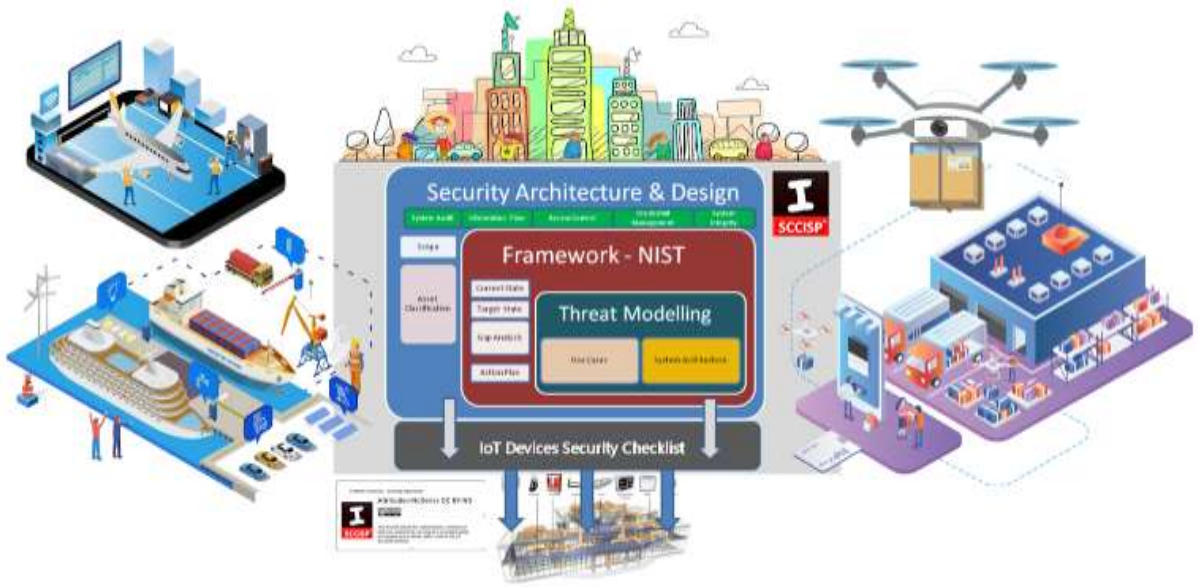
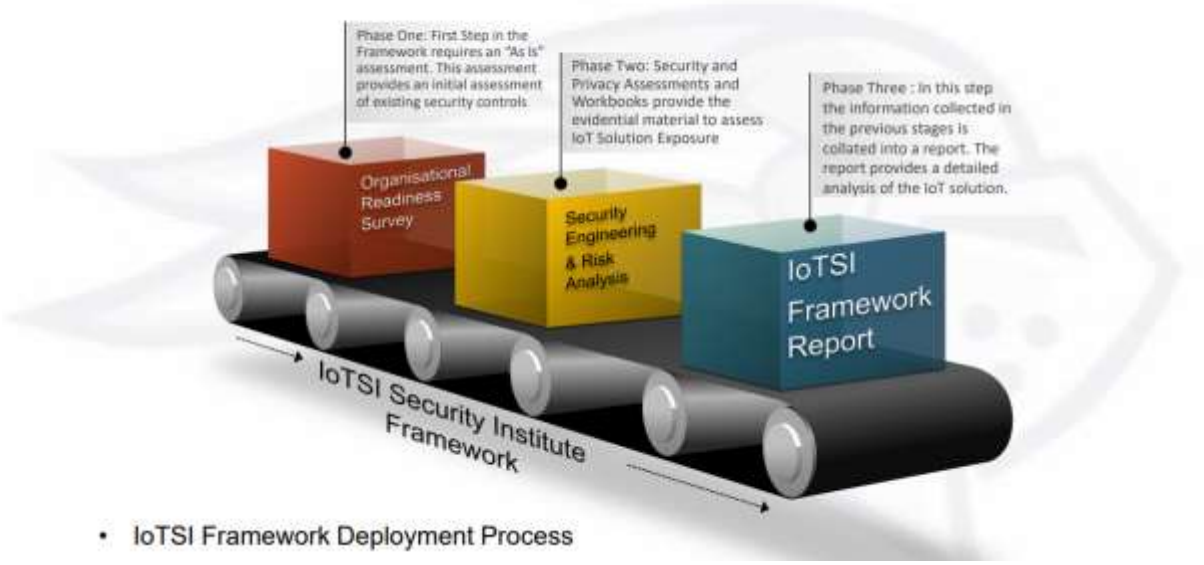
IoT Security Institute

