. The interdependency between municipality and the private sector is extensive and the ability to effectively underwrite insurance for next generation Smart Cities will be dependent on evolving legally binding agreements (e.g., service level agreements, terms and conditions, solicited/unsolicited proposals) to clearly define how to transfer or mitigate risk exposure associated with the supply chain.

- ***Management of risk from external services, systems, and products -*** Smart cities' reliance on external services, contractor-owned systems, and COTS products necessitates mechanisms to ensure the risks associated with external services, systems, and products are properly managed. This includes all aspects of the risk management process, including the prioritization of systems and assets; the selection and implementation of controls; and the independent assessment and continuous monitoring of systems. This may require contractual agreements, service level agreements, or participation in independent, third-party certification programs; these mechanisms must also be able to adapt to the evolving technology environment, threat landscape, and cybersecurity and privacy requirements.

- ***Require vulnerability notification from commercial product suppliers -*** Smart city deployments will undoubtedly involve COTS products and IoT devices of varying degrees of maturity - including cybersecurity and privacy capability maturity. As products mature and the threat landscape changes, it is essential for system and data owners to be notified of and aware of newly discovered vulnerabilities in a timely manner. Actions that follow notification of vulnerabilities will be dependent on the assessment of risk associated with that particular vulnerability, the available mitigations (e.g., patches), and the costs, including labor, financial, potential system downtime, downstream effects on interdependent systems, etc.

<u>Technical and IoT-Specific Considerations</u>

- ***Technological diversity and limitations -*** Given the diverse array of technologies in the Smart City environment (e.g., IoT devices), selected controls – including common controls – may not be able to be implemented as intended. Factors restricting implementation may include limitations in built-in functionality, processing power, battery life, etc. This may necessitate significant effort in terms of tailoring security and privacy controls, determining compensating controls, or assessing risk acceptance. Organizations and system owners will need to document how controls are actually implemented and configured and determine whether the residual risk is acceptable.[28]

- ***Common control challenges and opportunities -*** Collaboration across government departments and agencies can lead to increased efficiency, for example, with the identification and implementation of common controls. However, diversity of technologies, architectures, and infrastructures could limit the feasibility of common controls. Collaboration from policy,

[28] Additional discussion of IoT and associated cybersecurity and privacy risks and considerations can be found in the following resources: *NISTIR 8228: Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*; *NIST Cybersecurity White Paper: Internet of Things (IoT) Trust Concerns*; *NIST SP 1900-202: Cyber-Physical Systems and Internet of Things*; and the Cybersecurity and Infrastructure Security Agency's (CISA) publication titled *The Internet of Things: Impact on Public Safety Communications*.

governance, budget, and infrastructure perspectives may be needed to maximize the effective implementation of common controls. Establishing, implementing, and maintaining common controls can be enabled by some of the other considerations identified in this document (e.g., leveraging the procurement process, external communications).

- ***Continuous monitoring in highly dynamic smart environment -*** Smart city environments are highly dynamic with frequent changes to the technology environment. Corresponding cybersecurity and privacy requirements and controls will undoubtedly need to be revised, updated, reconfigured, etc. Organizations and systems owners will need to determine the appropriate minimum frequency at which necessary risk management processes will be conducted. This frequency may vary by system security category and impact level, mission, information type(s), and other organization risk factors. That said, the long-term risk management objective is to continue to move towards increased automation and truly continuous (i.e., real-time) monitoring of risk.[29]

<u>Legal and Liability Considerations</u>

- ***Understand new and/or additional regulatory exposure -*** Depending on the organization(s) and on the types of data being processed by the IoT system, various regulatory requirements may come into effect. For instance, if a system includes healthcare data (e.g., vital sign information from wearable sensors worn by first responders), HIPAA may apply. Alternatively, if a system includes data that allows members of the public to be identified (e.g., video recordings), various privacy regimes may apply, such as GDPR or California data privacy laws.

- ***Risk mitigation through cybersecurity insurance -*** Smart cities can consider cybersecurity insurance as a risk mitigation measure (i.e., risk transfer). Cybersecurity insurance is an expanding and open area of business support/development, and can reduce potential financial loss (i.e., consequence) and thereby reduce total risk. However, insurance would only be suitable for mitigating certain risks (i.e., those that can directly translate into monetary loss). A recent Wall Street Journal survey suggested that a

[29] Indeed, NIST 800-37 Rev. 2 recommends that "Organizations should maximize the use of automation, wherever possible, to increase the speed, effectiveness, and efficiency of executing the steps in the Risk Management Framework (RMF). Automation is particularly useful in the assessment and continuous monitoring of controls, the preparation of authorization packages for timely decision-making, and the implementation of ongoing authorization approaches—together facilitating a real-time or near real-time risk-based decision-making process for senior leaders. Organizations have significant flexibility in deciding when, where, and how to use automation or automated support tools for their security and privacy programs. In some situations, automated assessments and monitoring of controls may not be possible or feasible."

majority of the 25 largest U.S. cities have cyber insurance or are considering purchasing it.[30]

- ***Cautious use of non-disclosure agreements -*** The use of non-disclosure agreements (NDA) should be carefully considered. The municipality may need to share vendor information with external regulatory bodies or even other vendors (e.g., data formats sent by an IoT device may need to be known by packet inspection engines). NDAs should provide enough latitude to enforce the municipality's chosen cybersecurity and privacy risk posture while also respecting vendors' intellectual property and proprietary information. The municipality will benefit from periodic technology audit/risk review assessments, similar to those carried out for financial audits and reviews of banks, financial, and other complex organizations.

[30] Calvert, Scott and Jon Kamp. "More U.S. Cities Brace for 'Inevitable' Hackers," *The Wall Street Journal*. https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401

Chapter 5. Conclusion

Smart cities and communities are not sustainable or truly smart if they do not proactively and adaptively identify, deploy, and sustain cybersecurity and privacy risk management processes and measures. This Guidebook intends to assist all cities and communities with a Smart City cybersecurity and privacy risk management vision to familiarize with basic practices, major challenges, and key Smart City-specific considerations ultimately to avoid common and costly mistakes.

We wish to point out three caveats for reader awareness. One is that this Guidebook is intended for general purposes. More granular guidance for specific functions such as public safety or smart buildings can be found in GCTC SuperClusters' blueprints. Those blueprints and this Guidebook are aligned in cybersecurity and privacy as ensured by the CPAC and the SuperClusters' leadership teams.

The second caveat is that although this Guidebook lays a solid foundation for specific tools that can be used in support of cybersecurity and privacy risk management, such tools are not introduced at this time. CPAC aims at identifying such tools in the near future. One example is a cyber risk needs assessment tool that starts with municipalities' digital properties and characteristics and recommends best practices pertinent to their situation and target risk posture.

The third caveat is that technologies continue to rapidly evolve, as well as solutions, best practices, and considerations. This Guidebook is a living document and will be updated as warranted. Please be sure to reference the latest version.

We encourage readers to refer to the Appendices to see example use cases of how risk management processes can be leveraged and integrated in specific Smart City implementations. These use cases can exemplify cybersecurity and privacy risk management concepts in real-world scenarios. The Appendices also provide a list of references used in the development of this document and can provide readers with more in-depth and detailed information regarding specific aspects of cybersecurity and privacy risk management.

Appendix A. Smart Cities Use Cases

The following use cases demonstrate how aspects of the risk management framework has been operationalized and used to apply a risk-based approach to managing Smart City cybersecurity and privacy in real-world situations:

- **Use Case #1:** Tampa Hillsborough Expressway Authority (THEA) Connected Vehicle (CV) Pilot Security Management Operating Concept (SMOC)
- **Use Case #2:** Risk Assessment and Prioritization in the Smart City Cyber Resilience Planning Process
- **Use Case #3:** Risk Assessment in the County of San Mateo, California
- **Use Case #4:** Managing Cybersecurity and Privacy Risk for Smart Public Safety IoT Devices and Systems
- **Use Case #5:** Risk Management in a Privacy-Specific Context

These illustrative examples are intended to address specific aspects of cybersecurity and privacy risk management and are intended to help bridge the gap between the strategic/abstract concepts described herein and tactical/concrete activities in real-world scenarios.

Use Case #1: Tampa Hillsborough Expressway Authority (THEA) Connected Vehicle (CV) Pilot Security Management Operating Concept (SMOC)

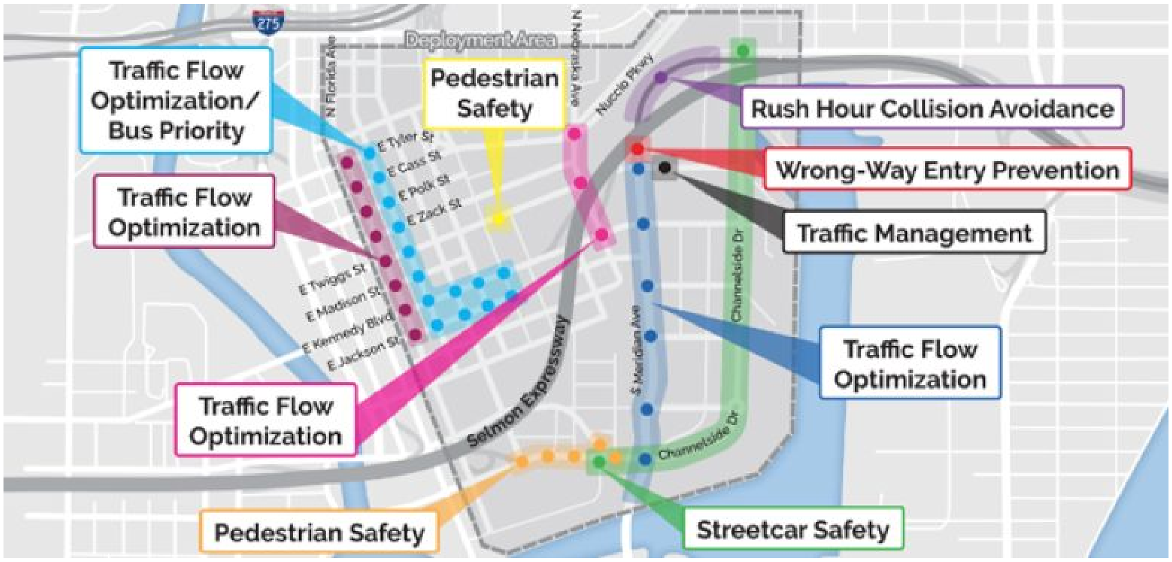
The following use case describes the development of a Security Management Operating Concept (SMOC) for phase I of the Tampa Hillsborough Expressway Authority (THEA) Connected Vehicle (CV) Pilot Deployment Program. This focuses on how the THEA team developed an approach to the SMOC (i.e., *Prepare*); categorized information flows and systems (i.e., *Categorize*); and selected security controls to establish draft, minimum security control baselines (i.e., *Select*). The resulting SMOC is largely based on the NIST RMF and provides guidance for ensuring “the privacy of pilot participants and the overall security of the Vehicle-to-Everything (V2X) system for the THEA CV Pilot.”[31]

The THEA CV Pilot Deployment Program is sponsored by the U.S. Department of Transportation’s (DOT) Intelligent Transportation Systems Joint Program Office and is focused on leveraging vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) technology to improve traffic safety, congestion, and emissions in Tampa, Florida.

