IoT Security Foundation

IOT CYBERSECURITY FOR FACILITIES PROFESSIONALS

IN THE SMART BUILT ENVIRONMENT

Release 1.0, March 2023

Triple A Rated

Accessible
Authoritative
Actionable

Notices, Disclaimer, Terms of Use, Copyright and Trade Marks and Licensing

Notices

Documents published by the IoT Security Foundation ("IoTSF") are subject to regular review and may be updated or subject to change at any time. The current status of IoTSF publications, including this document, can be seen on the public website at: https://iotsecurityfoundation.org/

Terms of Use

The role of IoTSF in providing this document is to promote contemporary best practices in IoT security for the benefit of society. In providing this document, IoTSF does not certify, endorse or affirm any third parties based upon using content provided by those third parties and does not verify any declarations made by users.

In making this document available, no provision of service is constituted or rendered by IoTSF to any recipient or user of this document or to any third party.

Disclaimer

IoT security (like any aspect of information security) is not absolute and can never be guaranteed. New vulnerabilities are constantly being discovered, which means there is a need to monitor, maintain and review both policy and practice as they relate to specific use cases and operating environments on a regular basis.

IoTSF is a non-profit organisation which publishes IoT security best practice guidance materials. Materials published by IoTSF include contributions from security practitioners, researchers, industrially experienced staff and other relevant sources from IoTSF's membership and partners. IoTSF has a multi-stage process designed to develop contemporary best practice with a quality assurance peer review prior to publication. While IoTSF provides information in good faith and makes every effort to supply correct, current and high quality guidance, IoTSF provides all materials (including this document) solely on an 'as is' basis without any express or implied warranties, undertakings or guarantees.

The contents of this document are provided for general information only and do not purport to be comprehensive. No representation, warranty, assurance or undertaking (whether express or implied) is or will be made, and no responsibility or liability to a recipient or user of this document or to any third party is or will be accepted by IoTSF or any of its members (or any of their respective officers, employees or agents), in connection with this document or any use of it, including in relation to the adequacy, accuracy, completeness or timeliness of this document or its contents. Any such responsibility or liability is expressly disclaimed.

Nothing in this document excludes any liability for: (i) death or personal injury caused by negligence; or (ii) fraud or fraudulent misrepresentation.

By accepting or using this document, the recipient or user agrees to be bound by this disclaimer. This disclaimer is governed by English law.

Copyright, Trade Marks and Licensing

Acknowledgements

We wish to acknowledge significant contributions from IoTSF members to this Best Practice Guide:

Co-Chairs of the IoT Security Foundation Smart Built Environment Working Group:

Sarb Sembhi, Virtually Informed Ltd

James Willison, IoTSF

Facilities Management Stakeholder Sub-group

Stakeholder Sub-group Lead:

Dave Cooke, IWFM

The IoTSF has worked in partnership with the Institute of Workplace and Facilities Management (IWFM) to produce this guide. IWFM is the body for workplace and facilities professionals. It exists to promote excellence among a worldwide membership community and to demonstrate the value and contribution of FM more widely. Its representative has chaired the working group which produced this guide. This knowledge of the industry coupled with the technical specialism of the IoTSF has proved a powerful alliance.

Editors:

Richard Marshall, Xitex Limited

John Moor, IoTSF

Sarb Sembhi, Virtually Informed Ltd

Jason Shaw, AECOM

James Willison, IoTSF

Contributors:

Emma Boakes, University of Portsmouth

Dave Cooke, IWFM

Nikdokht Ghadiminia, University of East London

Vitor Jesus, Aston University

John Moor, IoTSF

Nick Morgan, Derwent London

Rajeev Rege, Alumnus Software Limited

Sarb Sembhi, Virtually Informed Ltd

Jason Shaw, AECOM

James Willison, IoTSF

Peer Reviewers:

Vitor Jesus, Aston University

John Moor, MD, IoTSF

Ian Poyner, Consultant

Richard Marshall, Xitex Ltd

Mike Welch, Elite-IoT

Plus others – you know who you are!

Contents

1 Introduction

The advent of new technologies means our world has become increasingly digital. In recent years, this has included the introduction of new 'smart' and 'connected' technologies. 'Smart' meaning that it has an operating system running software to define its functionality, whilst 'connected' meaning it is also connected to other devices and (maybe) larger systems to achieve greater benefits to more stakeholders. Traditionally, these were thought of as information technologies (IT), however they are increasingly being used in operating environments in finer-grained, capability-constrained devices and operational technology (OT). These smart, connected, and pervasive operational technologies are often referred to as the Internet of Things, or simply IoT. It is when these devices and systems are integrated into a building/connected place and other systems that the benefits to stakeholders are realised.

The UK National Cyber Security Centre [Ref 1] defines a connected place as,

> *"a community that integrates information and communication technologies and IoT devices to collect and analyse data to deliver new services to the built environment, and enhance the quality of living for citizens"*

However, the potential risks to the smart and connected devices and systems associated with IoT are profound: smart, software-defined devices and services, are inherently susceptible to bugs and hacking; whilst connectivity increases the 'attack surface' of connected systems as routes into the system increase, and malicious actors do not need to be physically close to carry out their malign motives. When combined, these risks significantly increase the range of malicious actors as the payoff for a successful attack can be far greater and simpler to orchestrate; they can scale their attacks over many targets, and can work on different targets simultaneously. Many buildings using these connected technologies are not necessarily seen as 'smart' by those who work in them. Nevertheless, it is important to secure these systems and devices as they too may contain significant vulnerabilities. Additionally, connectivity means that some attacks spill over to other systems – for example, the 'wannacry' incident in 2017 reportedly cost the NHS £92m [Ref 2] in lost output and yet recovering data was considered collateral damage as it was not the intended target.

These risks are true across all smart and connected systems which are being introduced into our homes, offices, businesses, industry, government, and infrastructure. It is therefore essential that individuals, groups, and institutions, work together to respond to managing these smart-connected assets and their associated cyber security risks.

The IoTSF has produced this guidance to bring together cyber security expertise to support facilities professionals working in Smart Built Environments (SBE) – specifically Smart Buildings. The guidance presents IoT cyber security risk management best practices within a risk management framework and outlines the controls and processes to be applied to assure safe operation of IoT systems throughout a building's lifecycle.

1.1 Intended Audience

Facilities professionals are accustomed to managing a wide range of building-related risks, but cyber security risks may not be seen as a natural and key element of this portfolio. In today's SBE, this is changing and involves collaboration with IT and other specialists within the organisation and beyond. Since the convergence of many of the technologies has played a big role in the vulnerabilities, the response needs to be a joint effort between facilities professionals and the cyber and physical security professionals and teams.

This guide is intended to help facilities professionals play their part in establishing suitable governance arrangements to review and tackle the inherent risks. Achieving effective cyber security is not a one-off activity but is a continuous process, which follows the lifecycle of systems used in the smart built environment and the changing risk landscape. Maintaining cyber security should be a key on-going consideration for facilities professionals.

Although this guidance is primarily intended for facilities professionals, it is also for related specialists, support providers and stakeholders, i.e. those who have a role or are responsible for the wide range of built environment services (which enable and support business or operational performance or the cyber security of such devices and systems). Because of this, in the guidance the use of the term "systems" is to include not just SBE systems but any other system which may be connected to it whether it is intended to be part of the SBE systems or not. In some cases the connected systems may be IT, operational technology or other types of systems, regardless of whether the connection of these non-SBE systems is considered a good practice.

This guidance assumes that readers will be familiar with IoT application settings (i.e. buildings) but may have limited knowledge of the technologies and their cyber security requirements. It does not aim to make the reader a cyber-security expert but intends to increase the understanding and knowledge in managing IoT security risks so that all stakeholders can confidently enjoy the benefits of the technologies.

There are important milestones here for facilities professionals to understand and make a decision in relation to the business' objectives. As environments differ and vary so much it is difficult to be prescriptive but the decision on adoption needs to be made by the organisation. This document provides the opportunity to manage identified risk rather than accept the status quo. Each organisation may differ in terms of its structure, roles and responsibilities including those of facilities professionals. However, the functions and activities that need to be managed are more determinable.

1.2 Evolution of technology

Since the early 2000's, building control and management technologies have evolved with advancements in core technology, vendor interoperability and systems integration. Historically, a vendor's product would only connect into its own proprietary system and be operated in a silo. The situation today is very different, as manufacturers have made it simpler and cheaper to integrate new products onto existing multi-use networks, thus offering greater benefits to more stakeholders. [See Smart Building Technologies, Impacts & Implications for a more comprehensive breakdown].

This evolution has been driven by stakeholder interests, which has yielded increased benefits in non-consumer buildings technologies (often called "Smart Buildings" or "connected places"), as well as in domestic use environments (Smart Homes), infrastructure (Smart Cities), and other such Smart Building Environments (SBE).

Benefits from the advances may include:

- lower production costs, lower costs of integration and installation,
- reduced environmental impact and emissions,
- increased access to "real-time" data and information for analytics,
- AI applications enabling increased system performance outcomes.

The actual benefits to be realised vary from stakeholder to stakeholder, even to the point that they may even seem conflicting, e.g. whereas property owners may want to realise net zero, tenants may want much lower rents (which may make achieving net zero seem more expensive or a future goal).

Historically many of these building-related systems were provided as standalone installations with their own dedicated infrastructure and management system. Today, the great majority of this capability is provided by Internet Protocol (IP) based systems using a common infrastructure, often utilised over wide areas or long distances, bringing new capabilities. Such changes have created significant vulnerabilities and cyber security risk management concerns.

Many of the traditional propriety communications protocols have simply been updated to use the IT network protocol TCP/IP. Some of these new add-on communications protocols do not necessarily incorporate data security controls, such as transport layer security (TLS). As a result, they may be open to the types of cyber-attacks that IT systems are already familiar with; and will need to have relevant controls in place to secure data confidentiality, system integrity and availability.

1.3 Converged Systems; Building Automated Control Systems (BACS)

Contemporary buildings are often unique in the way their systems are put together, despite the use of common technologies. These systems are referred to as Building Automation and Control Systems (BACS) as defined by EN ISO 16484-2:2004 [Ref 3]. BACS systems can include any number of interoperable IoT elements and could be considered as the building systems' infrastructure. Whether IoT-centric or traditional BACS, the complete system may broadly comprise of but not be limited to the following types of systems:

- Building and energy management systems (BMS/EMS)
- Lighting control systems
- Security systems, such as CCTV and automated access control systems
- Vertical transportation systems, such as passenger/goods lifts and escalators
- Automated parking systems
- Wayfinding systems
- IT infrastructure hardware and devices

The Smart Building Infrastructure (SBI) can be viewed as the central nervous system around which the other smart building components are integrated. It includes the physical equipment, as well as the software layers that allow components to function. It enables these components to connect and communicate with one another. These systems will typically use an architecture comprising three levels of digital technology, providing management, automation and device-level functionality:

- Physical level: IT systems hardware, servers, workstations, network switches, etc.
- Software level: monitoring, artificial intelligence (AI), user interface, analytics, cloud computing, etc.
- Networking/Connectivity: intra (or inter) premises connectivity management.

Cyber-attacks can be carried out on any one of these three architectural levels and a successful attack on any could have an immediate impact upon the building's operations and any dependent intended benefits. A cyber-attack within an SBE can result in the compromise of a device, or other components, enabling a threat actor to take control of a critical system. This may allow settings to be changed, components turned off, or make plant equipment operate outside of its normal working parameters with the intention of damaging it. Once such access has been gained, this can often allow access to other devices in the system or allow theft of system data. In 2017 a casino in the United States installed a fish tank that 'featured internet connectivity. That connection allowed the tank to be remotely monitored, automatically adjust temperature and salinity, and automate feedings. It also allowed hackers to swipe 10 gigabytes of data from the casino that just installed it'. [Ref 4] A research report published by Kaspersky in 2019 highlighted the prevalence of cyber-attacks on smart buildings, 'with

nearly 40% of 40,000 smart buildings being impacted by a cyber-attack, either through the internet, removable media, email clients or shared folders on a corporate network ' [Ref 5].

The SBI is mainly the domain of the IT and/or networking teams, therefore, securing the SBI infrastructure will perhaps be much easier and straightforward than that of BACS. However, whilst the technology teams manage and secure the SBI from a technology attack, their physical aspects will still need to be secured by the facilities or physical security teams.

1.4 Document Structure

Section 2 outlines the main building technologies which are a part of a SBE and SBI. If these are compromised there can be impacts and implications to the business which need to be managed effectively.