The IoTSI SCCI Framework



Adopting a Synergistic Collaboration

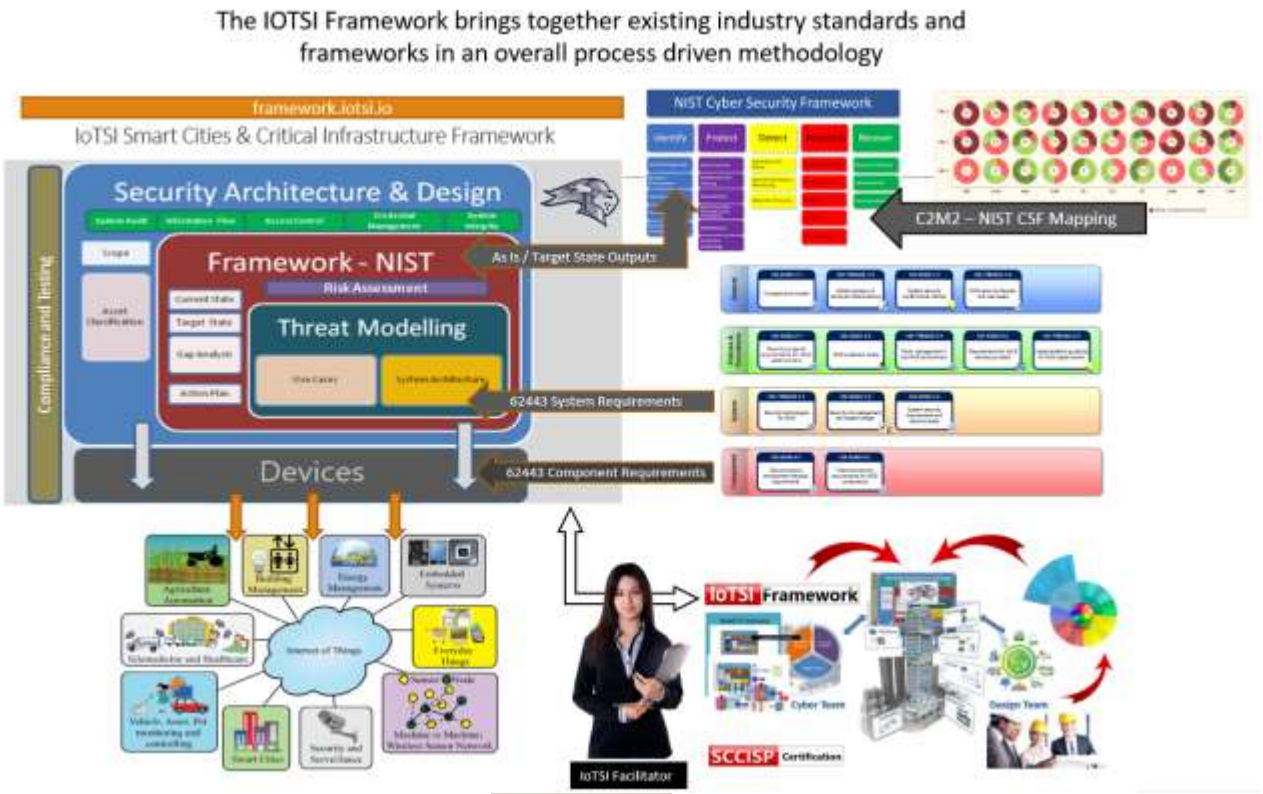
With the development of smart technologies, and the convergence of IT / OT environments the ability to manage and leverage diverse cyber security frameworks, standards, and procedures can be a challenging prospect.



