

Taming the Cyber Security Wicked Challenge

Semicon Europa 2024



John.moor@iotsecurityfoundation.org

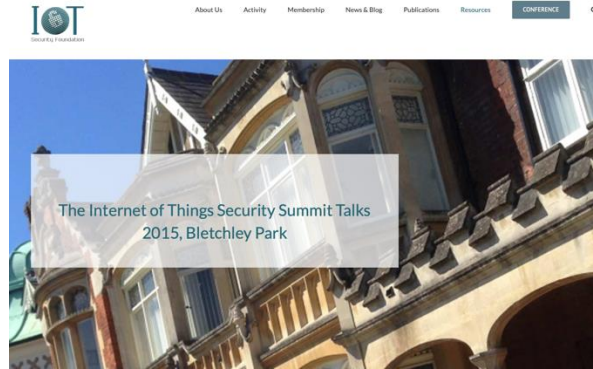
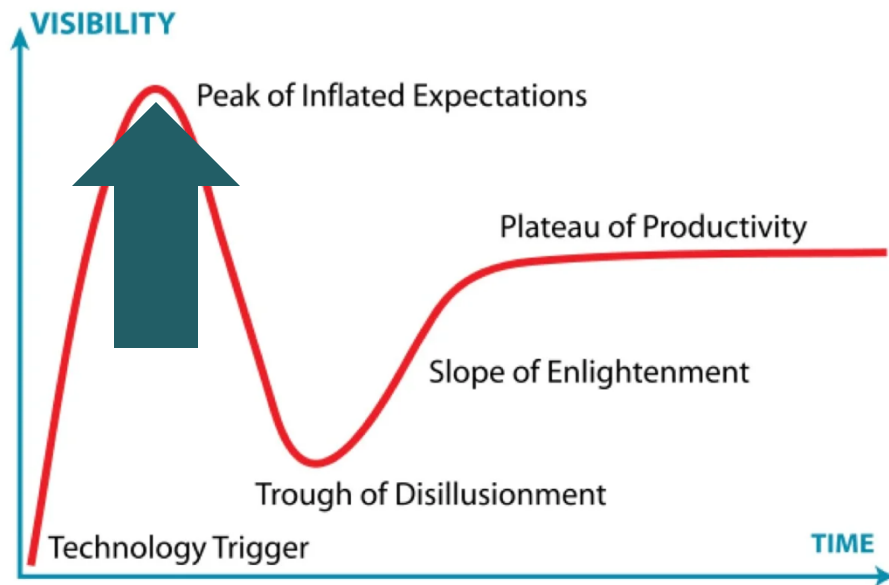
IoTSecurityFoundation.org



History: 2015/16 IoT security status 'egregious'



Gartner Hype Cycle



Anonymous hacker claims he broke into wind turbine systems

Fiat Chrysler recalls 8,000 more Jeeps over wireless hacking

Army of webcams used in net attacks

29 September 2016 | Technology

Our insecure Internet of Things is becoming terrifying

By Graham Templeton on September 8, 2015 at 8:37 am | 19 Comments

New, more-powerful IoT botnet infects 3,500 devices in 5 days

Discovery of Linux/IRCTelnet suggests troubling new DDoS menace could be worse

DAN GOODIN - 11/1/2016, 9:15 PM

Cyber criminals hack a REFRIGERATOR: Will the 'Internet of Things' create a new bot army for the spammers?

Lazy IoT, router makers reuse skeleton keys over and over in thousands of devices – new study

SSH logins, server-side HTTPS certs baked in firmware



TECHNOLOGY NEWS | Tue Oct 4, 2016 | 8:58pm BST

J&J warns diabetic patients: Insulin pump vulnerable to hacking

News > World > Americas

Hacker takes control of Ohio couple's baby monitor and screams 'bad things'

Multiple Backdoors found in D-Link DWR-932 B LTE Router

Wednesday, September 28, 2016 | Swati Khandelwal

IoT vulnerabilities and exploits dominate the news headlines

'we cannot carry on like this'
'you will get hacked'
Something needs to be done to protect users

Manufacturers must do better



Introducing the Internet of Things Security Foundation

Beyond the horror stories: the IoT Security Foundation was launched on

Sept 23rd 2015 in response to wide-ranging security concerns from IoT stakeholder groups

Make it Safe to Connect



Epiphanies of the Obvious:

- Security the same as Safety?
 - Constantly moves
 - Certification limited / Continuous Assurance
- Enemies of security - the 3 C's
- Cost, Complexity, (In)Convenience

Our
Founding
Values



SECURITY FIRST

Designed in at the start

FIT FOR PURPOSE

Right-sized for application

RESILIENCE

Through operating life

How does the IoTSF help?