Section 3 considers best practices to manage the risk to the SBE and SBI followed by a set of requirements. These cover Governance, Risk, Compliance, Operational Processes and Risk Response. It is of great importance that each requirement (and any surrounding issue) is addressed and recorded with the function or risk owner. This is likely to be best achieved with all stakeholders, where roles and responsibilities are established. Should a requirement be determined/agreed upon as not relevant, then it should be documented so that it may be seen at the review date and the conditions for the decision reconfirmed.

Chapter 4 outlines the use of CARS tables (where CARS stands for Communicated to, Approve an activity, be Responsible for and Support) to allocate roles and responsibilities [Ref 6]. CARS tables help define the key requirements set out in each section and expect the person or group completing them to identify who in the team it should be. These will include the typical roles for each requirement – e.g., Board, Risk Committee, Chief Information Security Officer (CISO), Chief Security Officer (CSO), Facilities Management (FM), Health & Safety (H & S), and Security teams.

Hence, we recommend the use of CARS tables to allocate roles and responsibilities for SBE security risk management with an example for Security Governance. [Readers may be familiar with RACI tables, matrix' or charts which use Responsible, Accountable, Consulted and Informed]. This can be applied to the other sections described in chapter 3.

The abbreviation and reference section is a useful overview of relevant international standards. There are new standards in related fields being regularly produced and so this list will be updated.

This document is a great credit to the SBE working group members whose commitment to excellence is evident. There will be new editions of this volume as the field of IoT expands into a range of SBEs and we encourage the reader to check they have the latest version (available from the IoTSF website at https://www.iotsecurityfoundation.org/best-practice-guidelines/).

Membership of the IoT Security Foundation grants access to online tools and communities to enable a better understanding of risk and its management. The reader is urged to make the best use of this document in its latest form and contact the IoTSF to comment on its usefulness, participate in working group discussions and thereby utilise its benefits to the maximum.

2 Smart Building Technologies, Impacts & Implications

Each building system technology is very different, but with enough similarities which may open them to different types of attacks to people, processes or technologies. This chapter provides further information about these systems.

2.1 Building & Energy Management Systems

Building management systems (BMS) enable building operators and management companies to monitor and adjust the performance of buildings systems. These systems typically comprise of sensors, actuators, controllers, and workstations, which can be managed either locally or via cloud-based solutions. Historically, BMS systems were connected together via separate communication networks, using either proprietary or open standard protocols, and remained predominantly independent from other systems. As clients and building owners increasingly want smarter buildings, manufacturers have responded with the development of sensors, devices and controllers that provide superior control and functionality over the Internet. Such connectivity has created opportunities to create smarter BMS, through converging critical BMS information and remote access anywhere in the world.

However, many of the traditional BMS protocols have been simply updated to use IP protocols, such as TCP/IP, as the transport layer, without incorporating secure communications protocols, such as transport layer security (TLS), to improve the security of data being transmitted. As a result, these systems are now open to the types of cyber-attack that IT systems are already familiar with; hence, they especially need controls in place where data cannot be encrypted.

In such a shared network environment, a compromised device or other component can enable a threat actor to take control of a critical system. This may allow them to change settings, turn components off or, make plant equipment operate outside of its normal working parameters with the intention of damaging it. Once such access has been gained, this can often allow the means to access other devices in the system or allow theft of system data. Therefore, it is important that IoT BMS devices and associated hardware and systems are identified and securely configured, have the most up-to-date firmware and software patches, and any known vulnerabilities are addressed or managed.

2.2 Safety and Security Systems

A range of IoT devices and systems may be deployed to help provide a safe and secure environment for building users. These systems often supplement and enhance the capabilities of staff responsible for these activities and sometimes replace a people-based approach. Historically many of these systems were provided as standalone installations with their own dedicated infrastructure and management system. Today the great majority of this capability is provided by IP based systems using common infrastructure, often utilised over wide areas or over long distances bringing new capability.

Integration of systems to give enhanced capability is becoming increasingly common and the introduction of data analytics and AI is being used to help operators handle the high volumes of data generated by these systems, identify events, and take decisions on what further action is required.

Safety and security systems provide potentially attractive targets to hostile actors who may have a variety of motives which include compromising security systems to allow other criminal activity or taking over life-safety systems to extort money from a company. Security systems may also hold a range of personal data on employees, which is also often attractive to attackers.

2.3 Electronic Security Systems

Security systems are very commonly used to validate identities and limit access to buildings and areas to authorised persons. These systems use a variety of readers, cameras, controllers, locking systems and barriers linked to a database of users and their access rights.

Intruder detection systems employing a range of sensors and detectors are used to monitor perimeters of buildings and key internal areas. These systems are often supplemented by CCTV systems with their own detection and recording capabilities and ability to operate in challenging environments e.g. very low lighting or areas dangerous to personnel. Security lighting, both covert and overt, is often deployed and linked to alarm systems or access control.

Specialised systems are often utilised in theft prevention particularly in retail environments where tags, detectors and alarm indicators are used to alert security staff to potential thefts.

Unified communications systems linking radio and Voice over IP (VoIP) are now increasingly common as are automated public address systems designed to alert people to specific events and direct them on what actions to take. The objective of attacking these systems may be to direct occupants so that the attacker's team is able to carry out their main goal in the building.

Each of these systems have made the news in their own right for the variety of attacks against them, as they are an obvious target for attackers, and are familiar to the public as example targets in movie heists and attacks. These systems may often appear as the first point of attack whether it be on the people, process or technology aspect.

2.4 Merged Access Control

Physical security and digital identity/network access management have for many years been considered and operated separately. However, in a Smart Building, which may have numerous IoT devices and systems such as doors, cameras, and PCs, there is a need to manage access in a converged approach. This is especially true given the increase in home working, and associated IoT devices. The facilities team responsible for access control should collaborate and ensure that remote access cannot be compromised by physical access and vice versa. Hence, a common view of the risks is vital in the management of physical and logical access control.

As with most building control systems, access control systems are a combination of embedded devices and the systems to control them. Each type of device can itself be a weak point, and consequently a target to take over the rest of the system, or just a landing point.

These systems sometimes have connections to employee data and may be key targets for the data alone. This change in the attack objective means that an attacking team may do so remotely. If the target data can be stolen and monetised without a chance of ever being identified at the target site, that is a more attractive option, thus, threat modelling is a very useful exercise for smart buildings and their systems. However, the need for robust physical security remains vital as attackers can also gain access to the network through social engineering and logging in to a pc on site. Hence the need to monitor and manage all areas of security.

Merged access control systems should alert the operator and or responsible persons when there is any unusual activity, or anomaly. For example, this may be a person badged into a building who is already logged in somewhere else. To determine the authenticity, the individual's pass is checked against a

live camera feed. If the two are different, then access may be denied appropriately. The speed of response also means more efficiencies, greater capabilities in compliance with privacy legislation and higher recognition from the business.

2.5 Vertical Transportation Systems

It is becoming commonplace for smart lift systems to be used in new building and refurbishment projects as they can provide useful operational real-time information with IoT sensors. These sensors can provide live data such as number of trips and door cycles, feedback on the ride (acceleration/deceleration, juddering, vibrations etc.) traffic trends and whether there are any faults with safety devices. The collection of this data can also assist with scheduling service visits and the planning of maintenance programmes.

Increasingly, larger buildings are using lift destination control systems that are server-based software solutions and use smart IoT lift equipment to provide greater efficiencies and reduce lift-waiting times. These smart systems can also be integrated with other technology, such as electronic access control systems to allow the building users' access credentials to determine access rights to floors, or CCTV systems monitoring people flow to enable the prioritisation of lift cars. The integration of such systems usually requires the use of an application-programming interface (API) and some middleware to enable data between the systems to be shared. These IoT systems require the secure exchange of data between two systems even though they are independently developed and, in many cases, independently managed.

This use of IoT devices and supporting technology hardware for lift systems has created new exploitable cyber-security vulnerabilities, which could impact the building operations. The integration of systems creates further vulnerabilities due to the necessity to share data and the requirement for those systems to use the same IT network for communications. Should an attacker be successful in compromising a lift system, control of lift cars could be obtained and may result in the lift system rendered inoperable or causing an entrapment scenario. Where IoT safety devices are compromised and cease to function correctly, e.g. if lift cars develop faults which are not reported and left unresolved, they could result in lift failure, expensive repairs and entrapment of building users.

2.6 Automated Parking

Automated Parking Systems refer to the automated parking of a vehicle inside a building. In its most complete form, it comprises of the following:

- The vehicle is driven to a safe entrance
- Once the vehicle is safely stopped, the driver exits the vehicle and performs a registration, typically using a screen
- The driver exits the entrance, which is then locked
- A set of moving lifts, escalators and/or pallets park the car at an available spot
- The vehicle is retrieved using the reverse process

These systems rely on three components:

- The mechanical lifts, escalators, or pallets to physically move the vehicle from/to the parking spot, along with the necessary coordination logic
- The registration system at the entrance and exits, which will consist of a human-machine Interface

- Internal vehicle tracking to park and always retrieve the correct vehicles, typically involving automatic number plate recognition (ANPR).

The required functionality, whole or in part, opens the building to new types of vulnerabilities with an impact on different dimensions, such as availability of service.

A particular vector of interest is the interface for users, assuming a fully user/automated system. This system should be, from a user perspective, like a pay point, except that it will be controlling a more complex system, which ultimately, can involve heavy machinery such as vehicle lifts and platforms. Since there will be network connectivity at the user terminal, a wide range of attacks may be possible. The APNR system is another component that relies on direct user input and needs to be secured.

2.7 Control Rooms

A control room in a building is a secure and access-restricted physical location, typically inside the managed building or group of buildings, from where the state of the building can be centrally monitored and managed. The typical physical layout of a control room consists of several screens and computers with audible alerting functions.

In some cases, components of the control room may be running in the cloud, where their functions are remotely accessible by facilities professionals. Depending on the degree of cloud integration and consolidation of data, it is possible that multiple facilities are managed from a single central location.

A wide array of technologies and tools can coexist in the same room; control rooms will also rely on networking and communication technologies, which are often heterogeneous, to monitor and manage different devices and sub-systems (e.g., CCTV, HVAC, lighting, etc.). Often, these sub-systems are managed using different non-integrated tools.

Due to the sensitive and often safety-critical nature of the functionality in a control room, and the privileged and wide-view of information about the state of the building, a control room requires special security measures to prevent unauthorised access to the systems of the building.

3 IoT Security Requirements for Smart Buildings

In the introduction, it was established that the field of IoT is both complex and dependent on many different devices and systems. As these are often connected to other systems and the internet, they are at risk from a range of cyber-attacks either remotely or internally. This means that like other IT systems there is a need for a range of mitigating controls and security measures to be put in place to reduce risks. However, these mitigating controls and security measures will be unique to each installed SBE system and different to similar measures deployed for IT systems. This document lists and numbers them as requirements**.** It is recommended that the facilities professional reviews each of the requirements and allocates responsibility to a person or team member. Often this can be more effectively achieved in a risk committee meeting with the appropriate people present.

Terminology: In the requirements sections listed below, the following terms "must", "must not", "required", "shall", "shall not", "should", "should not", "recommended", "may" and "optional" are used in accordance with the definitions in RFC2119 [Ref 7].

3.1 Governance, Risk and Compliance (GRC)

GRC has become critical to the established physical security profession as well as the cyber security profession. Both have an ever-growing number of standards, codes of practice and regulations, and with technology convergence, there are many more considerations and dependencies than ever before.

This section introduces security governance, risk, and data protection (as an example of regulatory compliance). The decisions, activities, and actions these professionals undertake are based on risk. Many have a deep understanding of risk and its relation to the work they do; in this section, we explore some of the more specific issues around IoT security rather than general GRC.

3.1.1 Security Governance Overview

In Smart Buildings, good Security Governance provides the framework for multi-disciplinary teams to work together to achieve their joint objectives. In practice, this means selecting and bringing together the core elements of People, Process, Information, Technology, and Facilities (commonly referred to as ‘PPITF’) with the right culture so that risks are managed by the right people at the right time with the right tools.

Security governance will likely vary among organisations and will depend on many factors, including organisational structure, the size of the enterprise, how the business works, how it utilises/depends on suppliers, and how the facilities team operates. In practical terms, these arrangements will also vary because of detailed factors such as the building occupation model, the nature of the organisation, and its appetite for risk. Further, there will be a need to either adjust or create new processes to support the above more effectively.