[31] Kolleda, Joshua; Dominie Garcia; and Tyler Poling. *Connected Vehicle Pilot Deployment Program Phase I: Security Management Operational Concept - Tampa Hillsborough Expressway Authority (THEA)*, May 2016.

Some smart transportation applications that may leverage the V2V and V2I technologies include intelligent signal systems; pedestrian collision warnings; transit signal priority systems; and wrong way entry warnings.

THEA CV Pilot Deployment in Downtown Tampa[32]



<u>Step 0: Prepare</u>

In this initial step, the THEA team conducted three primary activities:

- Gather references (e.g., FIPS 140-2, Common Criteria) and existing analyses (e.g., CAMP V2V-Interoperability reports, European Telecommunications Standards Institute (ETSI) Threat, Vulnerability and Risk Analysis (TVRA))
- Review existing resources on CV security analysis and requirements (e.g., DOT Security Credential Management System)
- Determine SMOC approach and develop high-level SMOC outline

<u>Step 1: Categorize</u>

In the next step, the team identified all information flows for each application in the Pilot and categorized them using Confidentiality, Integrity, and Availability criteria from FIPS 199. Devices that act as either source of destination for information flows were further categorized by the types of information and those Confidentiality, Integrity, and Availability criteria. Lastly, information flows were also assessed against privacy-specific criteria.

The following bullets summarize the primary activities of this step:

- Review and map smart transportation applications to be deployed
- Categorize information flows based on Confidentiality, Integrity, and Availability

[32] *Tampa Hillsborough Expressway Authority*, "THEA Connected Vehicle Pilot - Fact Sheet."

- Rollup information flow categorizations to the “information system”
- Supplement threat assessment with existing analyses
- Assess each information type for each application to determine extent systems will collect or store PII or PII-related information
- Update categorization and threat assessment, as necessary, based on CV Pilot team meetings

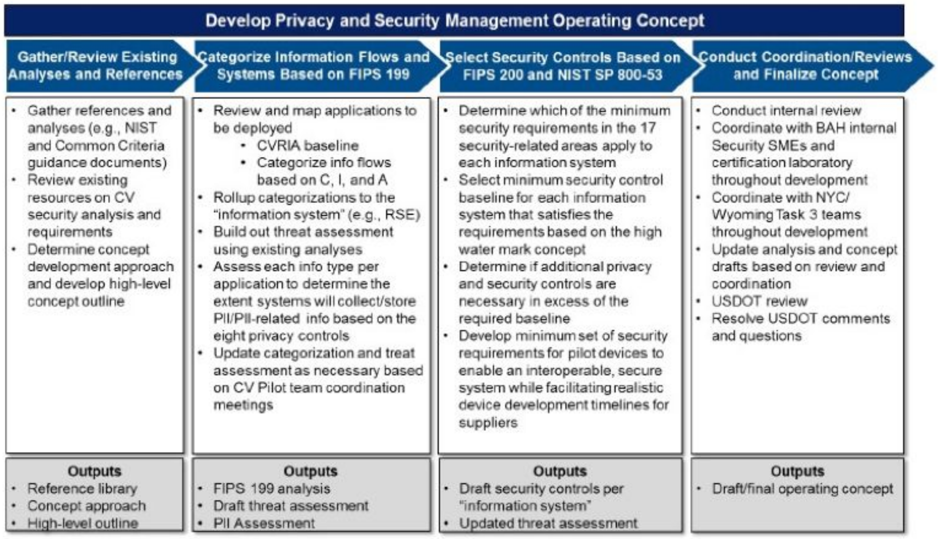
Step 2: Select

Based on the threat assessment and the categorization of information types, devices, and systems, the THEA team selected security controls and created minimum security control baselines for CV Pilot devices and systems. This exercise leveraged the FIPS 200 and NIST SP 800-53 resources and focused on areas such as communications, access, hardware, software, and operating system security considerations.

The primary activities included the following:

- Determine which security controls and requirements apply to each information system
- Select minimum security control baseline for each information system
- Determine if additional security and privacy controls are necessary beyond the baseline
- Develop minimum security requirements for pilot devices that balance interoperability, security, privacy, and realistic device development timelines for suppliers

Development of the THEA Privacy and Security Management Concept[33]



Develop Privacy and Security Management Operating Concept

Gather/Review Existing Analyses and References	Categorize Information Flows and Systems Based on FIPS 199	Select Security Controls Based on FIPS 200 and NIST SP 800-53	Conduct Coordination/Reviews and Finalize Concept
• Gather references and analyses (e.g., NIST and Common Criteria guidance documents) • Review existing resources on CV security analysis and requirements • Determine concept development approach and develop high-level concept outline	• Review and map applications to be deployed • CVRIA baseline • Categorize info flows based on C, I, and A • Rollup categorizations to the “information system” (e.g., RSE) • Build out threat assessment using existing analyses • Assess each info type per application to determine the extent systems will collect/store PII/PII-related info based on the eight privacy controls • Update categorization and treat assessment as necessary based on CV Pilot team coordination meetings	• Determine which of the minimum security requirements in the 17 security-related areas apply to each information system • Select minimum security control baseline for each information system that satisfies the requirements based on the high water mark concept • Determine if additional privacy and security controls are necessary in excess of the required baseline • Develop minimum set of security requirements for pilot devices to enable an interoperable, secure system while facilitating realistic device development timelines for suppliers	• Conduct internal review • Coordinate with BAH internal Security SMEs and certification laboratory throughout development • Coordinate with NYC/ Wyoming Task 3 teams throughout development • Update analysis and concept drafts based on review and coordination • USDOT review • Resolve USDOT comments and questions
Outputs • Reference library • Concept approach • High-level outline	**Outputs** • FIPS 199 analysis • Draft threat assessment • PII Assessment	**Outputs** • Draft security controls per “information system” • Updated threat assessment	**Outputs** • Draft/final operating concept

[33] Kolleda, Joshua; Dominie Garcia; and Tyler Poling. *Connected Vehicle Pilot Deployment Program Phase I: Security Management Operational Concept - Tampa Hillsborough Expressway Authority (THEA)*, May 2016.

The operating concept was reviewed, revised, and finalized with coordination across and input from multiple teams, including the THEA team, DOT, security experts, and testing labs. The SMOC authors recognize that the concept and the requirements included within it may need to be updated based on new inputs.

Use Case #2: Risk Assessment and Prioritization in the Smart City Cyber Resilience Planning Process

This use case summarizes an engagement between a GCTC Action Cluster member, Adaptable Security Corp (ADA), and a California municipality, focusing on how the risk management process, with a particular focus on risk assessment and prioritization, played a critical role in the overall cyber resilience planning process. The content covered in this use case primarily aligns with the *Prepare*, *Select*, *Assess*, and *Monitor* steps of the RMF.

In this example, the California municipality has Smart City systems and initiatives that rely on existing, legacy IT infrastructure as well as stand-alone, dedicated infrastructure. The Chief Information Officer's (CIO) office is conscious of the increasing cyber attacks, in particular ransomware, that have been waged against the public sector; as a result, they have decided to invest in cyber resilience planning for the entire IT and Smart City ecosystem. ADA has been assisting the CIO in the multi-year planning effort.

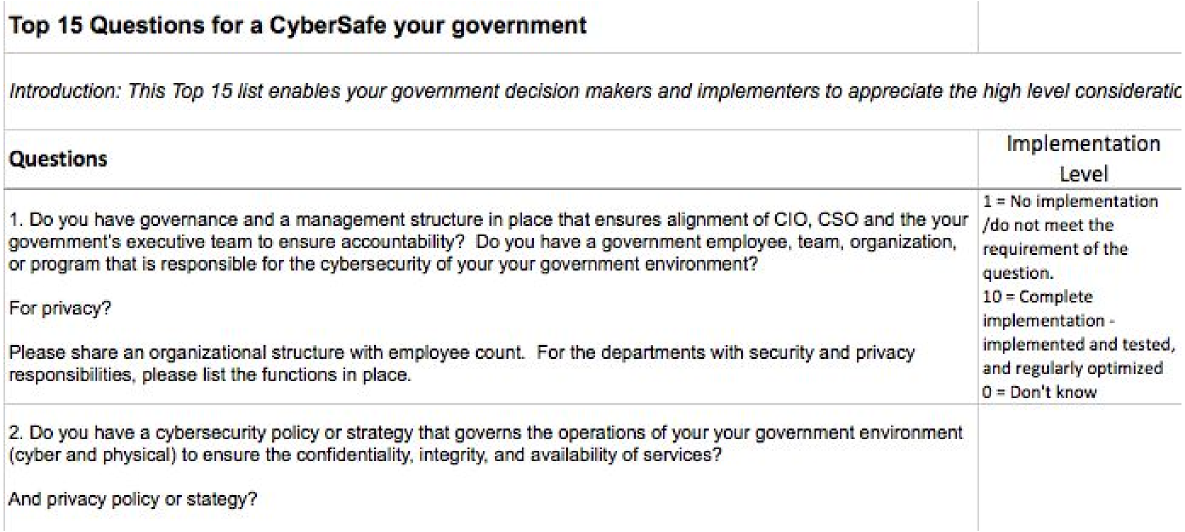
While the municipality had already adopted a comprehensive cybersecurity management plan and had already implemented the various risk management steps of *Prepare*, *Categorize*, *Select*, *Implement*, *Assess*, *Authorize*, and *Monitor* - albeit to varying degrees and different terminology - it was necessary to start with a risk assessment to understand and benchmark the municipality's starting cybersecurity and privacy status. The data presented in this use case has been modified to protect the municipality's sensitive cybersecurity and privacy information and is presented for illustrative purposes only.