Often numerous market sectors align to a particular set of cyber security standards. This can be due to a mandated requirement, or an industry preferred set of requirements that essentially underpin their responsibilities and obligations. In addition, many organizations have invested heavily in particular cyber security standard and do not have the skilled resources or inclination to shift to another set of GRC documentation. Aside from the motivation to select one cyber security standard over another, one aspect is certain; cyber security standards do not come in a one size fits all format. Often standards have specific qualities, objectives and resulting outcomes.It would be unreasonable to expect a single standard to have a catch all option. For example, objective driven versus technical assessment standards have a completely different set of objectives. They are intend to be used in conjunction to provide an overarching holistic view of cyber security capabilities and desired outcomes.

Furthermore, given the complexity of smart technology and infrastructure it would be a wasted opportunity to minimize an organization's options and its ability to integrate an array of applicable standards as part of their overall cyber security management program. Given the nature of IoT and IIoT security challenges and the convergence of IT and OT technologies most cyber professionals would highly recommend the ability to utilize a broad set of GRC standards when considered applicable.

A Consultative and Integrated Approach – Ensuring Safe and Secure Smart Eco-Systems



Given the collaborative and converging nature of smart eco-systems The IoTSI Smart Cities and Critical Infrastructure Framework provides a consultative process driven methodology that allows for the overarching mapping, utilization and integration of a diverse set of cyber standards within the overall assessment process flow of the IoTSI Framework.

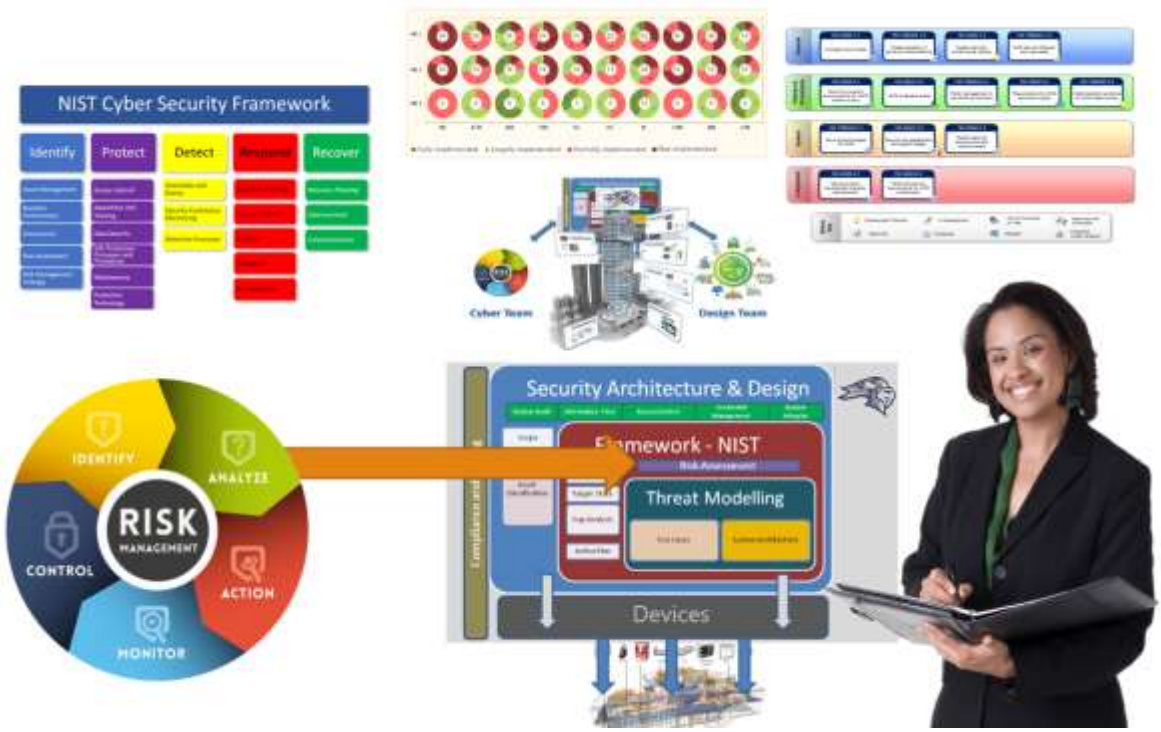
The IoTSI uses a component-based model that allows for systematic processing and data analysis. Leveraging a number of industry standards The IoTSI brings together processes and methodologies that can augment and underpin the IoTSI own methodology. The IoTSI strategy to utilize certain standards and to collaborate with others, allows for a familiarity of purpose and immediate understanding of intent.