In many settings, it is likely that a number of services will be outsourced, whether it is the installation / integration services, specific elements of the facilities management activities, or maintenance. This means providing good security governance in the procurement and management of any third-party activities will be vital to ensure that outsourcing does not become a weak link.

3.1.2 Security Governance Requirements

This section's intended audience are those personnel responsible for the governance of an organisation that has buildings where IoT devices are selected, installed, operational, updated and decommissioned. Given the propensity of such buildings, this will apply to most businesses. There must be a named executive(s) responsible for IoT devices and systems' security, and the related privacy of personal information of all users. Additional guidance is available from the Information Commissioners Office, for example on Video surveillance (including guidance for organisations using CCTV) [Ref 8].

Req No	Requirement
3.1.2.1	Business goals, priorities and expected outcomes in relation to the SBE, its assets, operations and security shall be documented appropriately.
3.1.2.2	There should be a documented strategic overview on how governance provides the required security activities (linked directly to business goals and priorities).
3.1.2.3	The governance structure shall provide clear decision-making responsibilities for security risk decisions across the whole organisation and eliminate siloed responses (with the risk committee at the top).
3.1.2.4	Resources to achieve the security goals should be allocated to manage risks effectively.
3.1.2.5	Clear policies, (internal) standards and other documentation that specify operational and managerial responsibilities for security decisions shall be developed and socialised with business stakeholders.
3.1.2.6	There shall be an agreed list of frameworks and standards to be complied with (and what cannot be complied with). This shall include the required levels of assurance and maturity (with an understanding that high levels of maturity are not a requirement for all controls or assets).
3.1.2.7	There shall be clarity as to who is responsible and accountable for which systems, processes, and risks across the SBE. Those who need to be communicated with or involved, have been identified, as well as those who are to provide cyber security support across the SBE.
3.1.2.8	The procurement team shall have the authority to use relevant policies and standards to ensure secure updateable solutions and contracted services are based on risks to the business and the SBE.
3.1.2.9	Both in-house and contracted services shall have defined responsibilities for compliance with policies, standards, and regulations.
3.1.2.10	There shall be defined roles, responsibilities and relationships for integrators, installers, and maintenance services across the SBE and the lifecycle of devices and systems.
3.1.2.11	The role of the facilities teams at all levels of security decision making shall be clear whether the team is in-house, outsourced or a combination of both.
3.1.2.12	The role of corporate IT and cyber-security in providing guidance and support to all SBE and SBI stakeholders in ensuring effective governance should be recognised, and resources are allocated. The arrangements for providing and managing the required expertise are clearly identified.
3.1.2.13	Guidance should be developed for the default fail-safe approaches for all technologies and services to protect people, the environment and the device or service according to legal obligations and business requirements.
3.1.2.14	A process of audit and review shall be established to ensure policies and arrangements are properly implemented and updated as necessary.
3.1.2.15	A reporting framework shall be established and incorporated into the wider enterprise GRC arrangements.

Table 1 Security Governance Requirements

3.1.3 Risk Management, Risk Assessment and Compliance Overview

Cyber security is not a static consideration; risks and threats to an enterprise are continuing to evolve and require regular reviews to ensure the selected controls remain fit-for-purpose. Any such reviews may also require updates to policies and the standards and frameworks which support them.

In many large organisations, there may be many physical and cyber security risk frameworks, standards, and policies. Historically the physical and cyber security risks have been addressed by teams, which had little in common with each other. The introduction of IoT technologies provides a shared interest for the physical and cyber teams to work together to manage, mitigate and reduce the impact of safety and security threats. With the increased threat of "blended" or "hybrid" security attacks, it is essential that those teams work together. For example, the attacker in these scenarios may start with an online phishing attack, and then impersonate a member of staff on the phone and gain entry to the building and business email. Each attack increases their knowledge to eventually raise invoices for thousands of pounds. If they have also gained control of the CCTV system, it could enable other thefts of cash from tills and bank vaults. Most facilities and cyber security management teams have an excellent understanding of the risk assessments they are used to undertaking, however IoT systems often introduce elements that neither team is completely familiar or experienced with.

It is essential that a formal process be adopted for understanding and assessing the risks posed by IoT systems. This risk assessment needs to draw on the required level of technical knowledge within the organisation or by employing external expertise. A facilities professional may lead such a collaborative approach or delegate it to a person sufficiently experienced. A workable response would be to form cross-functional security teams to conduct risk assessments and allocate responsibilities to maintain (upgrade and patch) systems.

The output of such assessments would need to be incorporated into a wider enterprise security risk management strategy or the main organisational risk assessment process so that the significant risks are more widely recognised and understood. ISO 14798 [Ref 9] , ISO 27005 [Ref 10], ISO 31000, [Ref 11] ANSI/ISA 62443-3-2-2020 [Ref 12]or SP 800-30 Rev. 1 [Ref 13].

Achieving GRC generally necessitates several specialist roles working together. SBEs are no different in that respect, facilities professionals utilising their skills and experience with that of others, including cyber security teams. Much of the documentation listed in the GRC requirements may already exist across the organisation in similar assessments or reviews. Where such documentation doesn't exist, there are likely examples available which can be used as templates for the SBE.

It is most unlikely that facilities professionals will be able to complete or compile all the requirements on their own without the involvement and participation of other specialists. This is why some of the governance requirements are important to ensure that facilities professionals are not left without the support of other specialists, including the cyber security team.

The requirements below are intended to cover gaps in risk which exist due to using standardised technologies with known benefits and costs. Unfortunately, some of the known costs include the implementation of additional controls. Fortunately, as similar technologies have been around for a while, there are known controls, actions and responses which can be taken by existing teams within most organisations. This means that no facilities professionals should be in a position where they are left on their own without access to the right knowledge, skills and expertise. However, even in the worst case, it is always possible to find consultancy services who can assist with such requirements, as they will have completed similar work for others in producing assessments, documenting standards, etc. on IoT devices and systems within an SBE.

The risk assessment process would need to consider the possible motives for a cyber-attack to help gauge the likelihood of a cyber-attack to the business by targeting the smart built environment.

3.1.4 Risk Management, Risk Assessment and Compliance Requirements

Req No	Requirement
3.1.4.1	A formal risk management approach shall be established and utilised with clear policies, processes, and responsibilities. Threat modelling should be used as a way of providing more informed threat decisions.
3.1.4.2	SBE and SBI risks and threats should have been identified and prioritised according to business needs and impacts to SBE and SBI IoT devices and systems.
3.1.4.3	Changes in policy and compliance with standards and frameworks shall be documented and shared with all those who rely on them.
3.1.4.4	Cross functional teams shall be identified to manage the SBE and SBI device and systems risks and to agree (and distribute) a baseline security posture for the SBE.
3.1.4.5	A cross functional team shall be established to agree security requirements for existing as well as new SBE systems and solutions. These include the verification processes and checks for the installation of new systems and solutions as well as maintenance of existing systems.
3.1.4.6	The level of security shall be established and agreed for new SBE devices and systems connecting to existing technologies and how they will be requested and tested.
3.1.4.7	Outdated and deprecated technologies, standards and protocols that shall not to be used within the SBE should be documented, (this may include for example, outdated encryption standards or protocols, or communications technologies, or use of open vs proprietary protocols, etc.).
3.1.4.8	There shall be a team responsible for creating and maintaining a list of network access to be granted and already granted, (including, for example, any third-party suppliers and support providers for the SBE systems).
3.1.4.9	There shall be an audit of the SBE IoT devices and connected systems to establish their current state (if this does not exist).
3.1.4.10	A Threat Model of the SBE shall be developed and shared with all teams who are to provide an input.
3.1.4.11	A SBE risk register shall be created and maintained, with inherent risk scores and incorporate outputs into wider ERM systems and processes.
3.1.4.12	Key Risk Indicators and any other risk metrics shall be tracked by the risk committee (or Executive Management) to identify trends or changes.
3.1.4.13	Regular updates on risks and risk mitigation measures shall be produced for use by the risk committee and within any wider GRC management arrangements.
3.1.4.14	Existing and new legislation shall be regularly reviewed, (for example, H&S, SBE, IoT security and data protection) and requirements [re-]assessed to ensure the implementation of mitigation controls.

Table 2 Risk Management, Risk Assessment and Compliance Requirements

3.1.5 Data Protection Risks

Data protection is a risk, which merits specific consideration as almost every commercial “smart”, or “connected” building will collect data that falls within the prevailing data protection legislation in whatever country the building is located. In today’s commercial environment, there is no way of avoiding a minimum level of data collection when using surveillance technologies to protect building estates, access control systems and visitor sign in systems.

The personally identifiable information (PII) controlled by building occupants (or controlled on their behalf) could include but not be limited to:

- CCTV footage.
- Electronic access control event data.
- Car parking and visitor bookings.
- Building location services.

The European General Data Protection Regulation (GDPR) 2018, [Ref 14] and the UK's enactment of the UK Data Protection Act 2018 [Ref 15], are possibly the most demanding Data Protection regimes in use and have been used as models by many other countries. Although responsibilities and obligations vary depending on the country, there are often similarities.

Data protection is a complex topic and outside the scope of this document, but the requirements and risks associated with the handling of this type of data must be assessed and acted upon. Noncompliance or failure to protect data adequately can result in significant fines from the regulators [Ref 16] in addition to the reputational damage to the organisation.

If facilities professionals are responsible for the operation of technology, which collects such data, they will have to ensure that they have involved and collaborated with the appropriate professionals in their enterprise to cover all data protection risks. This may start with the Data Protection Officer and extend to network security managers to get a better understanding of whether the organisation is currently complying with legislation.

3.2 Operational Processes and Risk Response

This section considers some of the requirements relevant for an organisation's secure SBE. Within the sub-sections there are recurring themes throughout the processes. For example, the resilience that is desired and covered in sub-section 3.2.18, is only achievable if it is considered appropriately in each of the previous processes, from the requirements through to Supply Chain, Design, etc. In many respects, the output and results from earlier requirements hand those over to the next group of professionals as and when they need to be involved, to ensure continuous security improvements.

As risks, vulnerabilities and threats are constantly changing, improvements to Smart Building security are also a changing continuum especially since the number of new technologies being integrated into existing systems is not static.

To be successful there must be an early focus dedicated to agreeing the scope of the work, provision for any funding requirement and an outline timescale for the work. This will become an on-going exercise, as the lifecycle of systems rolls on and new threats and requirements emerge. Since there are many more existing buildings and projects than new builds, the approach has to be to improve IoT security anywhere it is relevant to do so.

3.2.1 IoT Technology and Security

Many compromises may need to be made when considering IoT technology requirements. What is required may not be available, or available at a price point acceptable for managing the risk in question. These challenges are often the reality of security managers, regardless of whether they are from a physical or cyber security background. In the past, however, such decisions tended to be regarding systems which lasted 15-25 years when technological developments were slower. Now with technology development moving so fast, making the wrong decision can be costly if the selected

technology presents security issues, doesn't last as long as expected, or doesn't accommodate other technologies which are to be integrated.

To select IoT devices and systems with the most appropriate features and capabilities, the requirements of the facility need to be identified. Selection of the right IoT devices will facilitate accurate collection of data, change detection and environmental control in real time. The right selection of IoT devices similarly delivers the most secure end-to-end solution that fits with the level of sensitivity of the building/facility.

The factors worth considering when identifying requirements for system solutions broadly relate to the technology, device, system or solution. The approach will be guided by the risk assessment. The team must acknowledge the importance of each component's security status within the built asset and the implications of a security failure of any single component upon the whole asset or system(s). For example, the communications protocols between IoT devices and cloud platforms would also be taken into consideration: HTTPS and MQTT are the most commonly used protocols. HTTPS is document centric and entails request-response for client-server computing. MQTT is data centric for resource-constrained devices, which enable clients to operate independently from each other to facilitate enhanced reliability and confidentiality.

To avoid inherently insecure systems being installed into a building's ecosystem, it is crucial that a facilities professional set out their cyber/information security requirements in a brief, to be referred to throughout the selection process.

Essentially, success in the requirements stage of the lifecycle can be tied to the different teams and individuals brought in to advise on the cyber security aspects of every technology, component and device to be used in the project. Due to the complexity of many organisations as well as the technologies, it is often not possible for any single team to complete either a requirements stage or the procurement stage on their own.

It is difficult to dictate in any way what may or may not be a relevant requirement for the solution, due to each environment being very different and its connectivity to devices and systems being equally different. For this reason, we have also provided examples of requirements which may come into play depending on the environment and project itself.

