



# IoT cybersecurity guidelines, standards and verification systems

A CABA WHITE PAPER

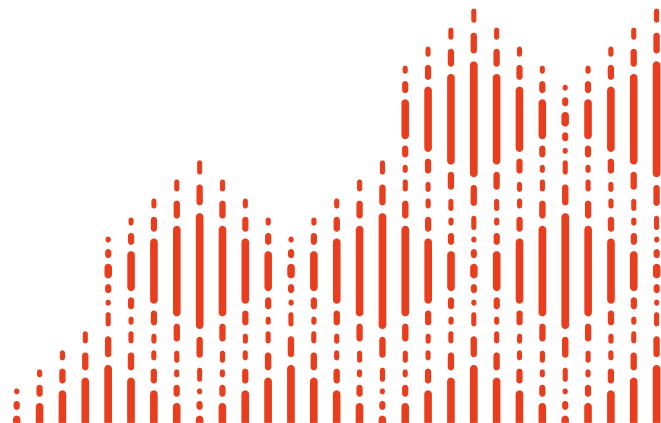
**Faud Khan**  
TwelveDot Inc.

**David Rogers**  
BC Hydro



Connect to what's next™

[www.caba.org](http://www.caba.org)





**IoT cybersecurity  
guidelines, standards  
and verification  
systems**

A CABA White Paper

**Authors**

**Faud Khan**  
TwelveDot Inc.

**David Rogers**  
BC Hydro

**Working Group**

**Amir Shabani**  
George Brown College

**Anne Breene**  
ArcoLogix LLC

**Casey Witkowicz**  
RYCOM Inc.

**Chris Larry**  
exp. US Services, Inc.

**Craig Spiegle**  
AgeLight LLC

**David Katz**  
Sustainable Resources  
Management Inc.

**Glenn Clapp**  
Control4

**Gonda Lamberink**  
UL LLC

**Kenneth Wacks**  
Ken Wacks Associates

**Kevin Woghiren**  
Current, powered by GE

**Marc Lacroix**  
eMcRey

**Ron Bernstein**  
LonMark International

**Steven Snyder**  
Domotz

**Thomas Grimard**  
Syska Hennessy Group,  
Inc.

Working Group:  
Individuals who either  
contributed ideas and  
input into the direction  
of paper or reviewed the  
final draft.

**Sub-Committee****Alex Glaser**

Harbor Research, Inc.

**Brittany Hack**

Consultant

**David Katz**

Sustainable Resources  
Management Inc.

**Derek Cowburn**

LumenCache, Inc.

**Dilip Sarangan**

Frost & Sullivan

**Heather Knudsen**

National Research  
Council Canada (NRC)

**Kenneth Wacks**

Ken Wacks Associates

**Konkana Khaund**

Frost & Sullivan

**Marek Dziedzic**

Public Services and  
Procurement Canada

**Michael Walther**

BeHome247

**Nikiforos Panorios**

Intelligent Buildings  
Europe

**Raphael Imhof**

Siemens Industry, Inc.

**Steve Samson**

Consultant

Sub-Committee: Under the direction of the Sub-Committee Chair, this formal committee reviewed and approved both the initial white paper proposal and final draft.

## ABOUT CABA

The Continental Automated Buildings Association (CABA) is an international not-for-profit industry association, founded in 1988, and dedicated to the advancement of intelligent home and intelligent building technologies. The organization is supported by an international membership of over 390 organizations involved in the design, manufacture, installation and retailing of products relating to “Internet of Things, M2M, home automation and intelligent buildings”. Public organizations, including utilities and government are also members. CABA's mandate includes providing its members with networking and market research opportunities. CABA also encourages the development of industry standards and protocols, and leads cross-industry initiatives. CABA's collaborative research scope evolved and expanded into the CABA Research Program, which is directed by the CABA Board of Directors. The CABA Research Program's scope includes white papers and multi-client market research in both the Intelligent Buildings and Connected Home sectors. [www.CABA.org](http://www.CABA.org)

## ABOUT CABA'S INTELLIGENT BUILDINGS COUNCIL (IBC)

The CABA Intelligent Buildings Council works to strengthen the large building automation industry through innovative technology-driven research projects. The Council was established in 2001 by CABA to specifically review opportunities, take strategic action and monitor initiatives that relate to integrated systems and automation in the large building sector. The Council's projects promote the next generation of intelligent building technologies and incorporate a holistic approach that optimizes building performance and savings. [www.CABA.org/ibc](http://www.CABA.org/ibc)

## ABOUT CABA'S CONNECTED HOME COUNCIL (CHC)

Established in 2004, the CABA Connected Home Council initiates and reviews projects that relate to connected home and multiple dwelling unit technologies and applications. Connected homes intelligently access wide area network services such as television and radio programming, data and voice communications, life safety and energy management/control information and distribute them throughout the home for convenient use by consumers. The Council also examines industry opportunities that can accelerate the adoption of new technologies, consumer electronics and broadband services within the burgeoning connected home market. [www.CABA.org/chc](http://www.CABA.org/chc)

## DISCLAIMER

This White Paper was developed and published by CABA for the industry with permission from the authors. CABA expresses its appreciation to the authors and contributors for making this White Paper available to be included as part of CABA's Members Library and CABA's Public Library. CABA, nor any other person acting on their behalf of CABA assumes any liability with respect to: the use of, or for damages resulting from the use of, any information, equipment, product, method or process disclosed in this White Paper.