Risk Assessment
Two risk assessment methods were utilized for a high-level understanding of the municipality's cybersecurity and privacy risk posture: the "CPAC 'Top X' Questions for a Trustworthy Smart City" (see Appendix C) and the Center for Internet Security's (CIS) Nationwide Cybersecurity Review (NCSR).[34] The former elicited much-needed background information such as the size of the municipality and cybersecurity staffing, while the latter assessed the maturity level of the municipality against 108

[34] "Nationwide Cybersecurity Review," *Center for Internet Security*. https://www.cisecurity.org/ms-isac/services/ncsr/

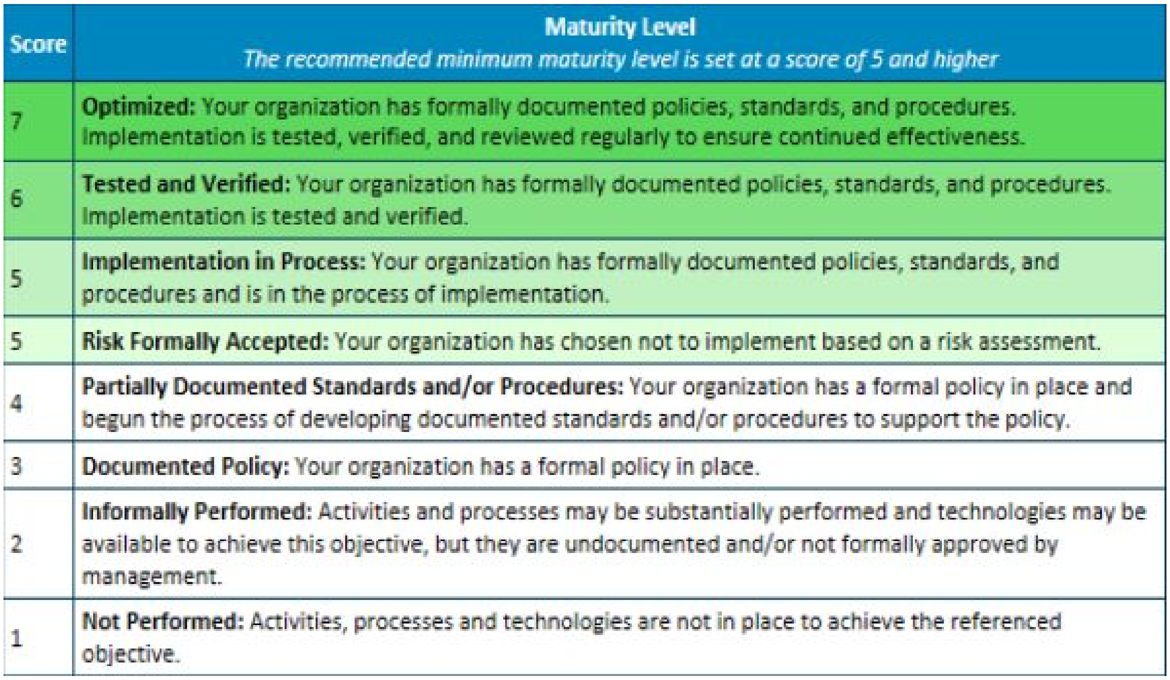
discrete controls. The NCSR maturity levels were based on a scale from 1 to 7, ranging from "Not Performed" to "Optimized," respectively. Example excerpts of each assessment have been included below.

Excerpts from "CPAC 'Top X' Questions for a Trustworthy Smart CIty"-Based Assessment[35]



Top 15 Questions for a CyberSafe your government	
Introduction: This Top 15 list enables your government decision makers and implementers to appreciate the high level consideratic	
Questions	Implementation Level
1. Do you have governance and a management structure in place that ensures alignment of CIO, CSO and the your government's executive team to ensure accountability? Do you have a government employee, team, organization, or program that is responsible for the cybersecurity of your your government environment? For privacy? Please share an organizational structure with employee count. For the departments with security and privacy responsibilities, please list the functions in place.	1 = No implementation /do not meet the requirement of the question. 10 = Complete implementation - implemented and tested, and regularly optimized 0 = Don't know
2. Do you have a cybersecurity policy or strategy that governs the operations of your your government environment (cyber and physical) to ensure the confidentiality, integrity, and availability of services? And privacy policy or stategy?	

NCSR Maturity Levels[36]

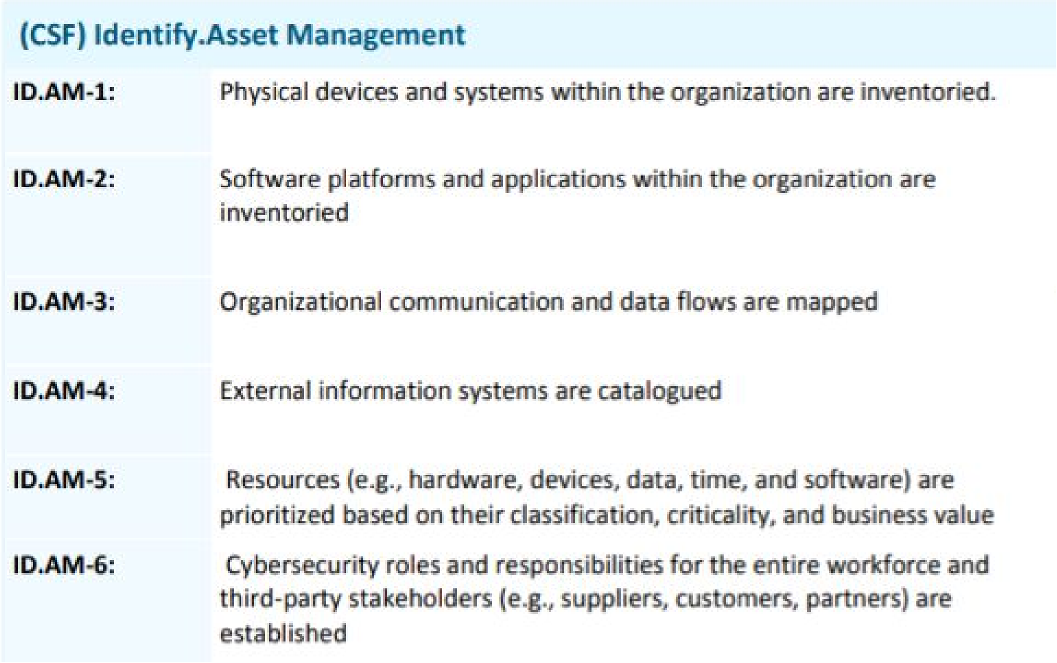


Score	Maturity Level *The recommended minimum maturity level is set at a score of 5 and higher*
7	**Optimized:** Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:** Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:** Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	**Risk Formally Accepted:** Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:** Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** Your organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:** Activities, processes and technologies are not in place to achieve the referenced objective.

[35] See Appendix C. CPAC "Top X" Questions for a Trustworthy Smart City.

[36] Multi-State Information Sharing and Analysis Center (MS-ISAC), *NCSR General User Guide*.

Sample NCSR Controls[37]



(CSF) Identify.Asset Management	
ID.AM-1:	Physical devices and systems within the organization are inventoried.
ID.AM-2:	Software platforms and applications within the organization are inventoried
ID.AM-3:	Organizational communication and data flows are mapped
ID.AM-4:	External information systems are catalogued
ID.AM-5:	Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6:	Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established

Risk Prioritization

The risk assessment resulted in two primary outputs: (1) the CIO and municipality established a vision "to enable smart, adaptable, and resilient County IT through risk-based prioritization, forward-looking security architecture, and cost-beneficial implementation;" and (2) a goal to raise the risk posture score to 5 or above (i.e., "risk formally accepted" or "implementation in process") in every category.

To accomplish this risk prioritization exercise, ADA and the municipality quantitatively assessed and ranked specific cybersecurity controls and the associated components of risk (i.e., vulnerability, threat, and consequence - or in this case, vulnerability, threat, impact, and likelihood). The output enabled the prioritization of controls for further investigation; investing in priority controls could reduce overall risk exposure. Example risk calculations are displayed in the table below and are intended to be for illustrative purposes only.

[37] Note that the NCSR is based on the NIST CSF and is focused on maturity levels of a specific set of cybersecurity and privacy controls; the CSF is a good tool for categorizing, organizing, and communicating those controls.

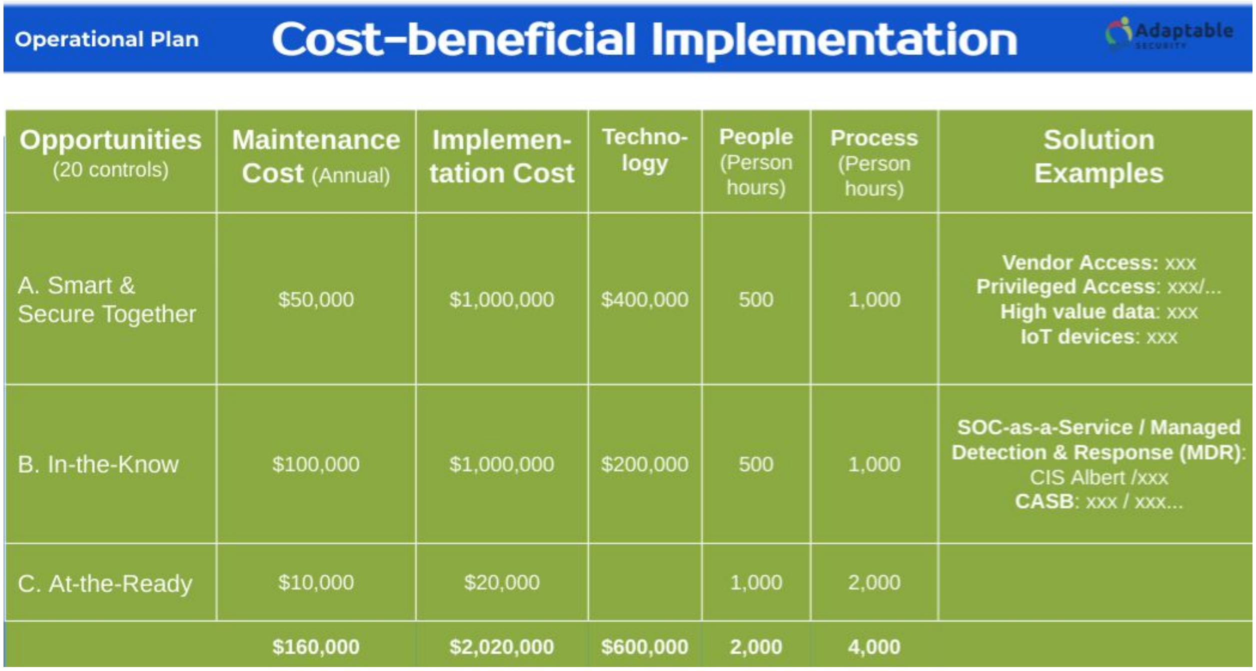
Example Risk Score Calculation

Control	Vulnerability Score (out of 5)	Threat	Likelihood	Impact	Risk Score (out of 80)
Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders are established	3	Ransomware	92%	4	35
		Phishing	92%	4	
		…	…	…	

Cost-Benefit Analysis and Control Selection

Following the risk assessment and prioritization, the next step was to identify the most economic options that would also provide satisfactory solutions to addressing the identified risks. The team adopted a model to estimate one-time implementation costs as well as ongoing annual maintenance costs. Furthermore, the implementation costs are broken down into three components: technology, people, and process; people includes consultants with specialized expertise, whereas process includes employees' time.