3.2.2 IoT Technology and Security Requirements

Req No	Requirement
3.2.2.1	There should be agreed standards / qualifications, versions, methods of testing, acceptance and performance, from both existing and proposed SBE solutions. These should be shared with the relevant individuals, teams and third parties.
3.2.2.2	Compliance with organisational cyber security standards e.g. ISO 27001, and their associated requirements should be agreed with suppliers, installers, and system integrators. Provisions should be made for existing suppliers to achieve these within required timescales, based on risk.
3.2.2.3	Where applicable the IoT security requirements shall include the following:
3.2.2.3.1	capabilities and competencies expected from the supplier organisation and the professional services to be utilised;
3.2.2.3.2	options, processes, etc. for remote administration of systems so that future as well as current risks can be assessed effectively;
3.2.2.3.3	options for any data migration that may be required;
3.2.2.3.4	any processing of personally identifiable information (e.g., CCTV & Access Control vendors) that is required and how to ensure the supplier and their sub-processors have appropriate technical and organisational controls in place to safeguard personal data through data processing agreements between the data controller and the processor;
3.2.2.3.5	where services or assets are sensitive and security requirements are not to be compromised over costs, the selection criteria is to be followed through by all suppliers and their contractors;
3.2.2.3.6	where services are likely to require a Proof of Value (PoV), there is a clear documented set of “must have” criteria which must be met;
3.2.2.3.7	the specification of environmental requirements, e.g. power or wireless networking arrangements;
3.2.2.3.8	the specification of product life requirements – how long the intended solution is expected to be in use;
3.2.2.3.9	the expectation of support and interoperability with other solutions or technologies;
3.2.2.3.10	critical services suppliers should be made aware that their critical suppliers may also be audited as part of the selection process.
3.2.2.4	Guidance should exist or be created and updated from time-to-time, as necessary, on IoT security specific issues. These may include for example, any of the following and the response required in given conditions:
3.2.2.4.1	how to assess the different types of wired and wireless communications (including for example, Bluetooth, Wi-Fi, etc.) and their impact on security, the network, data volumes handled, the risk of collision of simultaneously transmitted data signals, etc.;
3.2.2.4.2	how to assess the different types of interoperability issues with existing and emerging technologies and their capability to comply with security standards and future technology adoption;
3.2.2.4.3	how to assess the impact of real-time information received and transmitted by the sensors (in various formats) so that it can be used most effectively for the Detection, Response and Recovery functions;
3.2.2.4.4	on data requirements (in terms of secure storage, management, and access, and the received data being in real-time, time series or summarised) for all the relevant security functions and processes;

3.2.2.4.5	data access rules to different types of devices, systems, networks (etc.) based on needs and risks;
3.2.2.4.6	the use of remote monitoring and secure cloud-based solutions;
3.2.2.4.7	the acceptable and unacceptable approaches to how IoT devices and systems implement fail safe modes within the SBE and SBI;
3.2.2.4.8	how to respond where existing technology solutions do not comply with upcoming standards, or proposed solutions options don't fully comply with existing or upcoming standards or requirements;
3.2.2.4.9	the minimum testing that groups of devices and systems will be subjected to, to verify their suitability for use.
3.2.2.5	IoT security specific requirements should exist for the Protection, Detection, Response and Recovery functions. New solutions should meet these requirements to ensure effective resiliency.
3.2.2.6	An identity and access management policy should be developed and maintained for IoT devices and systems, in conjunction with the cyber and network security teams.

Table 3 IoT Technology and Security Requirements

3.2.3 Supply Chain Overview

Supply chains are increasingly interconnected and complex, and a modern organisation's dependence on them is growing. It is vital therefore, that the cyber security arrangements of the supply chain are carefully considered, as any element in an organisation's supply network can be targeted in a supply chain cyber-attack. Such attacks provide a gateway, since SBEs are complex technological and operational environments relying on many third-party suppliers for specialist services in design, installation, operations and maintenance of the SBE and SBI. Third party suppliers must demonstrate an appropriate level of cyber-security awareness, and implementation of security controls when delivering the services they are contracted to provide. It is crucial for facilities professionals to consider the supply chain risk in the selection process. Hence, this section should be reviewed alongside the Design and Procurement Overview 3.2.5 and

Design and Procurement Requirements listed in 0.

Assessing the capabilities of third-party suppliers is an iterative process comprising regular audits to ensure service providers meet the compliance requirements. Due diligence provides organisations with a greater visibility of a potential, or existing supplier's controls, operations, and cyber-security posture. Insights gained from supplier due diligence and applying security governance to suppliers can help manage risks more effectively.

When specifying a product or supplier's security requirements the NCSC's 12 Principles of Supply Chain Security [Ref 17] is a very useful reference document. These principles have been designed to help organisations gain and maintain the necessary level of control over their supply chain. It is strongly recommended that the facilities professional reviews these principles alongside the specific requirements listed below. This is especially important because much of an organisation's supply chain may consist of SMEs who may not have invested in cyber security and may inadvertently create the weak link in the supply chain. The supply of critical services must be completed by installers and integrators who can do so meeting the organisation's cyber security requirements as it is important to ensure that no services are left more vulnerable than before the supply of any new service.

3.2.4 Supply Chain Requirements

Req No	Requirement
3.2.4.1	Documentation shall be created to capture the security risks posed by different services being partially or wholly outsourced, how these risks will be mitigated and who will be responsible for them.
3.2.4.2	An information pack should be created which includes the minimum requirements for different groups of service risks that suppliers will be expected to mitigate.
3.2.4.3	A template of contractual terms, already translated from the security requirements, shall be created for use in supply contracts.
3.2.4.4	As part of the contractual template, the management, mitigation and reporting obligations shall be captured for the different types of breach incidents at supplier sites or those managed on behalf of the organisation.
3.2.4.5	Security requirements for the SBE and the SBI shall be produced regardless of who or how the service is or will be provided.
3.2.4.6	The complete set of up to date requirements shall be made available for potential suppliers of different levels of cyber security and non-cyber security services (e.g. physical security).
3.2.4.7	A supplier selection process shall be documented and maintained, which includes pre-contractual due diligence questionnaires and supplier security posture risk assessments on all ICT/OT/physical security / IOT suppliers. Such a process should give suppliers opportunities to ask questions before participating in the selection process. Documentation should also cover service renewal and changed supplier scenarios, newly changed service contracts, handover processes to new suppliers and requirements for terminated suppliers.
3.2.4.8	A process shall be provided for the regular review of existing suppliers meeting current security requirements, including any special requirements for specific risk areas, technologies, or types of systems.
3.2.4.9	A documented audit process shall be created, identifying all suppliers and establishing their criticality to meeting key business requirements which includes technical and organisational controls and provides information on possible impacts on future connected services.
3.2.4.10	The security requirements shall include existing services/suppliers and how they will achieve the security goals of the SBE.

Table 4 Supply Chain Requirements

3.2.5 Design and Procurement Overview

Although design and procurement are very different and dealt with by different teams within an enterprise, for the supplier of services they are connected. The cyber security knowledge and competencies they demonstrate are important throughout these processes, which is why we have included them together here.

3.2.5.1 Design

In the context of this guidance, we use ‘design’ to mean the specification of the system to be installed on-site by an installer or integrator (which should also be secure by design and default). Secure system design capabilities cannot be overemphasised particularly when they are to be integrated or connected with other shared SBI systems.

3.2.5.2 Procurement

In most organisations, the procurement teams are not as knowledgeable about security requirements as security professionals, which can result in security requirements being watered down for much cheaper, lower quality, less secure options. A lack of governance can result in procurement teams not considering the agreed security requirements.

The use of organisational security standards like Cyber Essentials (in the UK) [Ref 18] has served to elevate some physical security suppliers over others. Further, the introductions of Codes of Practice by the British Security Industry Association (BSIA) for installers of safety and security systems [Ref 19] are making the work of designers and procurement teams easier. As these approaches are spreading throughout the various security sub-sectors, including fire, lighting, HVAC, energy management, vertical transportation, etc. they are beginning to provide a base level of confidence in contractor installers and the manufacturing vendors they in turn are using.

When procuring devices and systems, which are expected to be in use for 15 to 25 years, it is important to know that even if the installer is not around for that period, the manufacturer will be, and that security updates will be honoured for at least the time stated. Additionally, it is important to know that installers will provide support for several years beyond the installation period and into the system being embedded.

The role of procurement in achieving security cannot be over emphasised because the due diligence to meet security requirements can determine how many extra resources may subsequently be needed to deal with any consequent security issues (which were missed or overlooked during procurement).

Suppliers sub-contracting a service need to be held accountable for the actions of their sub-contractors. Suppliers should detail in master service agreements the formal security posture assessments their sub-contractors are to be subject to. This provides reasonable assurance to facilities professionals that the sub-contractors have adequate technical and operational controls in place.

3.2.6 Design and Procurement Requirements

Req No	Requirement
3.2.6.1	A documented network security architecture shall be developed, which ensures the security of the SBI and the range of technologies, services, solutions, and providers it will need to accommodate.
3.2.6.2	A documented risk analysis shall be carried out as part of the SBI design process to identify and assess the impact of security related threats, exploits and vulnerabilities.
3.2.6.3	The SBI design shall ensure that future additions and alterations can be easily managed and tracked, including network services used by security devices, (this includes for example, where network segregation is not possible there are measures to protect devices from other network connections).
3.2.6.4	Controls for organisational network infrastructures, the SBE and the SBI shall be documented, and the proposed solution shall ensure that each one can be controlled, managed or isolated without any negative impact to the others.
3.2.6.5	All site specific or environmental requirements shall be available to prospective suppliers to consider during any site surveys or other inspections, which may be required before or during any design of the solution.
3.2.6.6	Where a solution provider will be required to undertake a Proof of Value (PoV) project, or test or validation of the solution, this should be made clear and a request for minimum requirements should be sought from the vendor.
3.2.6.7	All SBE and SBI procurement policies and procedures shall include principles of effective security.
3.2.6.8	All procurement processes shall include clear documented requirements for maintaining the security of the SBI and the policies which suppliers will need to comply with.
3.2.6.9	The FM should coordinate the procurement and cyber-security teams to test and validate designed solutions.
3.2.6.10	The FM, procurement and cyber security teams shall agree which solution is the best match for the previously agreed requirements and shall document any cyber security compromises agreed, why they were acceptable and how any outstanding risks are to be mitigated by whom at what cost.

Table 5 Design and Procurement Requirements

3.2.7 Installation, Commissioning and Acceptance Overview

Procurement and FM teams are very familiar with the installation, commissioning, and acceptance processes for systems they have worked on previously. However, the complexities of including the security of IoT devices and systems can be simplified by involving all the right expertise within the enterprise, or through additional specialist advisors.

The success of each phase in the system lifecycle is dependent on the communication in the previous phase; the more time spent agreeing requirements, how they will be met, and due diligence to verify this, results in a much smoother installation, commissioning and acceptance phase.

Installing and integrating IoT systems securely is not the same as installing and integrating similar non-IoT technologies. The IoT aspect, that is, the internet connection aspect necessitates that there is a major difference. Consequently, the British Security Industry Association's "Cyber Security Product Assurance Group" (CySPAG) created a Code of Practice for installers and integrators of safety and security systems . This guidance covers all the relevant requirements for secure installation of these systems. This Code of Practice is not mandated, yet it provides the requirements that should be

considered by designers, installers and integrators regardless of skill levels, experience or expertise. If your preferred installer or integrator is not familiar with these requirements, you will have to manage the requirements using alternative additional resources.

Security certifications may be held by a single individual within an installer organisation or by several individuals. Whatever the case, (where possible) it is important that those overseeing the work have the right certifications and experience to install all aspects of the devices and systems securely, e.g., is the lead installer familiar with network security to the level stated in the requirements and discussed with the internal network and security teams? Otherwise, the organisation is left with having to identify someone else familiar with the risks to take action and provide the necessary assurance. The objective would be to find installers with the right cyber (network) security training who do the work correctly once. It may be difficult to find installers who have the same network security skills as enterprises would want. However, it is important that the guidance in this document be used to meet expectations.

Device Inventory

It is important to maintain a comprehensive baseline inventory and asset register of all devices within the building infrastructure. The challenge is simpler for new upgrades of the infrastructure, or modern buildings, as registers are likely to exist, and technical tools are often available which can autonomously and periodically populate an inventory. Modern devices will also typically, support discovery protocols. For older deployments, however, this may be more challenging, particularly if the building has been in operation for a long period and undergone multiple cycles of infrastructure updates.