This CABA White Paper and other industry research reports can be found in CABA's Members Library and CABA's Public Library at: [www.CABA.org](http://www.CABA.org). This information is also keyword searchable. Contact the CABA office if you do not have the passwords to access this material by email [caba@CABA.org](mailto:caba@CABA.org) or phone 888.798.CABA [2222] or 613.686.1814 (x228). CABA encourages you to share this White Paper with others in your organization and the industry. Permission is not required from CABA to share this White Paper, as long as proper acknowledgment is provided to CABA.

**PUBLISHED**

June 2019

## TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION</b> .....	<b>6</b>
<b>2.</b>	<b>SCOPE</b> .....	<b>7</b>
<b>3.</b>	<b>THE ORGANIZATIONAL APPROACH</b> .....	<b>7</b>
<b>3.</b>	<b>CONSIDERATIONS FOR RELEVANT STANDARDS</b> .....	<b>10</b>
<b>4.</b>	<b>RISK</b> .....	<b>14</b>
<b>5.</b>	<b>STANDARDS SELECTION &amp; BEST PRACTICES</b> .....	<b>15</b>
	Cost factors and considerations .....	17
	Workflow Methodology for Selection .....	19
	<i>Step 1. Requirements</i> .....	19
	<i>Step 2. Supporting Documentation and Shortlisting of Possible Standards</i> .....	19
	<i>Step 3. Perform High Level Risk Assessment and Privacy Impact Assessment</i> .....	20
	<i>Step 4. Weigh Benefits against Risks for Standards</i> .....	20
	<i>Step 5. Short list of standards</i> .....	20
	<i>Step 6. Go/No-Go Standards Selection</i> .....	20
	<i>Step 7. Perform a Technical Risk Assessment and Privacy Impact Assessment</i> .....	20
	<i>Step 8. Record Identified Risks into a Risk Registry</i> .....	21
	<i>Step 9. Implement Controls based on Standard</i> .....	21
	<i>Step 10. Measure Control Implementation</i> .....	21
	<i>Step 11. Monitor Control Implementation</i> .....	21
	<i>Step 12. Archive outputs</i> .....	21
	<i>At End of Project Life</i> .....	21
<b>6.</b>	<b>CERTIFICATION VERSUS STANDARDS</b> .....	<b>21</b>
	Certification Selection .....	22
<b>7.</b>	<b>CONCLUSIONS</b> .....	<b>22</b>

## 1. INTRODUCTION

Currently there is no recognized international IoT cybersecurity standard to which IoT device manufacturers can conform. This leaves manufacturers without a label or customer-facing recognition program that they can leverage to promote their cybersecurity credentials. Recognized organizations such as UL, CSA, ISO, OCF, IEEE and IEC are working in this area, but their approaches differ, and there remains the need to look at the end-to-end solution encompassing the device, its controlling applications and back-end cloud services. Governments are now taking a role in promoting and developing standards, however with the exception of California, legislation seems a few years away.

Starting on January 1st, 2020, the California Bill SB-327 states that any manufacturer of a device that connects “directly or indirectly” to the internet must equip it with “reasonable” security features, designed to prevent unauthorized access, modification, or information disclosure.

IoT devices don't work in isolation; by their very nature they operate in a system that generally utilizes cloud-based servers and multiple third party service providers for connectivity and functionality. This widens the cybersecurity threat exposure to way beyond just what comes in the box when you purchase a new IoT device. Manufacturers are left to wonder where this is all heading, what can I do right now and how can I ensure my design meets an industry standard when no standards apply?

What are some of the main barriers to explain why manufacturers make insecure IoT devices? IoT manufacturers' view of security is often as follows:

- Financial motivation, manufacturers don't prioritize security – it's an after thought
- Competitive edge and speed to market is held back by focus on security
- Security hinders free innovation and innovation hinders security

This paper presents a framework for the cybersecurity standards and considerations that device manufacturers should consider to find the standards and best practices which are most applicable to their product and usage, and how third party accreditation might be applied. This paper will look at the credible actors in this space and compare and contrast their approaches to cybersecurity verification, accreditation or testing.

## 2. SCOPE

This document will provide a device manufacturer a framework to identify the standards and related best practices to consider when designing, building or supporting a device with smart technology typically found in homes and buildings.

Medical devices as well as automobiles are out of scope, as other standards such as UL 2900 for medical and NHTSA, SAE J3061 and Auto ISAC for automobiles may apply and with different regulatory requirements.

## 3. THE ORGANIZATIONAL APPROACH

When looking at security in the cyber age for products, we need to broaden our mindset away from thinking security is an "IT problem" to one that needs both a top-down and bottom-up strategy for implementation. Figure 1 shows how this might be implemented in a typical organization. This approach is applicable to organizations regardless of size or business sector and will ensure that business needs drive a solid security risk management practice.

Security is not complexity, security is a means to manage and mitigate risks. Complexity arise when engineers and product designers don't consider security and then need to bolt on security and privacy solutions - typically with disastrous results. This also correlates to direct and significant costs that could have been avoided.

This approach will help consider costs typically associated with security on the forefront to prevent cost overage and product/solution costs to skyrocket.