Furthermore, this flexibility allows for the inclusion of industry specific, or legal and regulatory requirements, to be included within the overall framework delivery and assessment model. These “industry or regulatory additions” can be used in conjunction with the Framework’s GRC documentation and processes or can be mapped and integrated into the IoTSI Framework Assessment and Deployment Process.

Figure 8 - Working with other Standards

The IoTSI Facilitator

Clearly when working across a range of standards, process flows and assessment activities is essential a facilitation methodology be utilized. The IoTSI Framework provides a consultant's approach to the assigned tasks and deliverables.



The IoTSI Framework is based on a process and deployment driven methodology. In order to provide detailed security by design services across a technology life cycle the IoTSI framework relies on a number of key documents.

The IoTSI Framework documentation process consist of the following key documents.

- IoTSI Smart Cities & CI Framework Overview
- IoTSI Framework Facilitation Guide
- Organisational Readiness Survey
- Privacy Impact Assessment and Control Guidelines
- Control Documents (risk assessment, workflows, etc.)
- IoT Devices Checklist
- Building Information Modelling
- Reference Architecture

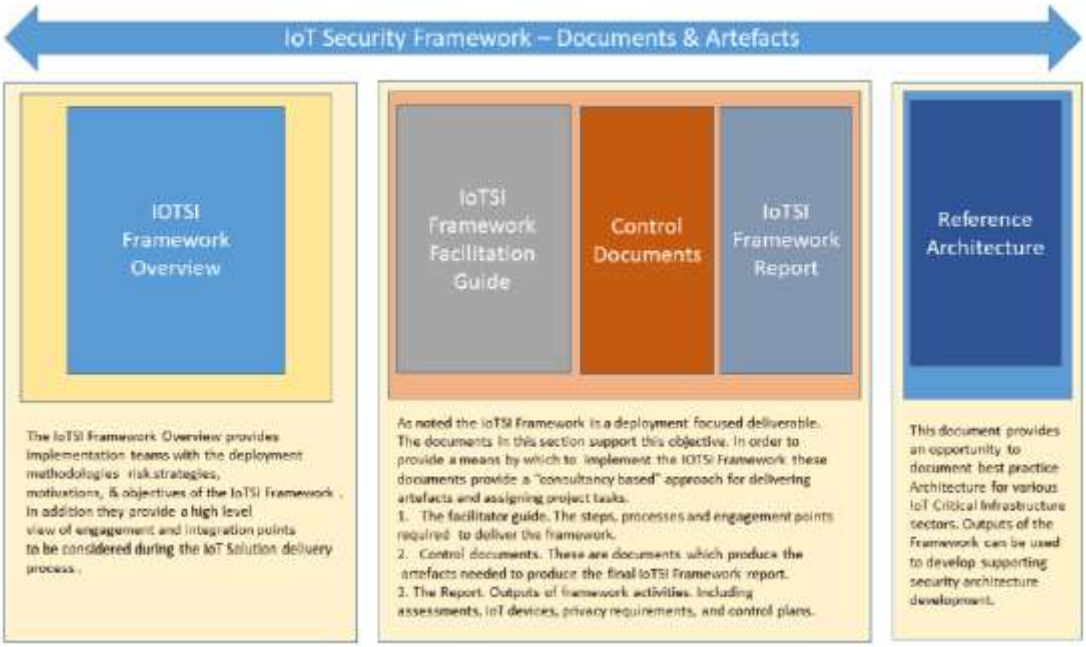


Figure 6 - IoTSI Documentation Explained

The following illustration represents the documentation as a sequence flow. This is an example and maybe approached in an alternate manner or different sequential order depending upon scheduling requirements and/or resourcing restraints. Where large teams are deployed, the IoTSI Facilitator can assign tasks in accordance with project management team preferences or current budget allocation. However, all required activities must be completed resulting in a definitive IoTSI Final report. In some case, not all artefacts are required. This may be due to the nature or type of implementation. For instance, Building Information Modelling may not be required for a small-scale in house project. However, any omission must be well founded and not attempt to undermine the overall objective of the IoTSI framework. Cyber professionals must ensure any non -inclusions are well understood and accepted by relevant stakeholders. The IoTSI acknowledges the complexity of IoT – IIoT solutions require flexibility in approach and must be scalable without compromising security best practices and standards. It is the base build approach that enables to IoTSI Framework to be adaptable to an array of Smart city and Critical Infrastructure scenarios.