To maintain a comprehensive inventory of all devices connected to the network, it is important to use automated tools regularly. Such tools are either free (open source), or proprietary. Many BACS use standard protocols that have discovery functionality and are often free. For example, the inventory discovery of BACnet devices; Modbus devices for which there are simple tools available to automatically discover connected devices; IP-based devices, such as those connected to an Ethernet LAN, where a number of tools are also available.

It is possible that the current infrastructure management tools already provide a degree of visibility to the current inventory, which is something the technical team or manufacturer will likely be able to answer. If so, it would be important to consolidate multiple sources of inventory.

The first inventory collection would be accompanied by both a manual and visual inspection and confirmation. Any devices not automatically discoverable would be subject to a different management policy and manually re-inspected periodically if they cannot be replaced or upgraded.

Any device discovery process during and post installation can confirm and verify what has been installed as part of the solution delivery project.

It is likely that the technical team managing the building needs to be engaged when provisioning and operating the tools required. Since it is possible that the inventory is managed using an inventory tool, access to the tool also needs to be negotiated and agreed.

The facilities professional, or any sub-contractor, is likely to be the owner of the inventory and will run the first manual inspection. The consolidated inventory baseline, at the first point in time, is thus a multi-stakeholder action. If dependent on a manual procedure, good calendaring and scheduling practices would need to be kept.

3.2.8 Installation, Commissioning and Acceptance Requirements

Req No	Requirement
3.2.8.1	Timescales, responsibilities, and processes shall be agreed before installation, commissioning and acceptance activities are carried out. Training considerations shall include a training plan, which should include what training, how much is required, and when it is to be completed. Other considerations include back-ups, how and where data will be stored, future maintenance responsibilities, etc.
3.2.8.2	During installation confirm that it meets the following security requirements:
3.2.8.2.1	Timescales and key measurable milestones should be set out and then monitored closely.
3.2.8.2.2	Contractors and installers should produce their own risk assessments and method statements for any planned work.
3.2.8.2.3	Connections to existing systems and infrastructure shall be risk assessed and shall be in-line with the previously agreed design. Components and configuration settings shall be documented for the maintenance of network security.
3.2.8.2.4	Each installed device / system component shall be updated to the most recent version, and there shall be a mechanism to be informed of security updates and how these will be implemented.
3.2.8.2.5	Security issues associated with data migration shall be identified and documented.
3.2.8.2.6	Training shall be provided for operational personnel on the requirements and responsibilities to ensure the system(s) they manage or oversee remain(s) secure.
3.2.8.2.7	Back-up and restore processes shall be tested (in accordance with existing policies) to ensure they are able to recover the system to full operability.
3.2.8.3	During commissioning, IoT devices and IoT centric systems shall be designed, installed, configured and tested so that they perform in accordance with the design specification or clients' requirements.
3.2.8.3.1	A commissioning process should be applied to new projects, upgrades or additions to existing systems.
3.2.8.3.2	Commissioning activities should be collaborative and carried out by the installer with the assistance of the end user, operator and/or appointed advisor.
3.2.8.3.3	A commissioning plan should set out how systems have to be configured and tested, and if appropriate, how old systems should be decommissioned.
3.2.8.3.4	Agreed testing procedures of systems should include checking the functionality and configuration of IoT device security configurations and secure communication settings.
3.2.8.3.5	Testing procedures should confirm systems meet design and performance objectives.
3.2.8.3.6	Detailed commissioning information and test sheets should be completed and issued before formal acceptance.
3.2.8.4	A formal point of handover shall be agreed only when system security responsibilities are fully transferred as per the agreed design and maintenance agreement.

3.2.8.5	Formal acceptance of the installed system should include resolving any outstanding security issues and who is to take what action, by when and any consequences related to these issues.
3.2.8.6	Immediately after acceptance of the solution, the asset register shall be updated to include all new devices, software, systems, components, etc. provided as an element of the solution, to include:
3.2.8.6.1	Device name, model, version, and manufacturer
3.2.8.6.2	Last verified (time and date)
3.2.8.6.3	Method of detection (manual or automatic)
3.2.8.6.4	end of the manufacturer's product lifetime
3.2.8.6.5	Whether it is in operation, maintenance or retired.
3.2.8.6.6	Physical and topological location (e.g., room and network IP address, MAC addresses)
3.2.8.6.7	Any unique identifiers such as a serial number
3.2.8.6.8	Ownership – agreed by all stakeholders.
3.2.8.6.9	Asset type and associated subsystem (e.g., HVAC or Lifts)
3.2.8.6.10	Software and firmware versions (and dates).
3.2.8.7	Processes and controls for day-to-day operation and maintenance of the system by any third parties shall be documented and include arrangements for any remote access to the system.

Table 6 Installation, Commissioning and Acceptance Requirements

3.2.9 Operations, Maintenance and Upgrading Overview

IT, network, and security teams have been used to managing and contracting operations, and the secure maintenance and upgrading of IP based systems, probably more so than physical security or facilities professionals. For this reason, it is advisable for facilities professionals to liaise with the IT, network and security teams about the processes and tools they plan to implement, before enacting, to achieve their security goals.

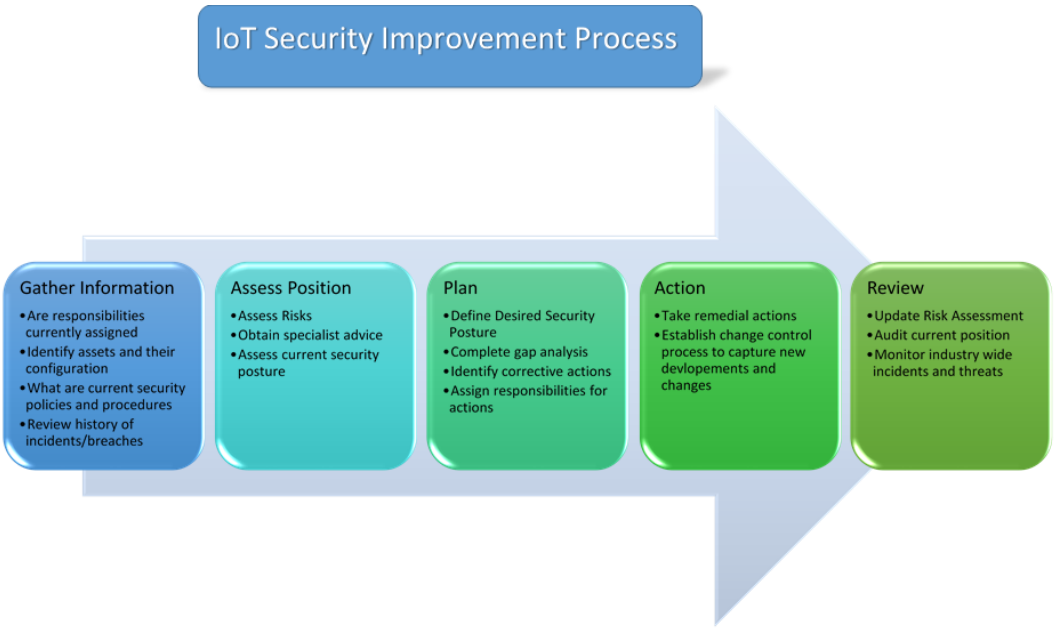
Configuration changes are one of the most critical processes that many organisations still don't get right. In a recent survey by Cyber security Insiders (on the State of Security Posture 2022), when asked the question "Which of the following areas do you believe are driving the most risk to your organisation?" 45% identified "Misconfigurations" as the third highest response [Ref 20]. Configuration changes by third party suppliers can complicate the response required, especially if you do not know what the norm was or is supposed to be, what it has been changed to, and the impact it has had on the rest of the system(s) or network.

Third party contractors can only be as good as you demand they are; what they do, when they do it, and how and where they share what they do are all part of the operations, maintenance and upgrading procedures and processes that must be agreed upon in advance. The additional increase in risk created by devices and systems running on the network rather than their own cabling cannot be underestimated – which is not to assume that anything that runs on its own network is secure.

In many respects, when it comes to smart building systems, maintenance is about keeping them running as they were installed and updating software and security patches as required. It is important to bear in mind that it is not just each system and its software, which need to be kept updated. Each IoT device is itself a computer, which, as it does not have a screen, a keyboard or mouse, is managed by the overall system software. However, as a computer the device has processing and networking capabilities, which means that it is open to attack just like any other computer. It also means that the device may require firmware (operating system) and security updates from time to time.

Smart Building devices and systems may not only connect to the main control system, but also to each other and even cloud-based services. This makes them particularly attractive targets to attackers, who may rely on vendors taking longer than usual to release security updates, but also the enterprise customers who may not install the security updates for several months after they are available.

An important aspect of maintenance and upgrading of SBE devices and systems is improving on a continual basis; the following diagram illustrates steps involved in this. It is outside the scope of this document to delve into this in more detail, although it is a responsibility that facilities professionals or a third party will need to undertake.



Most existing buildings will go through or have gone through stages where they had no smart technologies, to having some smart technology systems, to becoming considered as a complete smart built environment. Wherever an organisation is in its journey, the facilities team is ideally placed to work with colleagues from across the organisation to help establish a baseline from which to move towards a more desirable and mature security state.

3.2.10 Operations, Maintenance and Upgrading Requirements

Req No	Requirement
3.2.10.1	There shall be an up-to-date supply chain register for each SBE and SBI to ensure property managers do not lose sight of their supply chain and that appropriate access control and change controls are applied.
3.2.10.2	Complete the agreed, planned Post-Acceptance service review and where appropriate include the requirements into the regular maintenance reviews:
3.2.10.2.1	Updates to devices, systems, components and software inventory on the network shall be reviewed, in particular identifying changes, unused or redundant devices for removal, etc.;
3.2.10.2.2	changes made to the system configuration and their impact on the initial system security design assumptions shall be documented and any shortfalls mitigated;
3.2.10.2.3	back-up procedures shall be verified for successful completion to ensure they operate correctly during recovery events;
3.2.10.2.4	system event logs shall be checked for evidence of suspicious or abnormal behaviour e.g., multiple failed remote access attempts or excessive transmission faults;
3.2.10.2.5	perceived / observed problems with the software system shall have their root cause identified(as indicators of historic or active sabotage activity);
3.2.10.2.6	the inventory of authorised software applications running on network connected security devices shall be regularly maintained;
3.2.10.2.7	security updates and their successful completion shall be regularly monitored;
3.2.10.2.8	there shall be a process which ensures that there are no devices where the manufacturers' product lifetime support withdrawal is due to end soon and shall include appropriate remedial measures (whether the devices are due to be secured and remain in use or replaced individually or with other devices);
3.2.10.2.9	the application of the identity access management policy, including remote maintenance access, shall be monitored to ensure it is still being applied and current;
3.2.10.2.10	remote users shall be monitored to ensure that they are still current and don't have excessive rights;
3.2.10.3	All health and safety related systems (like HVAC system) shall be maintained according to relevant safety and security regulations and standards, and to escalate any variation from those required levels.
3.2.10.4	For updates and improvements, which require wider ranging changes and or resources, a process should be established that includes an implementation plan and review of the impacts of the improvements.
3.2.10.5	Appropriate audit and reporting arrangements should be established to ensure compliance with all key requirements.
3.2.10.6	A suitable change management process should be created and maintained for SBE and SBI systems and infrastructure.
3.2.10.7	All health and safety related systems (like HVAC system) shall be maintained according to relevant safety and security regulations and standards. Any variations shall be exceed these regulations and standards.

Table 7 Operations, Maintenance and Upgrading Requirements

3.2.11 Protection

The NIST Cyber Security Framework (see Appendix A) outlines a set of activities, or functions, that guide cyber security. One of these is the Protect function, which aims to ensure all assets identified during the preceding Assess (or Identify) function have the required level of protection. Every process discussed so far covers elements of the Assess function apart from the Operations, Maintenance and Upgrading, which has overlaps with this Protection function. Whereas the other topics covered earlier identify what needs to be done, this function actually ensures that it is done. As such, it utilises all the controls required in the above processes. Where the FM team does not understand the controls available to protect devices and systems, it will not be able to effectively utilise all the tools available to do this.

The Protect function, as it relates to smart building devices and systems, involves assessing and understanding the risk to the SBE and SBI, and working with third-party suppliers to deal with those risks. It also involves implementing other controls separate to those the contractor manages, which may include the network and other assets or processes. The network and cyber security teams can help clarify the necessary controls that may be needed and what is available according to the device, system and risk or threat in question. It is not possible to cover them all here.