The following table shows an example cost-benefit analysis where each "opportunity" represents an aggregated group of controls to address one or more identified cybersecurity or privacy risk. For example, the "In-the-Know" opportunity corresponds to a set of controls related to monitoring and detection, whereas "At-the-Ready" refers to incident response- and recovery-related capabilities.



Operational Plan

Cost–beneficial Implementation

Opportunities (20 controls)	Maintenance Cost (Annual)	Implementation Cost	Technology	People (Person hours)	Process (Person hours)	Solution Examples
A. Smart & Secure Together	$50,000	$1,000,000	$400,000	500	1,000	**Vendor Access:** xxx **Privileged Access**: xxx/... **High value data**: xxx **IoT devices**: xxx
B. In-the-Know	$100,000	$1,000,000	$200,000	500	1,000	**SOC-as-a-Service / Managed Detection & Response (MDR)**: CIS Albert /xxx **CASB**: xxx / xxx...
C. At-the-Ready	$10,000	$20,000		1,000	2,000	
	$160,000	**$2,020,000**	**$600,000**	**2,000**	**4,000**	

Success Metrics

ADA and the municipality intend to regularly (e.g., quarterly, annually) monitor and measure progress in managing cybersecurity and privacy risk through three metrics:

- Overall risk posture as indicated by updated NCSR risk assessment scores
- Cybersecurity awareness survey results across key stakeholder groups
- Rating of confidence in municipality's cybersecurity posture across key stakeholder groups

These metrics, along with the updated risk assessments, can provide indications about where risk management activities are successful, deficient, or need to be adjusted. This repeatable process of identifying, assessing, and prioritizing risks followed by selecting, implementing, and assessing appropriate controls enables the municipality to manage their risk posture and adapt to an ever-evolving operating environment and threat landscape.

Use Case #3: Risk Assessment in the County of San Mateo, California

This use case describes how risk assessment has been implemented in the County of San Mateo, California, and identifies activities that align most closely with the Step 0: Prepare and Step 6: Monitor steps of the risk management process. However, the assessment process and the outputs from the assessment also involve elements from and inform all of the other risk management steps (i.e., Step 1: Categorize, Step 2: Select, Step 3: Implement, Step 4: Assess, Step 5: Authorize). Refer to Appendix B of this Guidebook for an example of the risk assessment questionnaire and its application.

The County of San Mateo uses a Risk Assessment Questionnaire to ensure that technology projects are aligned with the County's Information Security Policy. The Risk Assessment Questionnaire must be completed and then subsequently reviewed and approved by the Chief Information Security Officer's (CISO's) Security Analyst before a project is approved by the Program Management Office; hence, it serves as a controlling mechanism for compliance with the Information Security Policy.

The Risk Assessment Questionnaire establishes a control process from the CISO's office that has expert security review and analysis of key aspects of any projects where cybersecurity and privacy risks need to be reviewed and deemed compliant with the County of San Mateo's Information Security Policy.

The Security Analyst follows the existing Information Security Policy, which covers requirements such as roles/responsibilities, signed NDAs, HIPAA mandates, and procurement reviews, when reviewing the answers to the questionnaire. Ultimately, the risk assessment process informs the Program Manager and all of the project's stakeholders on the Information Security Policy compliance requirements. By identifying and substantiating risks associated with specific projects, risk response decisions (e.g., risk mitigation, risk acceptance) can be made.

Use Case #4: Managing Cybersecurity and Privacy Risk for Smart Public Safety IoT Devices and Systems

This use case provides a notional approach to address cybersecurity and privacy risks related to incorporating IoT in smart public safety applications. This use case posits some of the major activities, key stakeholders, and potential resources for each step of the cybersecurity and privacy risk management process.

A key element of Smart Cities is smart public safety. Smart public safety starts with traditional public safety agencies - namely fire, law enforcement, emergency medical services, and 911 call centers - that would like to add IoT devices as another means of communication between first responders and between the first responders and the 911 dispatch centers. Public safety agencies are already starting to use body-worn devices (e.g., cameras and biometric sensors). During the incident operations, IoT data from sensors and other real-time devices can increase situational awareness and aid in incident command and control.

Step 0: Prepare
In smart public safety, public safety agencies themselves could be responsible for cybersecurity and privacy; alternatively, they could be partnering with IT or information security organizations (e.g., Department of Information Technology). In most states in the U.S., the state legislature authorizes and appropriates funds based on an authorized scope. The IT organization will often have a cybersecurity and privacy strategy that includes using one or more of the risk management frameworks, or elements thereof.

For this use case we are assuming that we are using the NIST RMF, which has been detailed in this Guidebook. There are also existing statewide security policies; but they do not allow connected IoT devices until risk management security capabilities have been defined, and devices provide the necessary capabilities to support the requisite cybersecurity and privacy controls.

It is the intention of this support for implementation of IoT cybersecurity and privacy to be funded by further State legislature appropriating funds for extending the risk management program for Smart Cities and smart public safety which includes usage of body worn devices and supporting vendor upgrades.

Step 1: Categorize
The information types collected, processed, and transmitted by the wearable IoT devices are real-time video and sensor data. The systems and system components are categorized as critical information data, and that mandates that the systems and networks be of a public safety grade mission critical mode of operation. Public Safety Grade cybersecurity and privacy policies and standards have been described for normal mobile devices, but corresponding policies and standards for IoT-based devices still need to be defined.

Step 2: Select
NIST RMF-based cybersecurity and privacy controls have been selected for IT systems security controls. Additional cybersecurity and privacy controls for IoT would follow the NISTIR 8196[38] and NISTIR 8228[39] and the new, example (12) security controls and (4) privacy controls.

No additional controls beyond those proposed in NISTIR 8196 and NISTIR 8228 have been identified. No tailoring of controls has been done as the IT Department wants to identify and implement a standardized and consistent (i.e., baseline) set of security control. This may change as the implementation of IoT devices is better defined.

Step 3: Implement
Cybersecurity and privacy requirements from NIST SP 800-37 Rev. 2, NIST SP 800-39, NIST SP 800-53 Rev. 4, NISTIR 8196, NISTIR 8228, and other documents were used to generate specific device security capabilities requirements that support and enable the selected cybersecurity and privacy controls.

The chosen vendor solution supports a shared operational model for the operational Security Operation Center (SOC) using security information and event management (SIEM) and security orchestration, automation, and response (SOAR) capabilities. Many of the RMF functions supported by IT Department are used in support of these new IoT devices, networks, and applications.

It is anticipated that the security operations center (SOC) will implement the tools and capabilities necessary to ensure that the IoT device security capabilities are leveraged to implement the selected security controls from NIST SP 800-53 and NISTIR 8228.

[38] Draft NIST Interagency Report (NISTIR) 8196, *Security Analysis of First Responder Mobile and Wearable Devices*, December 2018.
[39] Draft NISTIR 8228, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*, September 2018.

Step 4: Assess
The Security Operations Center mitigation and monitoring personnel have the responsibility for proper implementation and operation of the selected cybersecurity and privacy controls. The SOC is staffed by IT/IoT cybersecurity analysts and then vendor specialists. There is an agreement in place that clarifies the shared or dedicated tasks.

Step 5: Authorize
N/A

Step 6: Monitor
The Chief Risk Officer (CRO) and team are responsible to work with the SOC to understand how well the risk management program is working.

Use Case #5: Risk Management in a Privacy-Specific Context

This use case describes how the risk management concepts and processes presented in this Guidebook apply in privacy-specific applications. Given the overlapping relationship of cybersecurity and privacy, much of the information in this use case may sound similar to, or even identical to, aspects of cybersecurity risk management. This reinforces the notion that cybersecurity and privacy are closely related and should generally be considered in tandem.

One fundamental tenet of Smart Cities is the creation, collection, use, and other methods of processing often vast amounts of data to improve city services and operations. This has the potential to introduce significant data privacy risks. Whether we are discussing individual privacy, corporate privacy, or municipal privacy, compromised data can result in tangible and irreparable damage. For example, individuals can lose their reputation, job, family, health coverage, bank accounts, or control of their identity; a company can lose its intellectual property, reputation, customer base, etc.; and a municipality can lose control of its infrastructure and supported services, whereby thousands or millions of people can be affected.

The RMF provides a process for establishing a Privacy Program to help organizations protect data over its entire lifecycle. The activities described below are not intended to be comprehensive, but rather identify some key privacy and data protection considerations.

Step 0: Prepare

- Identify employees and external resources - including privacy experts - to participate in a cross-departmental and -functional team
- Provide privacy training so that everyone knows what to look for and what to consider.
- Establish a regular process and meeting to identify all department's data assets.
- Document what data types are processed; current data use procedures; how electronic information is handled; past problems or gaps in process; goals that may impact data types/use; employee training and experience; what systems are used to process data; and what condition those systems are in, to name a few.
- Create a table for Data Classification of the Elements. As risks associated with a data element are identified, that data element is assigned a Classification. The Classification informs the organization of the cybersecurity and privacy measures that need to be implemented and how data handling will be restricted.
- Identify and prioritize known privacy risks.
- Conduct privacy risk assessment including identifying and determining the efficacy of existing privacy controls.
- Consider strategies for implementing improvements and reducing privacy risk.
- Identify regulatory compliance requirements.
- Establish a Privacy Policy and/or Strategy to govern the organization's privacy risk management activities and include a mechanism to routinely update the policy or strategy.

Step 1: Categorize

The types of data that are created, used, shared, viewed, stored or processed in some other way, are classified by looking at the risk consequence if the confidentiality, integrity, or availability of the data is compromised at any point in its lifecycle. A greater risk generally requires greater risk mitigation measures. What electronic systems are needed? What level of security and privacy needs to be in the system design? For example, if a system breach revealed non-sensitive floor plans we may not be concerned; if a breach revealed bank account numbers, passwords, and balances, we would be. While privacy policies and regulations might determine data classification and commensurate security and privacy controls, security technology enables data protection to the appropriate level.

Step 2: Select

What options are available to achieve the necessary controls for protecting against or mitigating the various identified privacy risks? Data of the same classification levels should be subject to similar sets of cybersecurity and privacy controls. Low risk data can be stored less rigorously, and presumably, less expensively; data of greater privacy risk may be subject to increased, and in some cases, more expensive controls.

From a privacy perspective, data can be protected through a combination of administrative (e.g., policies, procedures), technical, and physical controls. Some key privacy-centric security controls that are often considered include encryption, de-identification, anonymization, media sanitization, and geographic storage restrictions. Application of cybersecurity and privacy controls to data-at-rest versus data-in-motion versus data-in-use may also affect the selection of specific controls.

Step 3: Implement

Identify the required tasks, step by step, to implement your plan and selected controls. Document and save all system designs, architecture with data flow charts, and the data classification involved.

Step 4: Assess

An important and prevalent tool for assessing privacy risk and the effectiveness of controls is a Privacy Impact Assessment (PIA). Assessments should be conducted objectively to determine whether implementation has been completed to specification and working as intended. Any deficiencies are documented, and a corrective plan is put in place. Once corrected, another assessment should take place to ensure compliance and that the desired outcome regarding the protection of privacy is achieved. Assessors should be independent and also experienced in the data type and security systems involved.