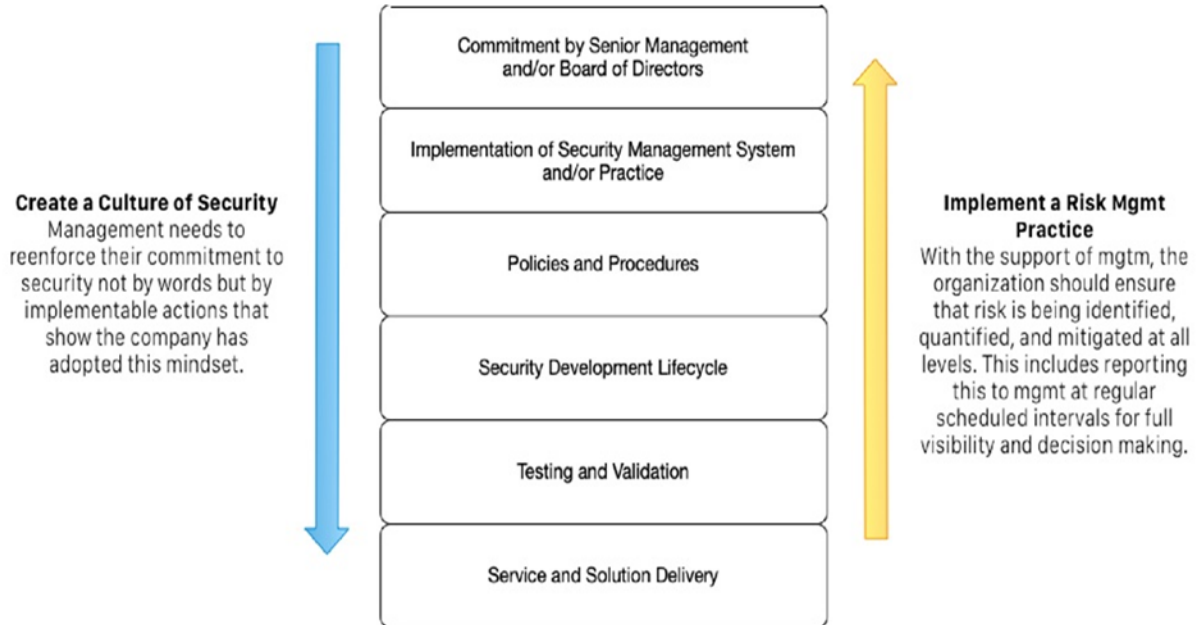


FIGURE 1. ORGANIZATIONAL APPROACH TO CYBERSECURITY

The implementation of a risk management practice will support the following:

- Staff at all levels will understand their role and responsibilities for cyber within the organization;
- The organization will be able to quantify risk for technology related implementations, not just the solutions being created;
- Development costs in the form of security fixes will be reduced as security is integrated from solution concept and not be a "bolt-on" after thought;
- Dealing with security incidents will be better coordinated and understood by all staff, including external third parties who might be necessary in such an event;
- External requirements such as regulatory will be quantified and mitigated from an overall business risk perspective;
- Solutions built by using approaches such Secure-by-Design and Privacy-by-Design to control costs will give quality solutions; and
- Management will understand the overall organizational risk at any given time so both business decisions rely on facts, not assumptions, about security risks both within the organization and in regard to solutions being developed.

## Minimum security and privacy aspects to consider

1. Devices and solutions need be formally tested before release – The solution including the device needs be tested for the presence of known and potential vulnerabilities. For some sectors formal third party evaluations are mandatory.
2. Vendors need vulnerability disclosure processes – The vendor should have a process within the organization that will allow reporting of potential vulnerabilities from third parties as well as the ability to do a vulnerability disclosure in the event that a vulnerability occurs even in their solution.
3. Encryption technology needs peer-reviewed and based on standards – Vendors should never develop proprietary encryption technologies, but use ones that have been peer-reviewed and be based on standards to ensure interoperability. This may include solutions for protecting data communications, but also the boot process and data storage.
4. Solutions should have secure update methods – The vendor should develop a secure method to facilitate updates to the device. This may include checks to ensure that the firmware has not been tampered prior to installation.
5. The vendor needs give specific dates that cover products with full support. Each vendor needs be very clear and concise to the date or period that a product will be support for software updates. When possible, users must be notified that a product has reached its end-of-life for software support.





It is important to note is that standards are based on ‘minimum levels of acceptable safety’, whereas best practices often rely on baselines. Successful IoT cybersecurity practices must relate to and surpass defined minimum levels of safety practices, and not best practice baselines which can sometimes lag behind required levels or are often a moving target for IT based systems.






Privacy concerns relate to the right to use the data and metadata collected from a device or user. These aspects are typically ignored by vendors and many collect “all” data from a device with no consideration to the impact or need to have this data but the thought that it will be important for something.






1. Vendors need to clearly outline their privacy practices. The vendor should give details of data being collected, processed, and stored for service users. This includes data breach protocols and third parties that provide this data for free or as a revenue stream for the organization.

### 3. CONSIDERATIONS FOR RELEVANT STANDARDS

Table 1 lists current standards or guidelines/programs related to cybersecurity applicable to IOT devices. For reference many standards cover the steps outlined above for implementation guidance.