Facilitation Guide

The Facilitation Guide provides the process by which the IoTSI Framework methodology is applied to an IoT Solution Cyber Assessment.

The Guide follows a professional service engagement model. Organisation can appoint their own internal IoTSI consultant to manage the facilitation process or enlist the services of an external IoTSI facilitator. There may be occasions where not all artefacts require completion. For instance, in the absence of Building Information Modelling, the relevant artefacts would not be processed. These requirements would be determined during initial team member appointments; as part of initial IoTSI facilitator led kick-off meetings

IoTSI Framework – Working with the Smart City Mandala

In order to understand and remediate the cyber and privacy challenges cyber industry professionals require an understanding of what a smart city really is; its purpose, how it functions, and perhaps more importantly how it interacts. From a technical perspective, smart cities could be described as urban areas that use different types of electronic data collection sensors to supply information, which is used to manage assets and resources efficiently.

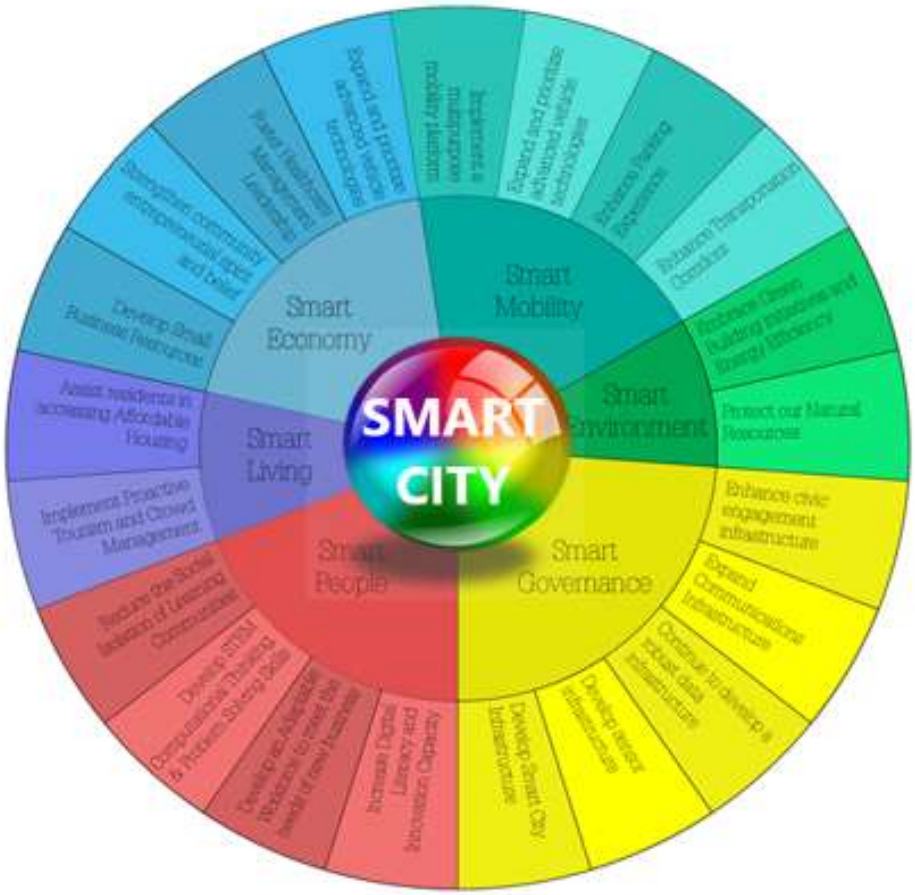
This includes data collected from citizens, devices, and assets that is processed and analyzed to monitor and manage traffic, waste management, law enforcement, information systems, schools, libraries, hospitals, and other community services.The IoT Security Institute would recommend a broader definition, as provided at the Smart Cities Workshop (2009). It defines a 'smart' city as '… a city that makes conscious effort to innovatively employ ICTs in support of a more inclusive, diverse and sustainable urban environment'

To protect this smart technology innovation it is necessary to understand the foundation upon which smart cities are built; taking into account the guiding principles and strategies that underpin their objectives.