Step 5: Authorize

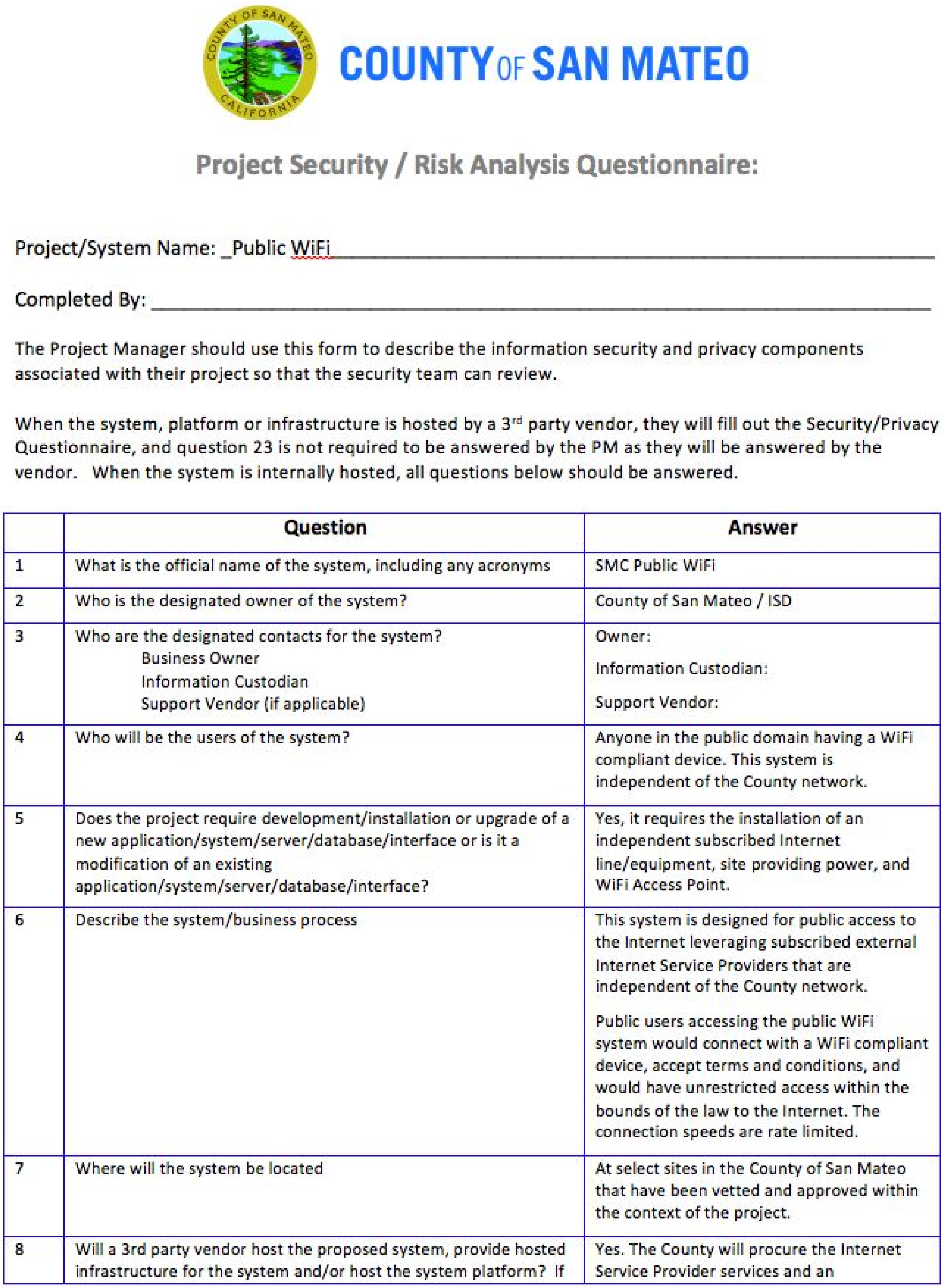
This step ensures accountability for a system that is designed to meet the required privacy needs. An informational package detailing all steps and outcomes is prepared, and includes responsible roles and their team names, as well as the risk assessments, privacy impact assessments, and strategy behind the decisions.

Step 6: Monitor

This step involves the ongoing evaluation of the privacy risk environment to identify changes as well as opportunities to achieve the desired risk posture. Inputs can include audits, incident debriefs, survey results, a changing threat landscape, and a changing regulatory environment. This monitoring can feed the refinement of privacy policies and procedures necessary to keep pace with evolving privacy risks.

Appendix B. Risk Assessment Example

The following risk assessment questionnaire (intended to accompany Appendix A: Use Case #3 - Risk Assessment in the County of San Mateo, California) provides a real-world example of how to assess and analyze risks that exist or are introduced by ongoing or new Smart City capabilities and projects. While the scope of this particular project and the associated risk assessment is limited, it should provide an example of a possible systematic approach to the risk assessment component of the overall cybersecurity and privacy risk management process. This can be adapted to fit the requirements of different organizations.



COUNTY OF SAN MATEO

Project Security / Risk Analysis Questionnaire:

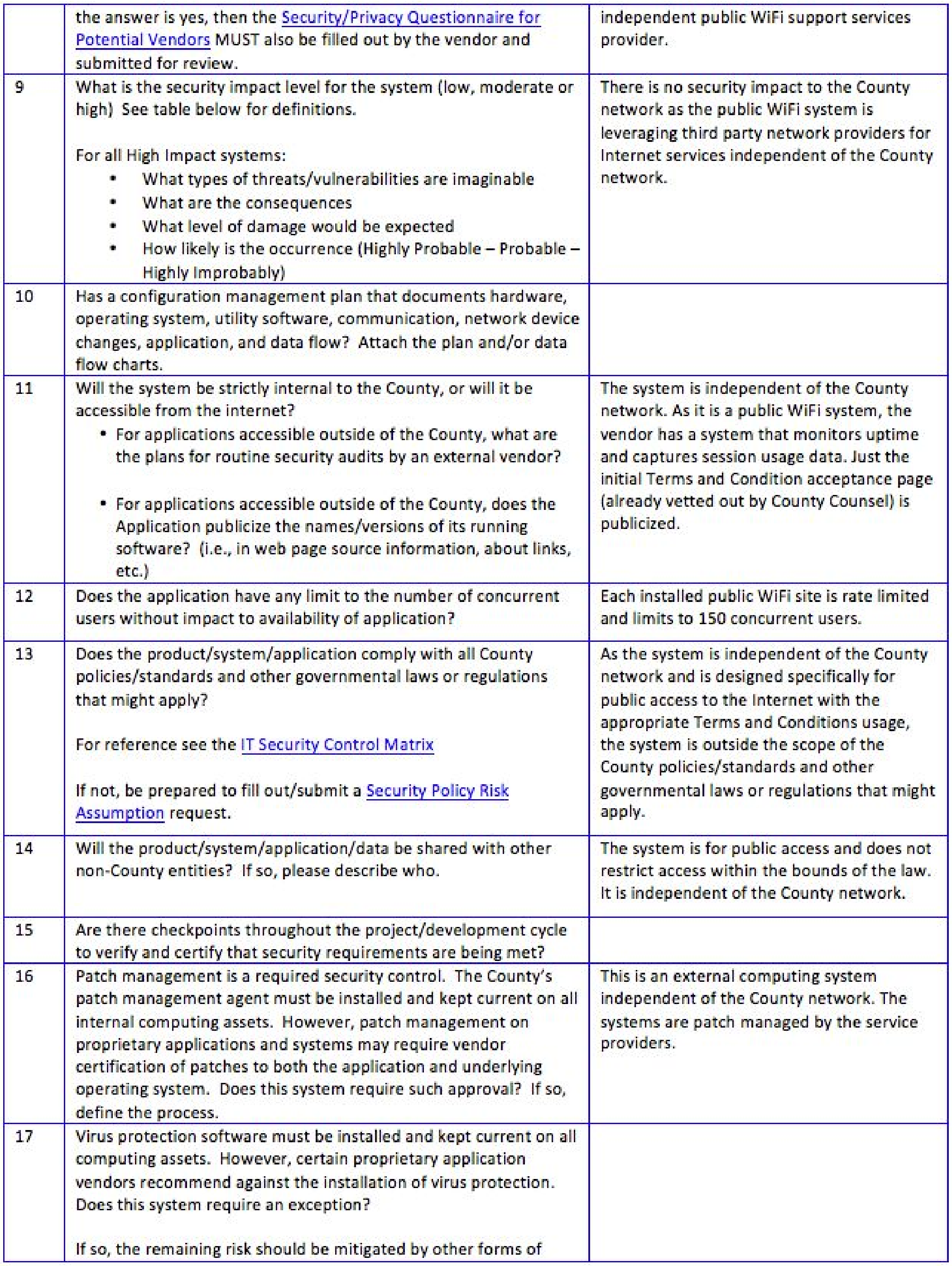
Project/System Name: _Public WiFi____

Completed By: ____

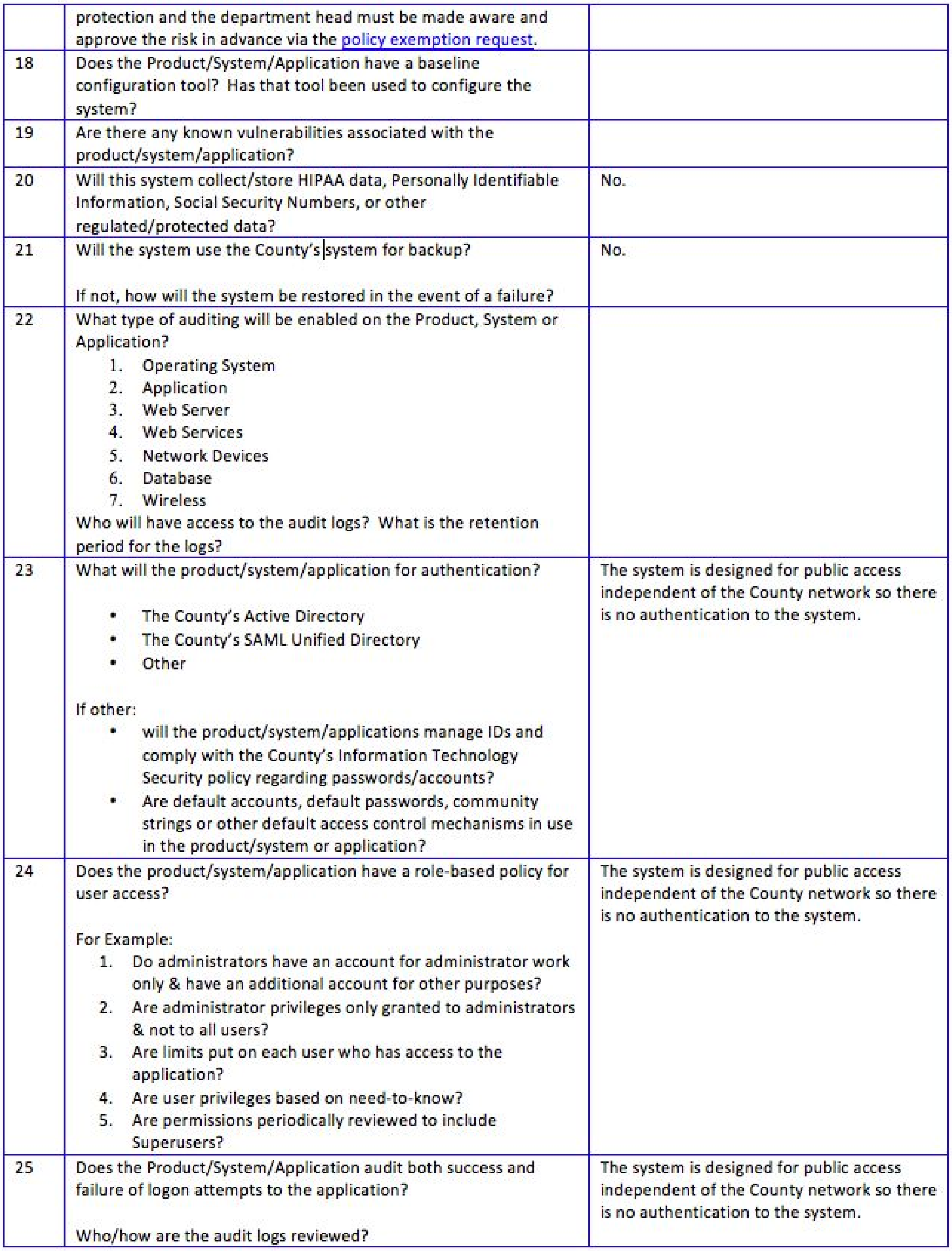
The Project Manager should use this form to describe the information security and privacy components associated with their project so that the security team can review.

When the system, platform or infrastructure is hosted by a 3rd party vendor, they will fill out the Security/Privacy Questionnaire, and question 23 is not required to be answered by the PM as they will be answered by the vendor. When the system is internally hosted, all questions below should be answered.

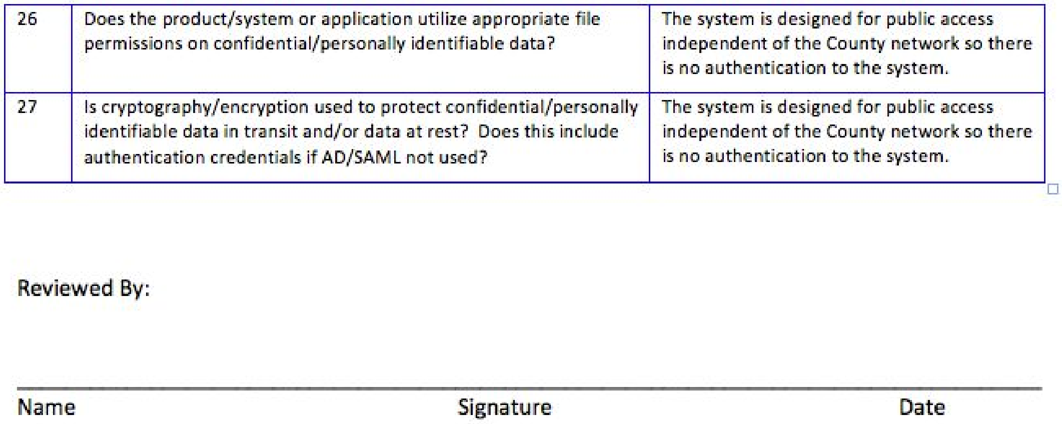
	Question	Answer
1	What is the official name of the system, including any acronyms	SMC Public WiFi
2	Who is the designated owner of the system?	County of San Mateo / ISD
3	Who are the designated contacts for the system? Business Owner Information Custodian Support Vendor (if applicable)	Owner: Information Custodian: Support Vendor:
4	Who will be the users of the system?	Anyone in the public domain having a WiFi compliant device. This system is independent of the County network.
5	Does the project require development/installation or upgrade of a new application/system/server/database/interface or is it a modification of an existing application/system/server/database/interface?	Yes, it requires the installation of an independent subscribed Internet line/equipment, site providing power, and WiFi Access Point.
6	Describe the system/business process	This system is designed for public access to the Internet leveraging subscribed external Internet Service Providers that are independent of the County network. Public users accessing the public WiFi system would connect with a WiFi compliant device, accept terms and conditions, and would have unrestricted access within the bounds of the law to the Internet. The connection speeds are rate limited.
7	Where will the system be located	At select sites in the County of San Mateo that have been vetted and approved within the context of the project.
8	Will a 3rd party vendor host the proposed system, provide hosted infrastructure for the system and/or host the system platform? If	Yes. The County will procure the Internet Service Provider services and an



	the answer is yes, then the Security/Privacy Questionnaire for Potential Vendors MUST also be filled out by the vendor and submitted for review.	independent public WiFi support services provider.
9	What is the security impact level for the system (low, moderate or high) See table below for definitions. For all High Impact systems: • What types of threats/vulnerabilities are imaginable • What are the consequences • What level of damage would be expected • How likely is the occurrence (Highly Probable – Probable – Highly Improbably)	There is no security impact to the County network as the public WiFi system is leveraging third party network providers for Internet services independent of the County network.
10	Has a configuration management plan that documents hardware, operating system, utility software, communication, network device changes, application, and data flow? Attach the plan and/or data flow charts.	
11	Will the system be strictly internal to the County, or will it be accessible from the internet? • For applications accessible outside of the County, what are the plans for routine security audits by an external vendor? • For applications accessible outside of the County, does the Application publicize the names/versions of its running software? (i.e., in web page source information, about links, etc.)	The system is independent of the County network. As it is a public WiFi system, the vendor has a system that monitors uptime and captures session usage data. Just the initial Terms and Condition acceptance page (already vetted out by County Counsel) is publicized.
12	Does the application have any limit to the number of concurrent users without impact to availability of application?	Each installed public WiFi site is rate limited and limits to 150 concurrent users.
13	Does the product/system/application comply with all County policies/standards and other governmental laws or regulations that might apply? For reference see the IT Security Control Matrix If not, be prepared to fill out/submit a Security Policy Risk Assumption request.	As the system is independent of the County network and is designed specifically for public access to the Internet with the appropriate Terms and Conditions usage, the system is outside the scope of the County policies/standards and other governmental laws or regulations that might apply.
14	Will the product/system/application/data be shared with other non-County entities? If so, please describe who.	The system is for public access and does not restrict access within the bounds of the law. It is independent of the County network.
15	Are there checkpoints throughout the project/development cycle to verify and certify that security requirements are being met?	
16	Patch management is a required security control. The County's patch management agent must be installed and kept current on all internal computing assets. However, patch management on proprietary applications and systems may require vendor certification of patches to both the application and underlying operating system. Does this system require such approval? If so, define the process.	This is an external computing system independent of the County network. The systems are patch managed by the service providers.
17	Virus protection software must be installed and kept current on all computing assets. However, certain proprietary application vendors recommend against the installation of virus protection. Does this system require an exception? If so, the remaining risk should be mitigated by other forms of	



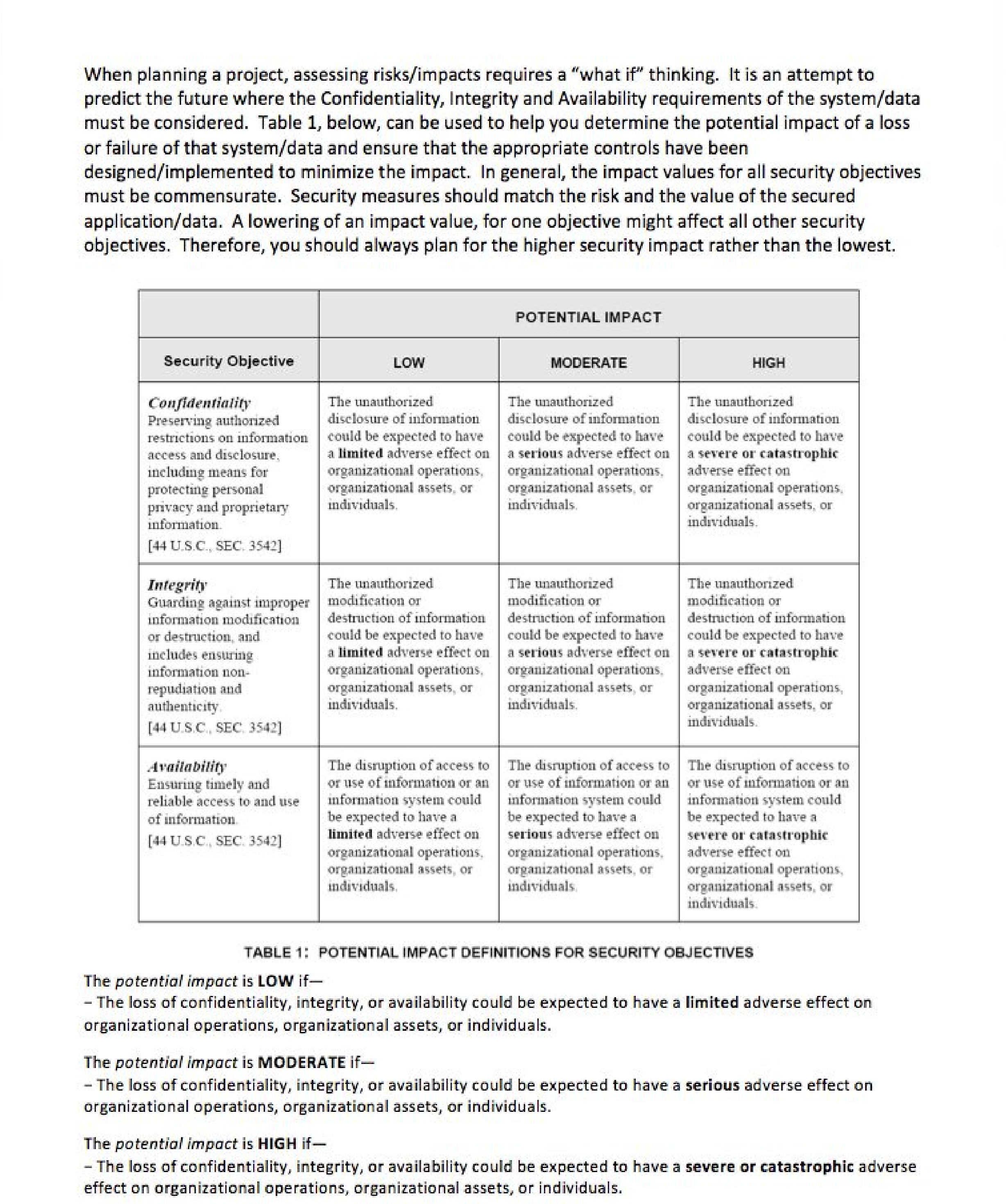
	protection and the department head must be made aware and approve the risk in advance via the policy exemption request.	
18	Does the Product/System/Application have a baseline configuration tool? Has that tool been used to configure the system?	
19	Are there any known vulnerabilities associated with the product/system/application?	
20	Will this system collect/store HIPAA data, Personally Identifiable Information, Social Security Numbers, or other regulated/protected data?	No.
21	Will the system use the County's system for backup? If not, how will the system be restored in the event of a failure?	No.
22	What type of auditing will be enabled on the Product, System or Application? 1. Operating System 2. Application 3. Web Server 4. Web Services 5. Network Devices 6. Database 7. Wireless Who will have access to the audit logs? What is the retention period for the logs?	
23	What will the product/system/application for authentication? • The County's Active Directory • The County's SAML Unified Directory • Other If other: • will the product/system/applications manage IDs and comply with the County's Information Technology Security policy regarding passwords/accounts? • Are default accounts, default passwords, community strings or other default access control mechanisms in use in the product/system or application?	The system is designed for public access independent of the County network so there is no authentication to the system.
24	Does the product/system/application have a role-based policy for user access? For Example: 1. Do administrators have an account for administrator work only & have an additional account for other purposes? 2. Are administrator privileges only granted to administrators & not to all users? 3. Are limits put on each user who has access to the application? 4. Are user privileges based on need-to-know? 5. Are permissions periodically reviewed to include Superusers?	The system is designed for public access independent of the County network so there is no authentication to the system.
25	Does the Product/System/Application audit both success and failure of logon attempts to the application? Who/how are the audit logs reviewed?	The system is designed for public access independent of the County network so there is no authentication to the system.