Category	Standard/Best Practices	Guidance	Pros/Cons
<b>Security Management</b>			
	<a href="#">ISO/IEC 27001:2013 &amp; ISO 27002 Information Security Management Standard</a>	Information security management system requirements	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provide a good foundation for a risk management practice organization wide</li> <li>Globally recognized</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Company needs be a base level of maturity to consider</li> <li>Can be costly to carry out controls</li> <li>Training and awareness company wide and on a regular basis.</li> </ul>
	<a href="#">ANSI/ISA 62443-2-1:2009</a>	Elements of a Cybersecurity Management System (CSMS)	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provide a good foundation for a risk management practice organization wide</li> <li>Globally recognized</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Company needs be at a base level of maturity to consider</li> <li>Can be costly to carry out controls</li> <li>Focus on product organizations</li> </ul>
	<a href="#">International Electrotechnical Commission (IEC) 62443-2-1 Industrial Network and System Security</a>	Provides security management as risk recognition/analysis, risk reduction, risk monitoring, and improvement	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provides a good foundation for product organization</li> <li>Globally recognized</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Company needs be at a base level of maturity to consider</li> <li>Can be costly to carry out controls</li> <li>Focus on product organizations</li> <li>Focuses on the industrial sector</li> </ul>
	<a href="#">CSA: T-200 Cybersecurity Verification Program</a>	Bi-National Cybersecurity Standard for Organization Security	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provide a maturity-based approach to implementing security controls for any product organization</li> </ul>

		Maturity and Secure Product Development	<ul style="list-style-type: none"> <li>Can be used on organizations of any size</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Company needs be at a base level of maturity to consider</li> </ul>
<b>Secure Product Design and Development</b>			
 <p><b>OWASP</b> Open Web Application Security Project</p>	<a href="#">OWASP Security Knowledge Framework</a>	Security by design with functionality in OWASP Security Knowledge Framework	<b>Pro</b> <ul style="list-style-type: none"> <li>Good set of controls for product development</li> <li>Globally recognized</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>No audit mechanism for controls</li> <li>Implementation is potentially subjective</li> <li>No third party support</li> </ul>
 <p><b>ASCI</b> Automation Standards Compliance Institute an ISA organization</p>	<a href="#">IEC 61508-3: 4.3.2. bDO-178B: 11.10.b &amp; ISO/IEC 15408-3: ADV TDS.1.1D</a>	ISA Requirements-Security Development Lifecycle Assurance (SDLA) Certification	<b>Pro</b> <ul style="list-style-type: none"> <li>Provide a good foundation for a SDLC implementation</li> <li>Globally recognized</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Requires specific skill set</li> <li>Can be costly to carry out controls</li> <li>Focus on product organizations</li> </ul>
 <p><b>CSA GROUP™</b></p>	<a href="#">CSA: T-200 Cybersecurity Verification Program</a>	Bi-National Cybersecurity Standard for Organization Security Maturity and Secure Product Development	<b>Pro</b> <ul style="list-style-type: none"> <li>Provide a maturity based approach to implementing security controls for a SDLC implementation</li> <li>Provides guidance on best practices</li> <li>Can be used on organizations of any size</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Company needs be at a base level of maturity to consider</li> <li>Needs staff with cyber skills</li> </ul>
 <p><b>NIST</b> National Institute of Standards and Technology U.S. Department of Commerce</p>	<a href="#">NIST Cyber Security Framework v1.1</a>	This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk	<b>Pro</b> <ul style="list-style-type: none"> <li>Aligns to controls used in ISO cyber standards</li> <li>Provides guidance on best practices</li> <li>Can be used on organizations of any size</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Regionally focused for US market</li> <li>Needs staff with cyber skills</li> </ul>
<b>Risk Management</b>			
 <p><b>enisa</b></p>	<a href="#">ICT Procurement Security Guide</a>	Security objectives need be understood & integrated by the vendor	<b>Pro</b> <ul style="list-style-type: none"> <li>Provide a guideline for purchasing products based on security features</li> <li>Can be used on organizations of any size</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>Difficult for vendor to prove compliance to guide</li> <li>Used primarily in the EU</li> </ul>