Unlike the Protect function for the rest of the organisation's infrastructure, which would cover everything from email to user awareness, this function for the SBE and SBI is narrower and easier to identify with the physical security, cyber security and network teams.

Historically, the Protect function used to receive the most attention, resources and investment. This was until cyber security professionals agreed that, with all the will in the world, and no matter how well you think you are protected, threat actors are still likely to get through. Since then, budgets have increased for the Detect, Respond and Recover functions too. The Protect function continues to be important. The focus of investment should respond to the risk across all of the assets (network, devices, users, data or applications), and the other functions.

A key area to focus on as part of this function is the SBI to ensure that is it capable of providing the protection to the organisation and other systems as intended.

3.2.12 Protection Requirements

Req No	Requirement
3.2.12.1	A team shall be established with clear responsibilities for reviewing the risks identified and implementing security of the SBI.
3.2.12.2	Ensure that the solutions the SBI sit and rely on are secure and able to provide the level and types of controls determined in previous processes and documents.
3.2.12.3	Any components of the infrastructure which pose a higher risk than the acceptable documented risk shall be identified, documented. Any risks identified shall be escalated to the organization's Risk Committee.
3.2.12.4	Physical access to system hardware shall be regularly evaluated so that it remains effective, as defined in the organisational cyber and physical security policies and procedures.
3.2.12.5	Standard checklists should be created to support verifying there have been no changes to the initial system software configuration state during installation, commissioning or updating of any system.

Table 8 Protection Requirements

3.2.13 Detection

Even with the adoption of security best practices, procurement processes and controls, it is not always possible to restrict determined, skilled attackers from compromising the building management and connected systems. Therefore, it is important to implement controls which can detect suspicious activity and alert security control rooms or facilities professionals accordingly. Malware often lies hidden for months as the attacker explores the system to decide what is of value and how to get it out. It is important, therefore, to monitor and detect anomalies in real-time to act on any suspicious activity.

There are many technologies which detect events, such as those based on collecting all log files and analysing them, including converged Security Incident and Event Management (SIEM) solutions. SBE and SBI often depend on unique and proprietary systems. Some 'off-the-shelf monitoring tools can cause many false positive reports or ignore network communications issues that may be important with regards to a potential threat. These technologies have improved but unless they are able to provide near real-time analysis, they are only providing a view of what happened in the past, not what is happening right now.

Facilities professionals must be able to use any detection technologies for their smart buildings devices and systems, as they have a different level of understanding, knowledge, skills and competence compared to those professionals in networking and security. If the networking and security teams want to increase the organisation's capabilities, it is in everyone's interest that they up-skill the facilities and physical security professionals and their associated teams (such as HR, Legal and Finance). Doing so without the appropriate training and education may only serve to frustrate everyone.

Such up-skilling approaches are strategic and would need to be incorporated into the governance, risk and compliance approach agreed by the enterprise. By investing in upskilling FM teams, organisations facilitate shared responsibility for the network, devices, users, data and applications. This is beneficial for compliance requirements, especially as the European and UK data protection regulations require data breaches to be reported within 72 hours. Despite this, an attacker can break into a network and undertake reconnaissance for several months before they identify the data they want to extract, and the first sign of the attack may be when data is seen leaving the network. It may be easier for attackers

to evade a single team, which tries to do everything, but with several teams working collectively with defined responsibilities overseeing all key assets/asset groups, this is more difficult.

Working together, the teams need to identify the many detection processes and indicators, which are specific to building control devices and systems.

3.2.14 Detection Requirements

Req No	Requirement
3.2.14.1	The organisation's approach to detecting and monitoring the SBE technologies shall be documented including an inventory of any monitoring of the SBI devices, systems, and solutions in use. This may be in the form of a policy or internal standard.
3.2.14.2	There shall be agreed documented procedures for how detected events are handled in different SBI technologies.
3.2.14.3	The SBI should have the detection tools and capabilities to implement the Cyber Kill Chain to block attacks.
3.2.14.4	All relevant individuals and security team members shall be trained to use the monitoring technologies to provide cover for extreme attacks as well as the "normal" times. The training should include (and document) what is to be considered a false positive or false negative, in which circumstances and when that same noise may need to be considered as an attack.
3.2.14.5	Detection tools and solutions should enable monitoring of all the technologies being protected – otherwise it is not possible to verify that a breach has taken place. Where it is not possible to monitor certain technologies, consideration shall be given to disabling them completely, for example, where there are no tools to monitor Bluetooth activity, disable it from all SBE devices on the whole site, as it is an obvious attack point which is not being monitored.
3.2.14.6	All the technologies being protected shall be monitored in real-time. Where it is not possible to monitor them in real-time consideration should be given to alternative options which should include automated alerts (in as close to real-time as possible).
3.2.14.7	Where real-time detection is not possible and there is to be a reliance on log files, there shall be a process and someone identified to be responsible for reviewing the logs with the regularity determined by the technology, systems, or components used in the SBI. Further, that the people responsible for reviewing the log files, shall have the right tools to analyse the volumes that are likely to be generated not just now but throughout the lifecycle of the current technologies producing the logs.
3.2.14.8	Real-time detection should exist for all communication technologies capabilities available on devices not just for wired networks.
3.2.14.9	Where Wi-Fi is used to connect devices to the network, there shall be tools and capabilities to not only monitor the networks and devices they are connected to, but also to monitor the unauthorised (shadow) networks within the site and connection proximity, for complete visibility of attempted connections and possible attacks.
3.2.14.10	Real time monitoring tools used and emerging technologies should be periodically reviewed, with a view to change/update as necessary to maintain security threat risk at agreed documented levels.

Table 9 Detection Requirements

3.2.15 Response

Not all detected events are security events, and there may be many false positives in the alerts. Equally there may be events which appear to be negative but turn out to be real incidents and require further exploration. The best approach for implementing the response function is similar to the detect function, by sharing expertise, knowledge and skills across the physical, facilities and cyber security

teams. This would ideally be in a converged security team setting but doesn't have to be if the enterprise hasn't adopted that strategy.

A cyber-security incident response playbook, or security playbook, helps to provide building operations stakeholders with a clear understanding of their roles and responsibilities regarding cyber security before, during and after a security incident. A security playbook also defines the Computer Security Incident Response Team (CSIRT) and establishes the contact liaison between the facilities professional's Executive Board and the rest of the incident response team.

The CNS Group writes 'Following the establishment of the CSIRT, an incident response plan needs to be implemented, including a step-by-step guide of key actions to be taken if a security incident has occurred. Investing in a response plan and employee training is a worthwhile investment, which helps to improve an organisation's cyber-security posture. It is important to run practice drills and exercises periodically, so that when an incident occurs, everyone is aware of the role they play, reducing the time to respond and minimising impact' [Ref 21].

In the SBE these exercises could include how to handle communication with tenants, or red-team exercises (which involve an all-out attempt to gain access to a system by any means necessary. Both the facilities and cyber security teams have different but vital response skills and making the best use of them is more likely if they work closely, rather than if they work apart.

The teams need to identify and develop those response plans, which are specific to the SBE and SBI.

3.2.16 Response Requirements

Req No	Requirement
3.2.16.1	A cyber-security Incident response playbook, or security playbook, shall be developed to provide building operations stakeholders with a clear understanding of their roles and responsibilities regarding cyber security before, during and after a security incident and for different attack scenarios.
3.2.16.2	The playbook shall identify the types of incidents to respond to and those which require the C-suite to be notified immediately and any communications with the press by PR.
3.2.16.3	An incident response plan shall be implemented, including a step-by-step guide of key actions to be taken if a security incident has occurred. The response plan should be specific to the SBE and SBI devices and systems.
3.2.16.4	Practice drills and exercises should be conducted periodically, so that when an incident occurs, everyone is aware of the role they play, reducing the time to respond and minimising impact.
3.2.16.5	Such cyber-security exercises should include how to handle communication with tenants, or red-team exercise members, which involve an all-out attempt to gain access to a system by any means necessary.
3.2.16.6	The cyber security team should produce a report for each incident response for senior management within agreed appropriate times which also meets legislative requirements.
3.2.16.7	There should be a lesson learnt process implemented to capture 'lessons learnt' after every practice or real exercise and corrective actions should be incorporated into standard practices.

Table 10 Response Requirements

3.2.17 Business Continuity, Recovery and Resilience

Although the Recover function and Business Continuity are separate topics, as recovery processes are often a subset of business continuity processes, here we have grouped them together for convenience.

As with the other functions, the FM and security teams must agree which processes are specific to building control devices and systems, and how the teams should work together to ensure effective recovery plans.

The Business Continuity Institute describes business continuity as:

"the key discipline that sits at the heart of building and improving the resilience of organisations. It is a tried and tested methodology organisations should adopt as part of an overall approach to managing risks and threats.

Business continuity management identifies an organisation's business priorities and prepares solutions to address disruptive threats. This understanding supports the design and implementation of plans to protect and maintain the key activities of an organisation in the event of any disruption. [Ref 22]."

A complete and effective recovery relies not just on the higher-level documents and collaboration but also on the lower-level joint working that has not been necessary in the past when building systems were not connected to the internet or operating on the network with other systems.

The capability to recover from an incident, such as an attack on a SBE or SBI, and restore normal operations will depend on the robustness of the systems and the abilities of the staff. There are several layers where system resilience can be built-in:

- Firstly, in the manufacturing, where devices and systems are built to be more resilient, such as alarms and monitoring devices which can operate in very high or low temperatures, or centrifuges designed to be unable to exceed safe speeds (as a result of the lessons learned from Stuxnet [Ref 23]).
- Resilience can be designed into the architecture of the systems and infrastructure from the outset or as an upgrade. There are a range of things to consider including mirroring of servers, cloud-based solutions, diversification of networks, automated backup and recovery solutions.
- System resilience through monitoring processes. For example, HVAC systems that are maintained on a week-by-week basis so that if a respiratory condition is diagnosed in staff, they are circulating clean rather than toxic air. Should the system be affected by an attack they need to be configured so that they continue to perform at safe levels. If a system is adversely impacted by an attack, it is important to have procedures and policies in place with real time monitoring details for engineers to repair the system and bring it online quickly.
- System resilience through additional security controls. For example, attackers often try to create access credentials for themselves, so if the system is set to delete any new administrator role created, there is one less thing for the system owner to consider.

There are many challenges with building systems, particularly when there is a mixture of legacy, hybrid and new technologies. For example, when 5G and other more complex communications are added, this means that even small software glitches can slow down a system and affect performance. Having this general oversight is crucial for effective and continued operations. In terms of lessons learned and continued improvement this is where the examples of previous attacks can help in the business impact analysis. This includes understanding what caused the attack and identification of risk treatments; how well did the organisation recover and what can be done to improve the systems and reduce or prevent the likelihood of future attacks?

3.2.18 Business Continuity, Recovery and Resilience Requirements

Req No	Requirement
3.2.18.1	The Business Continuity Management (BCM) standards shall be agreed and documented for the organisation to follow during a business continuity event.
3.2.18.2	A risk assessment of recovery procedures shall be conducted, including an analysis of how improvements can be made to reduce the impact of SBE and SBI attacks.
3.2.18.3	A Business Continuity Management process shall be established which includes formal risk and business impact analysis to identify critical business processes and their key dependencies as related to the SBE and SBI.
3.2.18.4	Appropriate levels of resilience shall be integrated into all SBE and SBI systems, equipment and infrastructure to ensure continued operation of business-critical activities in the event of foreseeable failures or incidents.
3.2.18.5	A backup regime shall be established, which includes off-site backups of all servers and any business critical technical/operational documentation affected by the SBE and SBI. This shall also include servers, applications and IoT controllers or edge devices in relation to any OT systems. This regime shall include documented processes for restoration of SBE systems and data.
3.2.18.6	A shared responsibility matrix shall be developed between the business and all external suppliers responsible for supporting the SBE core IT infrastructure and systems.
3.2.18.7	Master service agreements should be in place with all external SBE suppliers, which includes a data processing agreement, security patching and Service Level Agreements (SLAs).
3.2.18.8	A building specific business continuity plan/ disaster recovery plan shall be created for the SBE. As a minimum it shall be tested annually to simulate responses to various incidents (including cyber and physical security).
3.2.18.9	An SBE and SBI Crisis Management Team shall be trained to lead the response to any emergency or critical systems failure.
3.2.18.10	Real-time monitoring shall be implemented to identify repairs to systems so that they can be brought back online quickly, in the event that a system is compromised.