26	Does the product/system or application utilize appropriate file permissions on confidential/personally identifiable data?	The system is designed for public access independent of the County network so there is no authentication to the system.
27	Is cryptography/encryption used to protect confidential/personally identifiable data in transit and/or data at rest? Does this include authentication credentials if AD/SAML not used?	The system is designed for public access independent of the County network so there is no authentication to the system.

Reviewed By:

Name Signature Date



When planning a project, assessing risks/impacts requires a "what if" thinking. It is an attempt to predict the future where the Confidentiality, Integrity and Availability requirements of the system/data must be considered. Table 1, below, can be used to help you determine the potential impact of a loss or failure of that system/data and ensure that the appropriate controls have been designed/implemented to minimize the impact. In general, the impact values for all security objectives must be commensurate. Security measures should match the risk and the value of the secured application/data. A lowering of an impact value, for one objective might affect all other security objectives. Therefore, you should always plan for the higher security impact rather than the lowest.

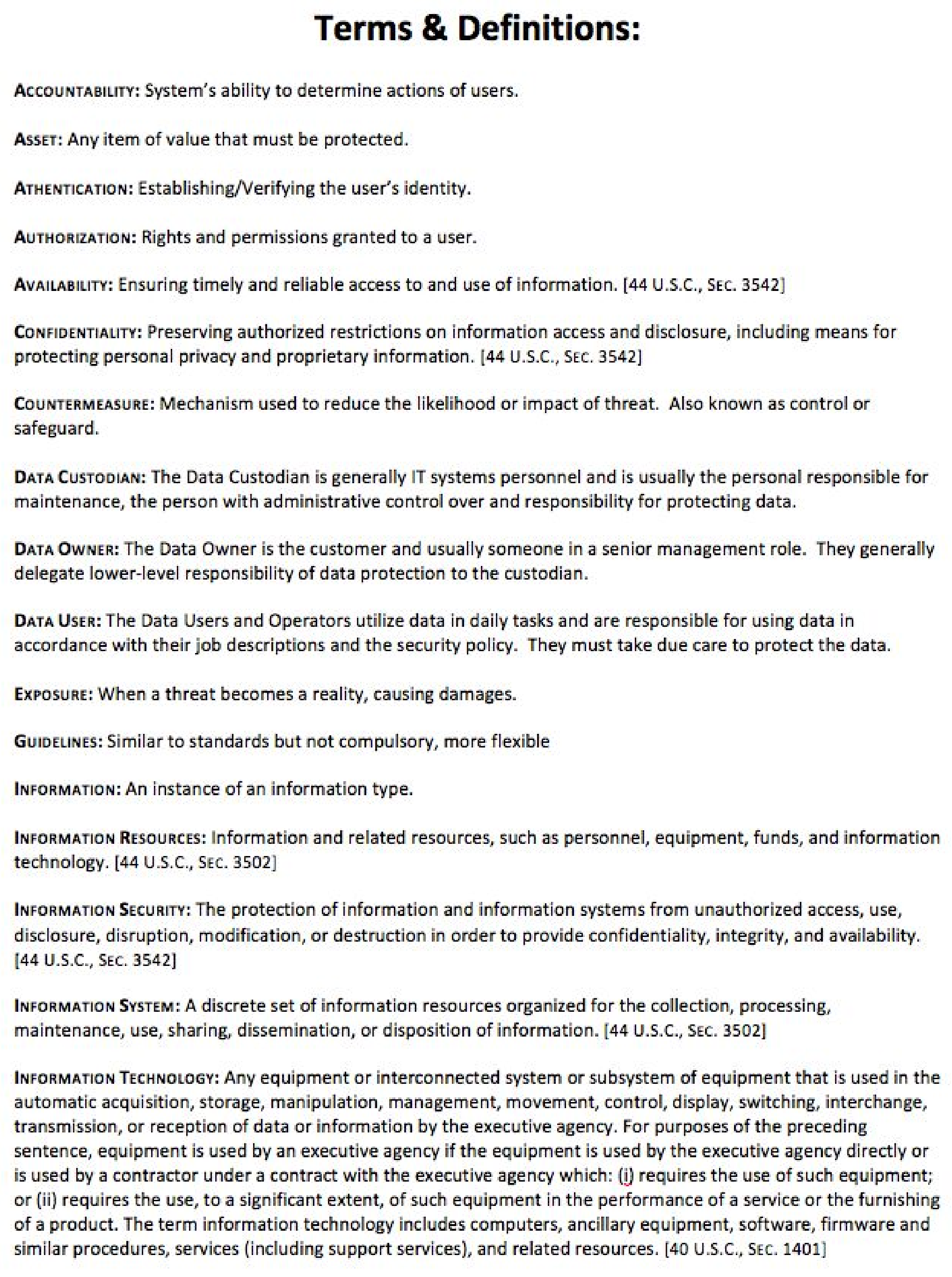
	POTENTIAL IMPACT		
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

The *potential impact* is **LOW** if—
– The loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

The *potential impact* is **MODERATE** if—
– The loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

The *potential impact* is **HIGH** if—
– The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.



Terms & Definitions:

ACCOUNTABILITY: System's ability to determine actions of users.

ASSET: Any item of value that must be protected.

ATHENTICATION: Establishing/Verifying the user's identity.

AUTHORIZATION: Rights and permissions granted to a user.

AVAILABILITY: Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

CONFIDENTIALITY: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

COUNTERMEASURE: Mechanism used to reduce the likelihood or impact of threat. Also known as control or safeguard.

DATA CUSTODIAN: The Data Custodian is generally IT systems personnel and is usually the personal responsible for maintenance, the person with administrative control over and responsibility for protecting data.

DATA OWNER: The Data Owner is the customer and usually someone in a senior management role. They generally delegate lower-level responsibility of data protection to the custodian.

DATA USER: The Data Users and Operators utilize data in daily tasks and are responsible for using data in accordance with their job descriptions and the security policy. They must take due care to protect the data.

EXPOSURE: When a threat becomes a reality, causing damages.

GUIDELINES: Similar to standards but not compulsory, more flexible

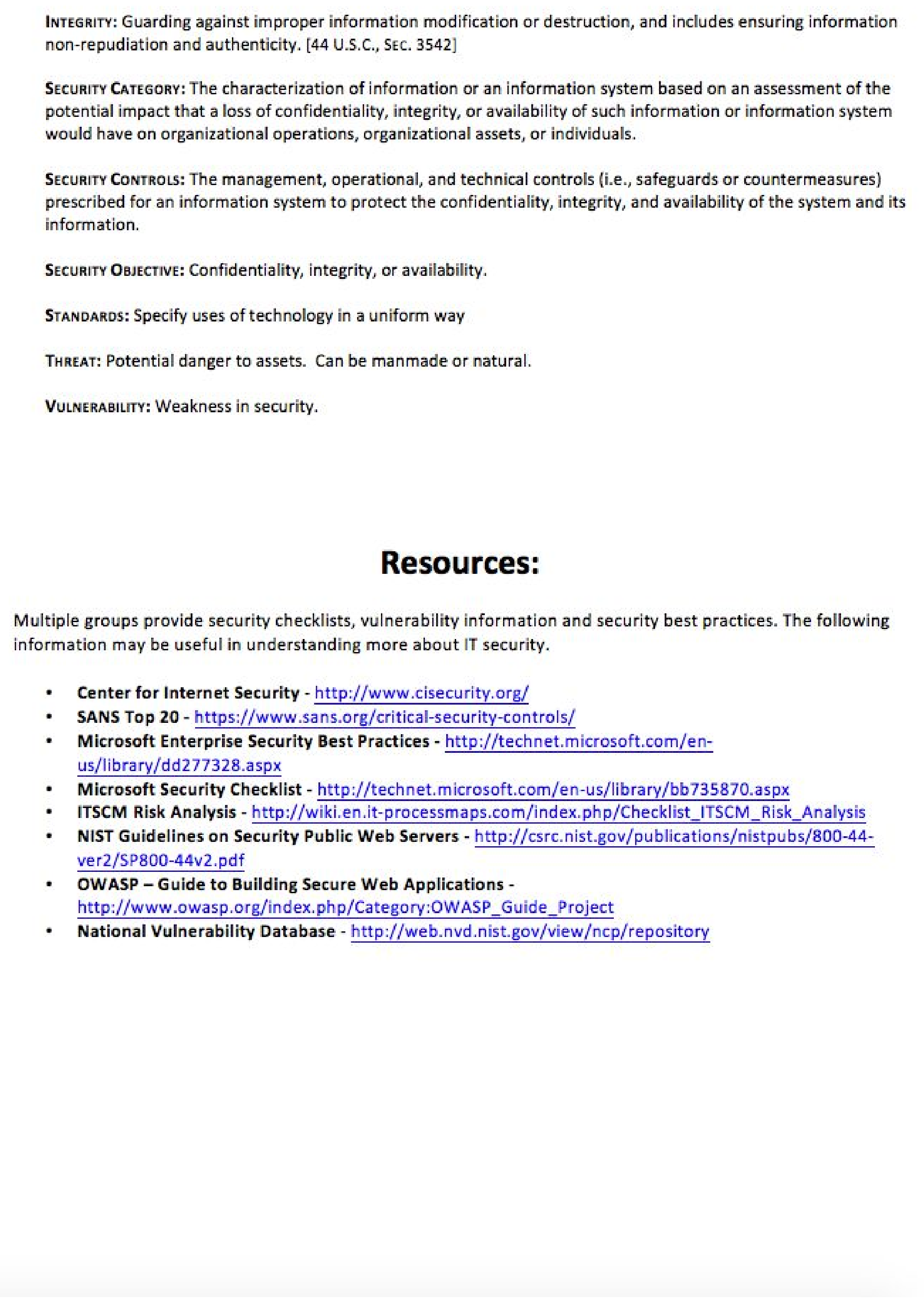
INFORMATION: An instance of an information type.