	<a href="#">ISO/IEC 27005:2011</a>	ISO 27005 international standard guidelines for IT risk management	<b>Pro</b> <ul style="list-style-type: none"> <li>▪ Provide a proven method to deploy a risk management process within an organization</li> <li>▪ Can be used on organizations of any size</li> <li>▪ Globally recognized</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>▪ Company needs be at a base level of maturity to consider</li> <li>▪ Should be part of an ISMS implementation</li> </ul>
<b>Incident Response</b>			
	<a href="#">NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security</a>	Good security program quickly recover the system after an incident has occurred	<b>Pro</b> <ul style="list-style-type: none"> <li>▪ Provides a detailed method to carry out an incident response program</li> <li>▪ Can be used on organizations of any size</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>▪ Requires specific security skill sets</li> <li>▪ Needs to have a basic level of process procedures implemented company wide</li> <li>▪ Regional standard</li> </ul>
	ISO/IEC 27035:2016 Information security incident management -- Part 1: Principles of incident management	Detailed guidance on implementing and managing a cyber incident response process	<b>Pro</b> <ul style="list-style-type: none"> <li>▪ Provides detailed methods to carry out an incident response program</li> <li>▪ Can be used on organizations of any size</li> <li>▪ Globally recognized</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>▪ Requires specific security skill sets</li> <li>▪ Needs to have a basic level of process procedures implemented company wide</li> </ul>
<b>General/IoT</b>			
	<a href="#">UL 2900-1: Standard for Cybersecurity Network-Connectable Products, Part 1: General Requirements</a>	Standard applies to network-connectable products & tested for vulnerabilities	<b>Pro</b> <ul style="list-style-type: none"> <li>▪ Provides detailed methods to check connected type products</li> <li>▪ In-depth assessment</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>▪ Needs to have a basic level of process procedures in place for SDLC</li> <li>▪ May need specialized skill sets</li> <li>▪ Can be costly</li> </ul>
	UL IoT Security Rating	Security best practices providing an IoT Security Rating and product security labeling	<b>Pro</b> <ul style="list-style-type: none"> <li>▪ IoT Security Rating Levels can be leveraged for security differentiation</li> <li>▪ Lower price point than UL 2900-1</li> </ul> <b>Cons</b> <ul style="list-style-type: none"> <li>▪ Is not a standard</li> <li>▪ Relies on vendor to decide on level of security</li> </ul>







	<a href="#">CSA: T-200 Cybersecurity Verification Program</a>	Bi-National Cybersecurity Standard for Organization Security Maturity and Secure Product Development	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provide a maturity based approach to implementing security controls for a SDLC implementation</li> <li>Provides guidance on best practices</li> <li>Can be used on organizations of any size</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Is an emerging standard</li> <li>Company needs be at a base level of maturity to consider</li> <li>Needs staff with cyber skills</li> </ul>
	<a href="#">EDSA-100 ISA Security Compliance Institute – Embedded Device Security Assurance</a>	Focuses on security of embedded devices & supplier practices for those devices	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provides a detailed methods to implement security controls for embedded solutions</li> <li>Globally recognized</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Can be costly</li> <li>Requires specialized security and engineering skills</li> </ul>
	<a href="#">IOT Alliance of Australia: Internet of Things Security Guidelines</a>	Purpose of to promote a ‘security by design’ approach to IoT for security and privacy for IoT device use	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provide a detailed methodology to designing and building a secure IoT solution.</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Specific security skillsets will be required</li> <li>Focused on Australian market</li> </ul>
	ISO/IEC 15408-1:2009 Evaluation criteria for IT security -- Part 1: Introduction and general model	To give a level of security assurance of a specific product, configuration and software revision	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provides detailed methods to assess products and providing a level of assurance for operating environments</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Requires specific security skill sets</li> <li>Can be cost prohibitive for SMB's</li> </ul>
	ISO/IEC 15045-3-1: HES gateway  ISO/IEC 15045-3-2: HES Gateway Privacy Framework	Home Electronic System (HES) guidance on a gateways and privacy	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Offers constant real-time end point intrusion and threat intel.</li> <li>Includes interoperability</li> <li>Sets IoT authorization, management of privacy and security mechanisms</li> <li>dashboard for user access, and other firewall functions</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Likely requires beta piloting</li> <li>Likely slows down bandwidth</li> <li>Standard is under Development</li> </ul>
	UK Code of Practice for Consumer Internet of Things (IoT)	Provide guidance for controls for consumer products and guidance on secure-by-design approach for this class of products	<p><b>Pro</b></p> <ul style="list-style-type: none"> <li>Provides a good resource for SBMs to develop secure IoT solutions for no cost</li> </ul> <p><b>Cons</b></p> <ul style="list-style-type: none"> <li>Focused on UK market but controls are universal</li> <li>No certification or attestation scheme</li> </ul>

TABLE 1 CURRENT CYBERSECURITY STANDARDS/PROGRAMS

## 4. RISK

When considering standards either for the organization or the products/solutions being developed the following questions need to be considered. The approach of selecting a standard to adopt should again be based on a risk-based approach to business. It needs to be considered as a requirement and be inclusive of your overall business plan, encompassing all aspects of the standard applicable to the business.