Table 11 Business Continuity, Recovery and Resilience Requirements

3.2.19 Decommissioning and Disposal

There are many reasons why a building IoT device or system may be decommissioned other than its disposal (termination or replacement due to end of life), including recommissioning at another site. Where relevant, one of the criteria during technology selection may be ease of secure and effective decommissioning of the device or system. Such requirements may include ease of data deletion so that it is unrecoverable and deletion or resetting of system configuration settings (including network access settings). This prevents the device or system from being discovered, removing it when other selected components may also be decommissioned at the same time.

It is important to note that making it easy for customers to be able to transfer ownership or delete data is one of the ETSI EN 303 645 baseline requirements [Ref 31]. In most cases, organisations will have agreed to either dispose of a device or system, or have arrangements for disposal with the third party managing it. Many IoT security standards and frameworks include the disposal end-of-life requirement as a critical final stage of the lifecycle.

The IoTSF Assurance Framework states in section 2.4.12.11 “The supplier or manufacturer of any devices and/or services shall provide information about how the device(s) removal and/or disposal shall be carried out to maintain the end user’s privacy and security [Ref 25].”

3.2.20 Decommissioning and Disposal Requirements

Req No	Requirement
3.2.20.1	A project plan should be established once it has been decided to decommission a system. This plan should include how any required functionality will be provided in the future e.g., commissioning a new system, how any data should be migrated, and a roll back plan should there be any commissioning problems. A final ‘no return’ cut-off date should be agreed for the system being decommissioned.
3.2.20.2	If the device or system is managed by a third party, the project manager should ensure that the party is involved at the appropriate levels so that all data, settings, etc. are considered, as necessary to avoid mistakes. This role should be something that is agreed as part of the contract agreement.
3.2.20.3	Timescales, responsibilities, and processes for any system de-commissioning should be agreed and documented.
3.2.20.4	Any data on existing systems shall be wiped before the system is dismantled. Responsibility for this and the standard to which the data is to be wiped shall be specified and a formal confirmation provided by the contractor once done. Consideration shall be given to spot checks while this process is taking place – there is no substitute for a documented assurance process carried out diligently [Ref 26].

Table 12 Decommissiong and Disposal Requirements

4 Recommendations and CARS Tables

4.1 Using CARS Tables

This guidance details best practice actions and recommendations to help build and maintain a secure environment. To help readers from the facilities profession take practical action each section lists a series of requirements.

For a successful implementation, relevant stakeholders need to understand what their specific role is in relation to any given requirement. To help with this implementation process the IoTSF has created a series of CARS tables. The CARS tables approach was developed by Baz Khinda at Wellingtone. A CARS table identifies the main stakeholder functions that are likely to be involved in implementation and suggests what their specific role is in relation to the recommendation. Then evidence of the mitigations made to address each risk is also recorded.

Readers of this guidance should create their own CARS tables and IoTSF members are encouraged to use the SBE Questionnaire for the recording process.

The following role definitions have been suggested:

C = Communicate – A catch all for both consult and inform to identify anyone who should be communicated with regarding a task, typically an end client.

A = Approve – "As a PM how do I know this piece of work has been completed to the right level of quality"? "Maybe trust the person identified as **R**esponsible, if they tell me it's complete then I'm happy." "Maybe I need to approve that piece of work myself or perhaps a formal approval from a quality inspector, senior manager or group of people is required."

R = Responsible – Just as in RACI tables, this is the person doing the work. "As a PM I want a single person marked down as Responsible". "Who is my point person, who has responsibility for this task?"

S = Support – Often work is not undertaken by just one team member but they might be supported by others. This clarifies the role of other team members as assisting with the task, but not being the named individual who has overall responsibility. In many cases the information security team, cyber-security team, risk team (or someone within any of these teams) provides support to the whole SBE.

Specific roles, titles and structures will vary considerably from organisation to organisation, so it is not possible to be definitive in these tables. Differences will occur depending on a number of factors including:

- The size and complexity of the organisation
- The applicable building occupation model
- The specific organisational structure and allocation of responsibilities
- The extent to which security responsibilities are merged between physical and cyber.

As part of the implementation process, each organisation will need to establish relevant stakeholders and bodies within their own organisations and then allocate CARS functions to them for each recommendation to be adopted. Once key stakeholders have been identified this should be a relatively

straightforward process. One approach would be to bring together all potential stakeholders in a workshop and discuss where responsibilities should lie and agree the way forward.

To assist in this allocation of responsibilities the table shown below has some generic stakeholders identified and examples given for how responsibilities could be allocated.

Security Governance: Requirement:	Board	Security Group	All Security Officers	Cyber & Physical Security Teams	Risk, Procurement and Other Teams
Clear business goals and priorities are set in relation to the Smart Built Environment, its assets and its security.	A	R	S	C	C
A strategic overview on how governance provides the required security activities linked directly to business goals and priorities.	A	R	S	C	C
Ensure that the governance structure provides clear decision-making responsibilities for security risk decisions across the whole organisation and eliminates siloed responses.	A	R	S	C	C
Resources to achieve the security goals have been allocated to manage risk effectively.	A	R	S	C	C
Clear policies, standards and other documentation which specify operational and managerial responsibilities for security decisions have been developed.	A	R	S	C	C
Frameworks and standards to be complied with and the required levels of assurance.		A	R	SC	SC
Clarity on who is responsible and accountable for which systems, processes, and risks across the business. Those who need to be communicated with and involved, have been identified.	A	R	S	SC	SC

Table 13 - Security Governance

5 Appendix A – Relevant Standards

Professional bodies and trade organisations have produced guidance documents and best practice guidelines to assist with unifying processes and optimising the management and maintenance of a Smart Building. The level of compliance to these standards inherently affects the management of cyber-security within facilities management organisations. In addition, there are generic standards and guidelines on secure management of digital information that are applicable to the organisations in charge of managing and maintaining intelligent facilities. The following is a list of directly related IoT security standards and other useful security standards from other domains.

Before exploring any of these, it is important to remind ourselves that many organisations that hold certifications in these standards have been breached. This should serve as a reminder that as useful as these documents are in getting an organisation started in cyber security, they are not to be considered as the be all and end all when it comes to managing risks around any IoT systems or devices.

5.1 IoT Security related Standards and Frameworks

There are many international standards and frameworks that can be used to help organisations understand the risks to IT and information systems. There are others, which are more general and ensure an enterprise-wide view of risk. The following standards are a curated selection of those currently used globally with relevance to the Smart Built Environment. Each merits a far more detailed application of its principles and controls than can be covered here. We do not prioritise importance and commend all for consideration and guidance in this field.

5.2 ISA/IEC 62443

The ISA/IEC 62443 series of standards [Ref 27] were developed by the International Society of Automation committee for industrial automation and control systems security (ISA99 committee). The standards, adopted by the International Electrotechnical Commission (IEC), provide a common language for product suppliers and all other control system stakeholders, as well as a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs).

The primary aim of ISA/IEC 62443 is to deliver secure “by design” and “by default” products. The principles of the ISA/IEC 62443-4-1 standard [Ref 28] define a set of security requirements for projects, including threat modelling and verification of the implementation. This overarching standard defines the selection of technical security requirements based on the type of product and its context of use.

ISA/IEC 62443-4-1 should be considered based on several reasons:

- This standard formalises cyber security management for the complete lifecycle of products.
- It is possible to employ the same principles to secure the product development in both commercial (Industrial IoT) and residential (consumer IoT) segments.
- The process can be certified to ensure a thorough implementation and the IACS industry may require a secure development process to be certified in the future.

The IEC-62443-4-2 standard [Ref 29] in the series (Security for Industrial Automation and Control Systems) provides the cyber security technical requirements for the key components that make up an IACS, specifically the network components, embedded devices, host components and software applications.

The ISA/IEC 62443-3-3 standard [Ref 30] in the series (System Security Requirements and Security Levels), specifies security capabilities that enable a component to mitigate threats for a given security level without the assistance of compensating countermeasures.

5.3 ETSI EN 303 645 – The European Telecommunications Standards Institute

ETSI EN 303 645 – The European Telecommunications Standards Institute (ETSI) created a technology product standard "Cyber Security for Consumer Internet of Things: Baseline Requirements" [Ref 31]. This standard provides basic guidance for organisations involved in the development and manufacturing of consumer IoT on how to implement these provisions. Although the document clearly states, "IoT products primarily intended to be employed in manufacturing, other industrial applications and healthcare are not in scope of the present document", any technical individual can easily surmise that the controls are a good base for any IoT device or service.

5.4 CAPSS (Cyber Assurance of Physical Security Systems)

CAPSS is a programme that has been jointly written by the U.K.'s NCSC (National Cyber-security Centre) and CPNI (Centre for the Protection of National Infrastructure) leveraging the expertise of both technical authorities [Ref 32].

Whilst CAPSS has been designed with critical national infrastructure in mind, property managers of smart buildings can gain assurance on the cyber components of CAPSS assured electronic security products.

The new standard works on a simplified approach, focusing on six main areas: physical security; secure configuration; network security; authentication management (privileges); monitoring, and cloud services. Each of these main areas have specific mitigations specified under three groups: DEV – development mitigations; VER – verification mitigations, and; DEP – deployment mitigations

5.5 Other Related Security Standards

The following is a short list of related widely used standards.

5.5.1 ISO/IEC 27000 Series

The ISO/IEC 27000 series [Ref 33] comprises information security standards published jointly by the International Organisation for Standardization (ISO) and the International Electrotechnical Commission (IEC). The origins of the standard series are over 20 years old and some of the elements have been included or adopted by cyber security frameworks or other certifications.

The series provides recommendations on information security management—the management of information risks through information security controls—within the context of an overall information-security management system (ISMS). The particular relevance to Smart Buildings security management is through the fact that the standards deal with managing risks to information held on similar technologies where some of the controls may be similar. Although there are definitely similarities, the series does not cover technical aspects of IoT devices or systems. This is mostly due to it being an organisational standard rather than a technology standard.

This series of standards is mainly used by large enterprises, as they can be very costly to achieve and maintain for smaller businesses. The advantage of this series, however, is that they either are

mentioned in, or are the basis of, other related frameworks, regulation or legislation. As they are mapped with other existing compliance frameworks, compliance with this standard often means compliance with other standards, frameworks, regulation or legislation.

5.5.2 NIST Framework for Improving Critical Infrastructure Cyber security

The US National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cyber security [Ref 34]: *"Provides a common language for understanding, managing, and expressing cyber security risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cyber security risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cyber security risk across entire organisations, or it can be focused on the delivery of critical services within an organisation."*

The Framework Core provides a set of common activities to achieve specific cyber security outcomes, and references examples of guidance to achieve those outcomes. The main Core Functions are: Identify; Protect; Detect; Respond; Recover. The Functions should be performed concurrently and continuously to form an operational culture that addresses dynamic cyber security risk.

This Framework is included here even though it is one that is often used by businesses wanting to use a formal approach to cyber-security but not take the ISO 27K series certification route. It is an organisational framework that is used by information security teams around the world to manage risk. The Framework is not intended nor created specifically for Property Managers to protect their buildings, its principles for managing risk (just like the ISO 27K series) may be used across the business – similarly, this Framework is an organisational one (not for a product or technology).

5.5.3 Cyber Essentials

The ISO/IEC 27000 series are a very important set of organisation cyber-security standards; however, they may be out of reach for many businesses due to the financial resources required. To overcome this limitation, it is still possible for businesses to demonstrate their commitment to cyber-security by undertaking lower-level organisation cyber-security certifications than the 27000 series of standards. Currently only Cyber Essentials from IASME meets that requirement.

Cyber Essentials (CE) is available as either CE Basic (CE Basic), which is self-certifying, or CE Plus (CE+), which involves a Certifying Body to make an assessment [Ref 35]. CE Basic covers a self-assessment of five groups of controls, which are considered to reduce around 70% of the most common vulnerable areas: firewalls and internet gateways, secure configuration, software patching, user accounts and malware. CE+ involves a technical audit of a business' system to verify that CE controls are in place.

For many Facilities Managers CE is a quicker more cost-effective approach to demonstrating commitment to cyber-security than traditional organisational ISO/IEC cyber-security standards. One of the ways such certifications can be used is that because it is renewed every year, a business can extend it to include other properties as it expands its compliance.

5.5.4 Other Cyber security Domain Standards

- BS ISO/IEC 29100:2011 IT Security Techniques privacy framework [Ref 36], Focused on organisations involved with operation of information and communication technologies, offering services that entail personally identifiable information.
- IET/CPNI Technical Briefing-Resilience and Cyber Security of Technology in the Built Environment [Ref 37], Addresses organisations involved with operation and management of

smart buildings and provides guidance on managing cyber-security threats to smart buildings, based on a set of instructions and relevant case studies.