INFORMATION RESOURCES: Information and related resources, such as personnel, equipment, funds, and information technology. [44 U.S.C., SEC. 3502]

INFORMATION SECURITY: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

INFORMATION SYSTEM: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [44 U.S.C., SEC. 3502]

INFORMATION TECHNOLOGY: Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. [40 U.S.C., SEC. 1401]



Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., Sec. 3542]

Security Category: The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Objective: Confidentiality, integrity, or availability.

Standards: Specify uses of technology in a uniform way

Threat: Potential danger to assets. Can be manmade or natural.

Vulnerability: Weakness in security.

Resources:

Multiple groups provide security checklists, vulnerability information and security best practices. The following information may be useful in understanding more about IT security.

- **Center for Internet Security** - http://www.cisecurity.org/
- **SANS Top 20** - https://www.sans.org/critical-security-controls/
- **Microsoft Enterprise Security Best Practices** - http://technet.microsoft.com/en-us/library/dd277328.aspx
- **Microsoft Security Checklist** - http://technet.microsoft.com/en-us/library/bb735870.aspx
- **ITSCM Risk Analysis** - http://wiki.en.it-processmaps.com/index.php/Checklist_ITSCM_Risk_Analysis
- **NIST Guidelines on Security Public Web Servers** - http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
- **OWASP – Guide to Building Secure Web Applications** - http://www.owasp.org/index.php/Category:OWASP_Guide_Project
- **National Vulnerability Database** - http://web.nvd.nist.gov/view/ncp/repository

Appendix C. CPAC “Top X” Questions for a Trustworthy Smart City

This “Top X” discussion list summarizes key questions to be considered in planning and implementing cybersecurity and privacy for a “Trustworthy Smart City.” It is provided as a complement to the in-depth GCTC-SC3 Cybersecurity and Privacy Advisory Committee (CPAC) Guidebook. The CPAC team has intentionally modeled this discussion list on other listings, such as the Center for Internet Security’s (CIS) Critical Security Controls[40]. This list can be thought of as a “discussion tool” to be used in parallel with or in advance of the CPAC Guidebook, identifying key areas to consider in risk management for a “Trustworthy Smart City” - an increasingly significant challenge facing cities and communities around the globe.

The “X” in the title of this list has been selected to emphasize that this list is intended to be flexible and can evolve, as necessary. In addition, this list, or portions of the list, can act as the foundation or starting point for other cybersecurity and privacy risk management tools.[41]

1. Do you have an **employee, team, organization, or program** that is responsible for managing cybersecurity and privacy risk in your Smart City environment? Is a **management structure** that aligns leadership and mission owners across organizational and jurisdictional boundaries in place to sustain these efforts and support accountability?

2. Do you have an overall **cybersecurity and privacy risk management strategy or approach** that governs the operations and risk posture of your Smart City environment to ensure the confidentiality, integrity, and availability of services?

3. Have **strong policies**, including related physical security policies, been developed, communicated, and enforced to execute your risk management strategy or approach?

4. Do you have an **accurate, real-time inventory** of all authorized and unauthorized hardware and software assets and their configurations in your Smart City environment?

5. Do you **manage and authenticate** identities, credentials, certificates, privileges, and behaviors of users, devices, and services in your Smart City environment?

[40] “CIS Controls,” *Center for Internet Security*. https://www.cisecurity.org/controls/
[41] See, for example, Appendix A, Use Case #2: Risk Assessment and Prioritization in the Smart City Cyber Resilience Planning Process

6. Do you have an understanding of **normal behavior** in your Smart City environment and are you actively **monitoring** for unauthorized usage, intrusions, suspicious behaviors, etc.?

7. Do you have processes and capabilities, including a staging environment, in place for **patch management** across the Smart City environment?

8. Have you implemented measures to ensure the **protection and privacy of data** created, collected, and used - including data-at-rest, data-in-use, and data-in-motion - within the Smart City environment?

9. Do you have a **testing and assessment process** - including software assurance, penetration testing, and vulnerability assessments - for the sustained evaluation of software, hardware, and services?

10. Do you have a strategy for **independent validation or auditing** of the efficacy of cybersecurity and privacy controls associated with both internal and external processes, products, and services and their contribution to the overall risk posture?

11. Have cyber and cyber-physical **incident response and recovery plans** - including **breach notification** policies and processes - been developed? Have these plans been coordinated and exercised with relevant government agencies, first responder organizations, quasi-governmental entities, private sector partners, and the general public?

12. Have you fostered a security culture by instituting an **education, training, awareness, and outreach** program for employees, partners, and customers?

13. Do your **procurement and acquisition** processes and documentation explicitly address cybersecurity and privacy risk management requirements, including liability?

14. Do you have a strategy for managing cybersecurity and privacy risks related to **supply chain** and system, vendor, and jurisdictional interdependencies?

15. Have you collaborated with government officials, including law enforcement, to develop a strategy and approach for cybercrime **prevention and deterrence**?

16. Have you developed relationships within your organization and with external collaborators, partners, and peers to facilitate **information sharing** related to cybersecurity and privacy threats, trends, and best practices?

Appendix D. References

"About GCTC," *NIST*. https://pages.nist.gov/GCTC/about/the-gctc/.

Barrett, Brian. "DOJ Indicts Hackers for Ransomware that Crippled Atlanta," *Wired*. November 28, 2018. https://www.wired.com/story/doj-indicts-hackers-samsam-ransomware/.

Calvert, Scott and Jon Kamp. "More U.S. Cities Brace for 'Inevitable' Hackers," *The Wall Street Journal*. September 4, 2018. https://www.wsj.com/articles/more-cities-brace-for-inevitable-cyberattack-1536053401.

Choudhury, Amit Roy. "SingHealth Breach a Wake-Up Call for Smart Nation Singapore," *GovInsider*. August 14, 2018. https://govinsider.asia/innovation/singhealth-breach-wake-call-smart-nation-singapore/.

"CIS Controls," *Center for Internet Security*. https://www.cisecurity.org/controls/.

Deere, Stephen. "Atlanta's Cyber Attack Could Cost Taxpayers $17 Million," *The Atlanta Journal-Constitution*. August 1, 2018. https://www.ajc.com/news/confidential-report-atlanta-cyber-attack-could-hit-million/GAljmndAF3EQdVWIMcXS0K/.

Greer, Chris and Dr. Douglas Maughan. "Smart and Secure Cities and Communities Challenge." August 29, 2017.

Higgins, Kelly Jackson. "Malware Built to Hack Building Automation Systems," *DarkReading*. January 16, 2019. https://www.darkreading.com/vulnerabilities---threats/malware-built-to-hack-building-automation-systems/d/d-id/1333671.

Kearney, Laila. "Atlanta Officials Reveal Worsening Effects of Cyber Attack," *Reuters*. June 6, 2018. https://www.reuters.com/article/us-usa-cyber-atlanta-budget/atlanta-officials-reveal-worsening-effects-of-cyber-attack-idUSKCN1J231M?feedType=RSS&feedName=technologyNews.

Kolleda, Joshua; Dominie Garcia; and Tyler Poling. *Connected Vehicle Pilot Deployment Program Phase I: Security Management Operational Concept - Tampa Hillsborough Expressway Authority (THEA)*, May 2016.

Multi-State Information Sharing and Analysis Center (MS-ISAC), *NCSR General User Guide*.

National Institute of Standards and Technology, Engineering Laboratory, Smart Grid and Cyber-Physical Systems Program Office, *Cybersecurity for Smart Cities: Phase 2 Report*, June 2019.

National Institute of Standards and Technology, *FIPS 199: Standards for Security Categorization of Federal Information and Information Systems*.

National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1.*

National Institute of Standards and Technology, *NIST Cybersecurity White Paper: Internet of Things (IoT) Trust Concerns*.

National Institute of Standards and Technology, *NIST SP 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations*.

National Institute of Standards and Technology, *NISTIR 8196 (Draft): Security Analysis of First Responder Mobile and Wearable Devices*.

National Institute of Standards and Technology, *NISTIR 8228 (Draft): Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks*.

National Institute of Standards and Technology, *NIST Special Publication 1190GB-5: Guide Brief 5 - Assessing Energy System Dependencies.*

National Institute of Standards and Technology, *NIST Special Publication 800-37 Revision 2: Risk Management Framework for Information Systems and Organizations.*

“Nationwide Cybersecurity Review,” *Center for Internet Security*. https://www.cisecurity.org/ms-isac/services/ncsr/.

“Risk Management Framework (RMF) Overview,” *NIST*. February 12, 2019. https://csrc.nist.gov/projects/risk-management/risk-management-framework-(RMF)-Overview.

“Risk Management Framework (RMF) - Prepare,” *NIST*. February 12, 2019. https://csrc.nist.gov/Projects/Risk-Management/Risk-Management-Framework-Quick-Start-Guides/Step-0-Prepare.

"Risk Management Framework (RMF) - Step 1: Categorize," *NIST*. February 12, 2019. https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/step-1-categorize.

"Risk Management Framework (RMF) - Step 2: Select," *NIST*. February 12, 2019. https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/step-2-select.

"Risk Management Framework (RMF) - Step 6: Monitor," *NIST*. February 12, 2019. https://csrc.nist.gov/projects/risk-management/risk-management-framework-quick-start-guides/risk-management-framework-(rmf)-step-6-monitor.

Romo, Vanessa. "Georgia Charges Iranians in Ransomware Attack on Atlanta," *NPR*. December 5, 2018. https://www.npr.org/2018/12/05/673958138/georgia-charges-iranians-in-ransomware-attack-on-atlanta.

Tampa Hillsborough Expressway Authority, "THEA Connected Vehicle Pilot - Fact Sheet."

Thomson, Iain. "Guilty: The Romanian Ransomware Mastermind who Infected Trump Inauguration CCTV Cams," *The Register*. September 21, 2018. https://www.theregister.co.uk/2018/09/21/cctv_ransomware_trump_washington_dc/.