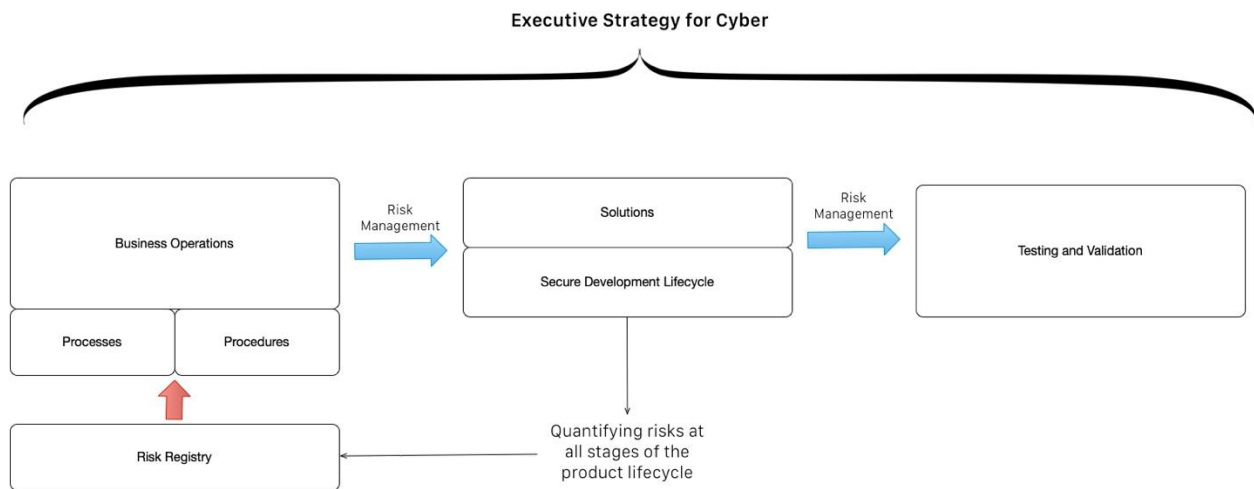


Figure 2: Executive Strategy for Cybersecurity

The age of an organization will typically drive the level of maturity of the process and procedures that have been developed and implemented. Regardless of the current maturity level, your striving for improvement will be critical to implementing risk management practices for both the organization and solutions being developed. However, having a means to balance these inputs will aid in creating a culture of security which will result in more secure products and better cost-effective and secure design. These aspects are outlined in the above Figure 2: Executive Strategy for Cybersecurity.

The process will always begin with a requirement. The requirement needs to be driven by; the customer, a partner, R&D, regulatory compliance or even a combination of these. Regardless of where it originates it needs to be documented, quantified, and mitigated at some level that is acceptable to the organization. This will document the company's approach to addressing the risk. This requirement might be targeting a project or technology not just a single feature within in a product.



Potential trade-offs during this process need be considered as well. These cover a range of issues but when evaluating the need to adopt the standard you need to consider the following:

- a. What impacts will these features have to potential revenues or market share of the solution? What happens if not implemented?
- b. From a competitive perspective, will adding this feature offers a means for the solution(s) to stand out in the market?
- c. Cost of implementation of the standard, will the solution need to be completely architected for implementation? If so, what is payback period on the project expenditure? Is a customer willing to help pay some of these costs?
- d. Will exposing the solution bring increased risk to customers? If so, what are the potential ramifications if the “worst case” situation occurs?
- e. Will this standard offer a means for solution assurances to the buyer?
- f. Will this standard have applicability globally or just in a single region?
- g. What is the future life of this solution? How will technology advancements affect these product risks?

When selecting a standard one of the critical areas of consideration is jurisdiction of the standard. For example, if you adopt a standard in a specific region but want to expand sales to another area you should consider the potential costs of making the necessary changes to meet the requirements of both markets.

The other aspect to consider is the level of assurance that a standard will bring to both the organization and solutions being developed. If it is fundamentally changing these solutions the options needs be re-evaluated.

## 5. STANDARDS SELECTION & BEST PRACTICES

Table 2 provides details to standards classes and when to consider them including potential costs. After this a workflow is provided that details a methodology that can be used to select and implement standards within the organization.



<b>Standards classes</b>	<b>When to consider</b>	<b>Who should consider it</b>	<b>Potential Costs</b>
Security Risk Management	To give assurance to the organization has a method to find and mitigate cyber risk in business operations including services solutions	Any organization regardless of sector but it may include vendors, integrators, VARs. If looking to go international with products should select an ISO or IEC based standard	\$100,000+ depending on the current level of process maturity and implementation of controls
Secure Product Design and Development	To give a level of assurance that implemented development process has the necessary controls to find and mitigate cyber threats	Product developers, service providers, and vendors	\$25,000+ depending on current implemented development process and procedures. Training costs will need to be considered for all staff
Risk Management	Establishes assurance for methods to quantify risks	Any organization looking to make sure that risk is managed across both the product	\$50,000+ depending on the process implementation, systems deployed and training for staff
Incident Response	Establishes assurance for methods to deal with security incidence	Any organization looking to carry out an end-to-end cyber response process	\$25,000+ depending on process implementation, size of organization, training, and system/tool deployment
General/IoT	Many other standards may supplement other standards used within an organization. Their selection needs be based on specific requirements from either a regulatory or customer specific project	Any organization looking to bolster their current security position. Organizations should consider implementing other standards before implementing to help create a framework in place that will aid in decision making process for selection	\$100,000+ depending on current standards frameworks deployed and that can be leveraged

TABLE 2 STANDARDS CLASSES

For IoT vendors in North America, the key issue facing them is which standards will become legally binding codes. At this time, we are only aware of one which is the California Senate “SB-327 Information privacy: connected devices”. This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

However two fairly new standards are very likely to enter codes, at the national standards level and these are:

1. UL 2900-1 USA Certification Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
2. CSA T-200-CVP Canadian Certification Standard for Evaluation of Cybersecurity for Endpoint to Endpoint Connected Devices

Once these two standards above become legally binding codes IoT vendors may be liable for damages from cybersecurity incidents if found to be non-compliant.