- PAS 555:2013 Cyber-security Risk Governance and Management [Ref 38], this publicly available specification is focused on cyber-security, including people, process and technology and offers insight into efficient risk identification, management, and mitigation.
- BS 10754-1:2018 Information technology. Systems trustworthiness. Governance and management specification [Ref 39]. It addresses the principles of software trustworthiness, based on measures for governance, risk assessment and management as well as a compliance instruction.
- ISO 19650-5:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management [Ref 40].

5.6 Additional Smart Building Management and Maintenance Guidance

- ANSI/BICSI-007 Design and implementation for intelligent buildings [Ref 41] Addresses commissioning and management procedures of a smart building, including the requirements of networks supporting building services devices. It also includes protocols and instructions for information exchange of building services.
- EN ISO 16484-1 Building automation and control systems project specification and implementation [Ref 42], Provides guidance on developing project documentation, entailing design, installation and commissioning considerations for a Building Automation and control system (BACS) or alternative systems used for the management or operation of a smart building (e.g. BMS).
- EN 50173-6:2018 Information technology – generic cabling systems – part 6: distributed building services [Ref 43], Focused on the cabling systems structure and specifications, it entails considerations regarding the network infrastructure supporting the network building services and their corresponding devices.
- BS EN 50136-1:2012+A1:2018 Alarm systems. Alarm transmission systems and equipment - General requirements for alarm transmission systems [Ref 44] Provides information and descriptions of various concepts related to alarms, alerts, and notifications, assisting organisations in categorisation and management of alarm systems.
- BSIA 210 An installer's guide to Internet Protocol (IP) in the security industry [Ref 45], Addressing baseline considerations associated with the use of an IP network for various smart building systems and devices, including electronic security systems such as video surveillance, etc.
- Cisco Building automation system over IP (BAS/IP) design and implementation guide [Ref 46], Focused on managing building services protocols over an IP network, this document entails useful instructions on the design of active networks, such as switches, firewalls, etc.
- CIBSE Guide H – building control systems [Ref 47], This guide provides information on the control systems used for environmental conditioning plants and the associated networks (IT networks for BMS devices) and integration (full network convergence, interactions, and commissioning). The document also includes useful instructions on the control of various building management systems, with specific attention to HVAC plants.

6 References and Abbreviations

6.1 Organisations

The following organisations are referenced in this document:

BSIA	British Security Industry Association
CISCO	
CPNI	Centre for the Protection of National Infrastructure
ETSI	European Telecommunications Standards Institute
IASME	Information Assurance for Small and Medium Enterprises
IEC	International Electrotechnical Commission
ICO	Information Commissioner's Office
IoTSF	Internet of Things Security Foundation
ISA	International Society of Automation
ISO	International Organization for Standardization
IWFM	Institute of Workplace and Facilities Management
NCSC	UK National Cyber Security Centre
NIST	US National Institute of Standards and Technology

6.2 Definitions and Abbreviations

For the purposes of the present document, the following abbreviations apply:

BACnet	Building Automation and Control Network
BACS	Building Automation and Control System
BAS	Building Automation Systems
BMS	Building Management System
CAPSS	Cyber Assurance of Physical Security Systems
CARS	Communicate, Approve, Responsible, Support
CCTV	Closed-circuit television
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSO	Chief Security Officer

DPA	Data Protection Act
ENISA	European Union Agency for Cyber security
FM	Facilities Management
GDPR	General Data Protection Regulation
HR	Human Resources
HVAC	Heating, Ventilation, and Air-Conditioning
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIC	Industrial Internet Consortium
I/O	Input/Output
IEC	Institution of Engineering and Technology
IoT	Internet of Things
IP	Internet Protocol/Intellectual Property
IT	Information Technology
OT	Operational Technology
PC	Personal Computer
PII	Personally Identifiable Information
PoV	Proof of Value
PM	Project Manager
SLA	Service-Level Agreement
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security

6.3 References

The following references are used in this document:

1. NCSC. Connected Places Cyber Security Principles. Available at: https://www.ncsc.gov.uk/collection/connected-places-security-principles [Accessed 24th February 2023]
2. UK Department of Health and Social Care. “Securing cyber resilience in health and care: October 2018 progress update”. Available from: https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update [Accessed 24th February 2023]
3. ISO. 16484-2:2004 Building automation and control systems (BACS) — Part 2: Hardware Available from https://www.iso.org/standard/29682.html [Accessed 24th February 2023]

4. Matthews, L. *Criminals Hacked A Fish Tank To Steal Data From A Casino*. Available at: https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino/ [[Accessed 24th February 2023]
5. Lindsey, N. "New Kaspersky Report Suggests 4 in 10 Smart Buildings at Risk of Cyber Attack". Available at: https://www.cpomagazine.com/cyber-security/new-kaspersky-report-suggests-4-in-10-smart-buildings-at-risk-of-cyber attack/ [Accessed 24th February 2023]
6. Wellingtone Ltd., Baz Khinda, "Quick Tips The RACI Matrix – Surely CARS is better?". Available at: https://wellingtone.co.uk/raci-matrix-or-cars/ [Accessed 24th February 2023]
7. IETF – RFC 2119 Key words for use in RFCs to Indicate Requirement Levels. Available at: https://www.ietf.org/rfc/rfc2119.txt [Accessed 24th February 2023]
8. ICO. Video surveillance (including guidance for organisations using CCTV) Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-video-surveillance-including-cctv/ [Accessed 24th February 2023]
9. DIN EN ISO 14798. Lifts (elevators), escalators and moving walks - Risk assessment and reduction methodology. Available at: DIN EN ISO 14798 - European Standards (en-standard.eu) [Accessed 24th February 2023]
10. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks. Available at: https://www.iso.org/standard/80585.html [Accessed 24th February 2023]
11. ISO. 31000 Risk management. Available at: https://www.iso.org/iso-31000-risk-management.html [Accessed 24th February 2023]
12. ANSI/ISA-62443-3-2-2020, Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design. Available at: https://www.isa.org/products/ansi-isa-62443-3-2-2020-security-for-industrial-a [Accessed 24th February 2023]
13. NIST. SP 800-30 Rev. 1 Guide for Conducting Risk Assessments. Available at: https://www.nist.gov/publications/guide-conducting-risk-assessments [Accessed 24th February 2023]
14. EUR- LEX. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434 [Accessed 24th February 2023]
15. GOV.UK: Data Protection Act 2018: Available at https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted [Accessed 24th February 2023]
16. ICO. "Penalties". Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/penalties/ [Accessed 24th February 2023]

17. NCSC. “Supply chain security guidance”. Available at: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security [Accessed 24th February 2023]

18. NCSC. “About Cyber Essentials”. Available at: https://www.ncsc.gov.uk/cyberessentials/overview [Accessed 24th February 2023]

19. BSIA “Installation of safety and security systems Cyber-security code of practice”. Available at: https://www.bsia.co.uk/cyspag/ [Accessed 24th February 2023]

20. Cybersecurity Insiders. 2022 State of Security Posture Report [Balbix]. Available at: https://www.cybersecurity-insiders.com/portfolio/state-of-security-posture-report-balbix/ [Accessed 24th February 2023]

21. CNS Group. “Best practises for developing cyber security playbook”. Available at: https://www.cnsgroup.co.uk/docs/default-source/think-pieces/cns_security_playbooks_final.pdf [[Accessed 24th February 2023]

22. BCI “Good Practice Guidelines 2018 Edition”, p 6. Available at: https://www.thebci.org/product/good-practice-guidelines-2018-edition---download.html [Accessed 24th February 2023]

23. NCSC. “Denial of Service (DoS) guidance”. Available at: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection [Accessed 24th February 2023]

24. GOV.UK. Guidance. Code of Practice for Consumer IoT Security. Available at: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security [Accessed 24th February 2023]

25. Internet of Things Security Foundation, IoT Security Assurance Framework Release 3.0. Available at: https://www.iotsecurityfoundation.org/best-practice-guidelines/ [Accessed 24th February 2023]

26. ISO/IEC. 27001 Information Security Management. Available at: https://www.bsigroup.com/en-IL/Information-Security-ISOIEC-27001/ [Accessed 24th February 2023]

27. ISA/IEC. 62443 Series of Standards. Available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards [Accessed 24th February 2023]

28. IEC. Standard 62443-4-1:2018, “Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements”. Available at: https://webstore.iec.ch/publication/33615 [Accessed 24th February 2023]

29. IEC. Standard 62443-4-2:2019, “Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components”. Available at: https://webstore.iec.ch/publication/34421 [Accessed 24th February 2023]

30. IEC. Standard 62443-3-3:2013, “Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels”. Available at: https://webstore.iec.ch/publication/7033 [Accessed 24th February 2023]

31. ETSI. Standard EN 303 645, V2.1.1 2020-06, “Cyber Security for Consumer Internet of Things: Baseline Requirements”. Available at:

https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf [Accessed 24th February 2023]

32. U.K. Centre for the Protection of National Infrastructure, “Cyber Assurance of Physical Security Systems (CAPSS)”. Available at: https://www.cpni.gov.uk/cyber-assurance-physical-security-systems-capss [Accessed 24th February 2023]
33. International Organisation for Standardization, ISO/IEC 27000, “Information technology — Security techniques — Information security management systems — Overview and vocabulary”. Available at: https://www.iso.org/standard/73906.html [Accessed 24th February 2023]
34. National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cyber security”. Available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf [Accessed 24th February 2023]
35. IASME Consortium, “Cyber Essentials”. Available at: https://iasme.co.uk/cyber-essentials/ [Accessed 24th February 2023]
36. ISO/IEC. ISO/IEC 29100:2011 Information technology: Security techniques: Privacy framework. Available at: https://www.iso.org/standard/45123.html [Accessed 24th February 2023]
37. IET/CPNI Technical Briefing, “Resilience and Cyber Security of Technology in the Built Environment”. Available at: https://communities.theiet.org/groups/blogpost/view/297/289/1655 [Accessed 24th February 2023]
38. BSI. PAS 555:2013 Cyber Security Risk - Government and Management - Specification. 2013. Available at: https://shop.bsigroup.com/ProductDetail?pid=000000000030261972 [Accessed 24th February 2023]
39. BS 10754-1:2018 Information technology. Systems trustworthiness. Governance and management specification. Available at: https://shop.bsigroup.com/ProductDetail?pid=000000000030351844 [Accessed 24th February 2023]
40. ISO 19650-5:2020 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling — Part 5: Security-minded approach to information management. Available at: https://www.iso.org/standard/74206.html [Accessed 24th February 2023]
41. ANSI/BICSI 007-2020, Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises. Available at: https://www.bicsi.org/standards/available-standards-store/single-purchase/bicsi-007-iot-intelligent-building [Accessed 24th February 2023]
42. BS EN ISO 16484-1:2010 “Building automation and control systems (BACS) Project specification and implementation.” Available at: https://www.en-standard.eu/bs-en-iso-16484-1-2010-building-automation-and-control-systems-bacs-project-specification-and-implementation/ [Accessed 24th February 2023]
43. BS EN 50173-6:2018 Information technology. Generic cabling systems. Distributed building services. Available at: https://shop.bsigroup.com/ProductDetail/?pid=000000000030365923 [Accessed 24th February 2023]

44. BSI. BS EN 50136-1:2012+A1:2018 “Alarm systems. Alarm transmission systems and equipment. General requirements for alarm transmission systems Standard”. Available from: https://shop.bsigroup.com/ProductDetail?pid=000000000030331087 [Accessed 24th February 2023]

45. BSIA. “Installation of access control systems- using IP technology – a guide” Available at: https://www.bsia.co.uk/zappfiles/bsia-front/pdfs/261%20installation-of-access-control-ip-technology.pdf [Accessed 24th February 2023]

46. Cisco 2008 v8.1, Building automation system over IP (BAS/IP) design and implementation guide. Available at: https://www.cisco.com/c/dam/en_us/solutions/industries/docs/trec/jControls_DIG.pdf [Accessed 24th February 2023]

47. ANSI/BICSI 007-2020, Information Communication Technology Design and Implementation Practices for Intelligent Buildings and Premises. at: https://www.bicsi.org/standards/available-standards-store/single-purchase/bicsi-007-iot-intelligent-building [Accessed 24th February 2023]


IoT
Security Foundation
www.iotsecurityfoundation.org