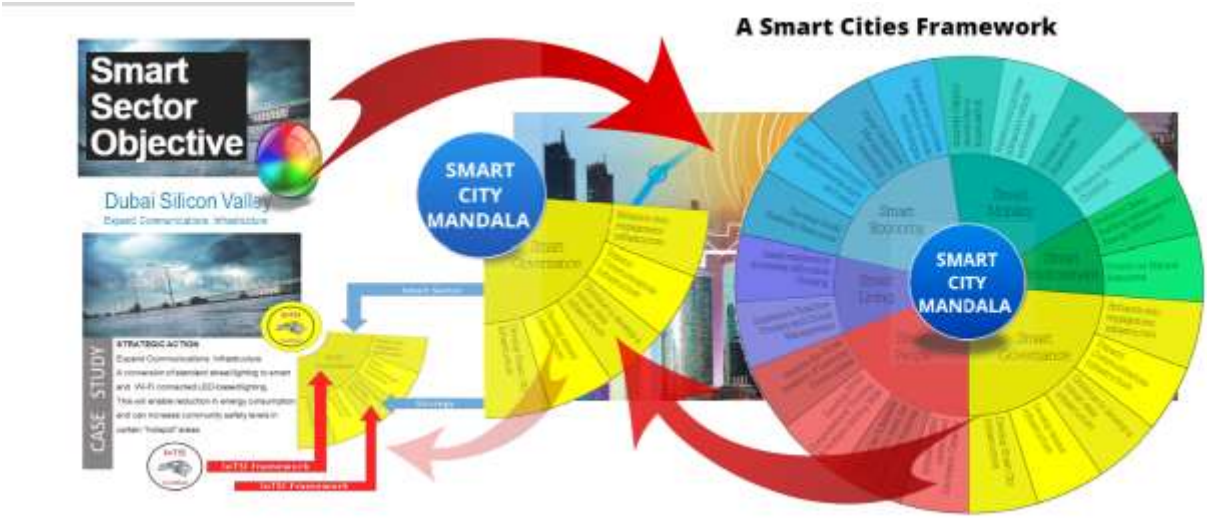
Key to any Smart City deployment are the six sectors to a smart city strategy. These include:

- Smart Governance
- Smart Environment
- Smart Living
- Smart Mobility
- Smart People
- Smart Economy

The following mandala illustrates the six sectors and their corresponding subsets. These subsets identify the smart city deliverable necessary to enable and maintain a smart city environment.



Each of the six of sectors has a unique objective that underpins a city's overall smart cities strategy. Each city may have a different point of departure or long-term objective; however, each is looking to implement a smart roadmap that is in the best interest of their communities, Critical to this objective is the "security and privacy by design" analysis of each of these objectives. The IoT Security Institute took this six-sector approach and developed a cyber and privacy framework that incorporated the long-term development of Smart City's strategies whilst providing a cyber and privacy foundation for the associated technologies and processes required to meet these objectives. We at the IoTSI believe this unique approach has allowed for a more flexible and scalable approach not necessarily available in more traditional cyber management offerings. The IoTSI framework allows for early integration into smart technology IoT/IIoT initiatives. Furthermore, the framework has developed with the ability to align to diverse workflows; as seen in the design engineering and construction fields. The IoTSI Framework extends beyond traditional IT delivery models, encompassing a myriad of requirements and models that are integral components of a smart cities or critical infrastructure eco-system.



The future of smart urban planning will usher in an era of creativity, functionality and convenience resulting in unprecedented opportunities. Key to this successful building evolution will be the assurance that private, public and corporate cyber safety is maintained and protected to community expectations.

The complete IoTSI Smart Cities and Critical Infrastructure Framework documentation library is available at framework.iotsi.io

Author: Alan Mihalic, SCCISP