### Cost factors and considerations

When looking at the overall cost of implementing a standard or certification there are costs associated that may include some of the following:

- a. Hiring consultants and/or external third parties with skills in implementing a standard;
- b. Costs to carry out controls that might range from purchasing software, hardware, resource time to implement, and support costs for these;
- c. Current company maturity for process and procedure will also be a consideration as it may dramatically increase the costs related to external third party support;
- d. Training of staff for new tools and technology, process, and procedures that must now be followed;
- e. There will be project management and related costs for internal resources to dedicate to these new controls;
- f. Cost of required assessments;
- g. Costs of the required audits;
- h. Costs of certification, which vary by the certification and effort;

- i. Software development;
- j. BOM costs e.g. hardware security modules, retooling and keys/certificates; and
- k. Performance implications (battery life, latency, etc.).

When factoring aspects of your decision these cost aspects need to be considered in-depth as they will have direct impact to the length of time that it will take to implement the standard.

The two emerging IoT Cybersecurity Standards slated to become National Codes in North America use two uniquely different approaches. Whereas the UL 2900-1 standard applies a broad range of penetration tests the Canadian T-200 applies penetration tests, only tailored to the unique features of each end-point to end-point IoT system. This tailoring is determined by T-200's exhaustive site audits covering six key Domains of Cybersecurity focus. The complexity and number of penetration tests of the UL 2900-1 certification tests are reflected in their certification costs being higher than for the T-200 tailored penetration test certification costs.

## Workflow Methodology for Selection

Figure 3 illustrates the workflow process to see whether you need a standard. The following provides each process aspect in detail.

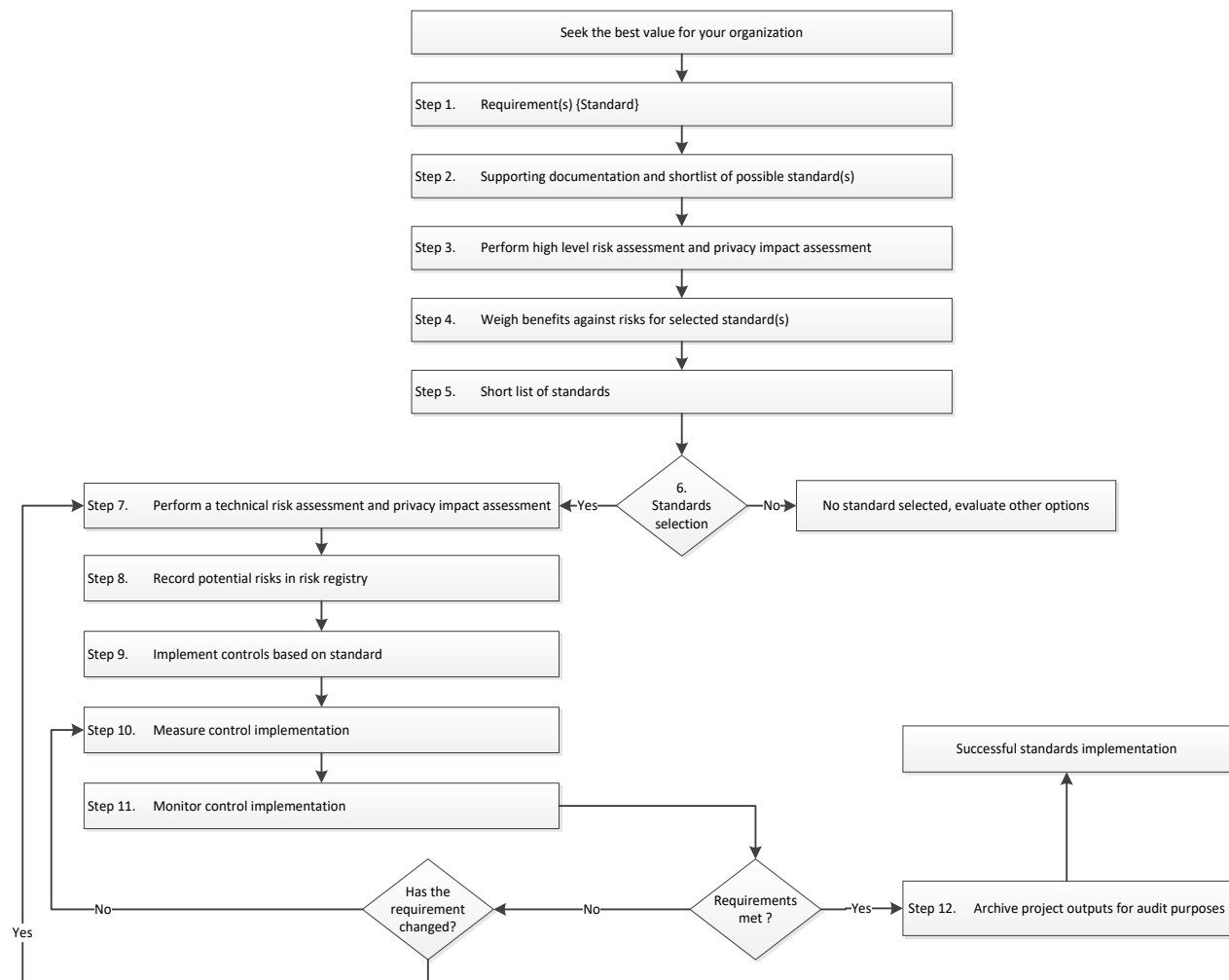


Figure 3: Methodology for Selecting a Standard

### Step 1. Requirements

This process needs always begin from an executive decision. This will result in the security risk management being driven via a project management framework to track each of the follow related tasks. This will typically start with a project kick off (brain-storming session) to identify and list the essential requirements.

### Step 2. Supporting Documentation and Shortlisting of Possible Standards

Once this initial shortlist is created, the focus will shift to collecting and developing the supporting documentation including the possible standards.

### ***Step 3. Perform High Level Risk Assessment and Privacy Impact Assessment***

At this point, the organization needs to carry out high level risk assessments for the standard being considered and a privacy impact to see if any data collected is personally identifiable information (PII). If so, what and how is that going to be collected, processed, stored, and/or destroyed needs to be understood.

### ***Step 4. Weigh Benefits against Risks for Standards***

There are many considerations for the cost/benefit analysis, these include:

- a. Cost – What is the cost to get the standard implemented including 3rd party support, cost to delivery to other projects, evaluation and certification costs?
- b. Resource Impact – Will this impact your overall ability to deliver your core services and/or solutions?
- c. Time – How much time will this consume? How will this impact other projects during the same time period?
- d. Maintenance – How will your organization continue to make sure that aspects of the standard are maintained over the length of the product? What kind of product support, warranty and service will be required?
- e. Jurisdiction – You should ask if the standard recognized in the geographic sales area of your product. If it is not, you need to consider an alternative standard or a pathway for equivalency.

### ***Step 5. Short list of standards***

Based on the earlier steps you are now in a place to derive a short list of potential standards that would apply to your requirements.

### ***Step 6. Go/No-Go Standards Selection***

A formal internal review needs be conducted at this point to decide whether the organization is committed to implementing or conforming to the standard(s) and/or solution.

### ***Step 7. Perform a Technical Risk Assessment and Privacy Impact Assessment***

Once the decision is made to adopt a specific standard a full and in-depth technical risk assessment needs be performed to benchmark the current state of security and how correction controls will mitigate these risks outlined previously. This applies to a privacy impact assessment for the data being collected.

### *Step 8. Record Identified Risks into a Risk Registry*

Based on the two risk assessments performed above (Technical Risk and Privacy Impact) the identified risks need be tracked in a risk registry along with task leads, target completion dates, and identified mitigation action.

### *Step 9. Implement Controls based on Standard*

Use the standard to carry out the necessary control(s) into the solution for the organization.

### *Step 10. Measure Control Implementation*

For each control deployed, validate and document that the control has been properly implemented and the risks mitigated. This will typically be confirmed via testing and validation but may include working data collection aspects as well.

### *Step 11. Monitor Control Implementation*

Implement the necessary key performance indicators (KPIs) and other processes to continue to measure the controls in practice. These should include a process to find and mitigate failures in field.

### *Step 12. Archive outputs*

Archive relevant information on testing and controls monitoring for audit purposes.

### *At End of Project Life*

Once the solution reaches end-of-life make sure all project data is securely stored and/or destroyed as required. Regulatory requirements may determine when the product reaches end of life and govern audit evidence of this projects and data destruction.

## 6. CERTIFICATION VERSUS STANDARDS

When considering your options (Certification or Standards) the key differentiator between the two approaches is that until standards are incorporated into codes they are typically voluntary and offer the guidelines for controls. Where for the most part, certification is a mandatory for specific products in specific categories. This might even be a requirement within certain geographies that products/solutions need to undergo certification before market release.

While security standards may exist, currently many do not have a formal assessment mechanism to give assurance that the controls meet the standard.

The implementation is completely subjective to each organization. Standards such as ISO 27001 do offer a means for certification which includes regular formal audits and organizations must show how they comply. However, the inherent cost to carry out this framework of audits is also substantially higher.

### Certification Selection

Finding an appropriate certification will apply the same selection process described above for standards. The big difference is the cost of implementation and use or external third parties that might be required to carry out, verify, and document the required evaluation for the certification. This will include regular testing and evaluation by the certification authority. Certification needs be considered for specific product sectors and might be mandatory in specific jurisdictions globally.

In some situations, certification costs are often significant and the organization must weigh the cost and benefit and potential new market expansion and projected revenues to the cost required for compliance.

## 7. CONCLUSIONS

While the choices of standards and certifications are many and customers will each have different requirements for security controls, creating a well thought out evaluation process will help define the right strategy, based upon the market forces and business outlook. Security requirements are being increasingly demanded by many customers and in some cases mandated in many sectors such as the utility sector under NERC Compliance. The ability to quickly find which ones to consider will have impacts on your business and in the markets where your products might be sold.

This guide provides a method which covers all relevant aspects and issues from the beginning of the selection process to the necessary ongoing maintenance. The successful choice and implementation of the standard will make sure the best and most cost-effective and competitive advantage is provided for products and organizations. This may in turn improve intangible assets by improving consumer confidence for marketing and reducing risk of litigation for misuse of IoT products.

Looking ahead to the near future, the bottom line for all IoT vendors is that unless they comply with emerging national cybersecurity standards now, they put themselves at risk for potential legal liabilities. The market will decide which of the two Standards UL 2900-1 or T-200 will enter code across North

America.





© CABA 2019

888.798.CABA (2222)

613.686.1814 (x228)

Connect to what's next<sup>™</sup>

[www.caba.org](http://www.caba.org)