- Focal point for best and next practices since 2015
- Range of Best Practice Guides & Whitepapers covering
 - Secure Design
 - Vulnerability Disclosure
 - Software Bill of Materials
 - Supply Chain Security
 - Smart Built Environment
 - Next Gen Router and Network Security
 - ManySecured.net
 - Engineering Trustworthy AI
 - TechWorksAI.net



• Class leading Security Assurance Framework

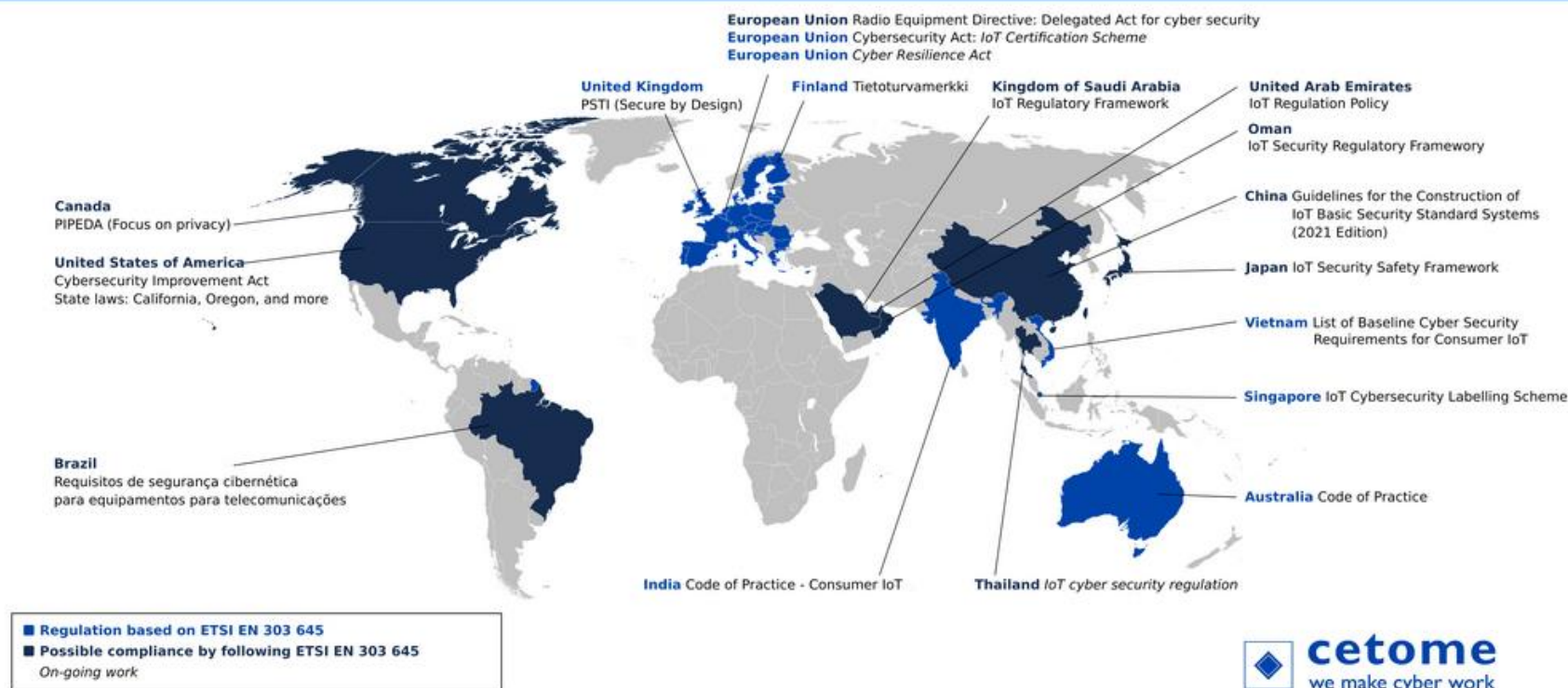
2.4.3 Business Security Processes and Responsibility								
Req. No	Requirement	Guidance	ETSI	NIST	ENISA best practices	Compliance Class and Applicability	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy.					Mandatory for all classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance framework process.					Mandatory for all classes	Business	Responsibility
2.4.3.3	Intentionally left blank to maintain requirement numbering							
2.4.3.4	The company follows industry standard cyber security recommendations.	Such as: UK Cyber Essentials, NIST Cyber Security Framework, ETSI EN 303 645, 50177005.				Mandatory for all classes	Business	Policy

Global Cyber Requirements



Oct 10, 2024

IoT Cyber Security Regulations across the world



European Council
Council of the European Union

[Home](#) > [Press](#) > [Press releases](#)

Council of the EU | Press release | 10 October 2024 13:30

Cyber resilience act: Council adopts new law on security requirements for digital products

The Council adopted today a new law on cybersecurity requirements for products with digital elements with a view to ensuring that products, such as connected home cameras, fridges, TVs, and toys, are safe before they are placed on the market (**cyber resilience act**). The new regulation aims to fill the gaps, clarify the links, and make the existing cybersecurity legislative framework more coherent, ensuring that products with digital components, for example ‘**Internet of Things**’ (IoT) products, are made secure throughout the supply chain and throughout their lifecycle.

Reference: cetome, Panorama of IoT Cyber Security Regulations Across the World.

<https://cetome.com/panorama>

12/11/2024

IoTTF @ Semicon Europe, 12th November 2024 – Munich, DE

Fit for the Future Assurance



- Pre-standards, pre-compliance
 - The world changes constantly
 - Foundations need to be firm

Print version: 15k+ downloads



- In the Future, how do we evolve?
 - Collaboratively Maintain, Update and Map Requirements

For Framework Users MARKET READY

- Lifecycle Tool: From developer audit to conformance teams
 - Simple, low cost, do once
 - Process guidance and better tooling
 - Application adaptable
 - Market Ready: Downstream interoperable with certification schemes and global legislation requirements

ANNOUNCEMENT: We have to *'Go Digital'*

- **Fit for purpose NOW, fit for the FUTURE.**

Let's start with a question



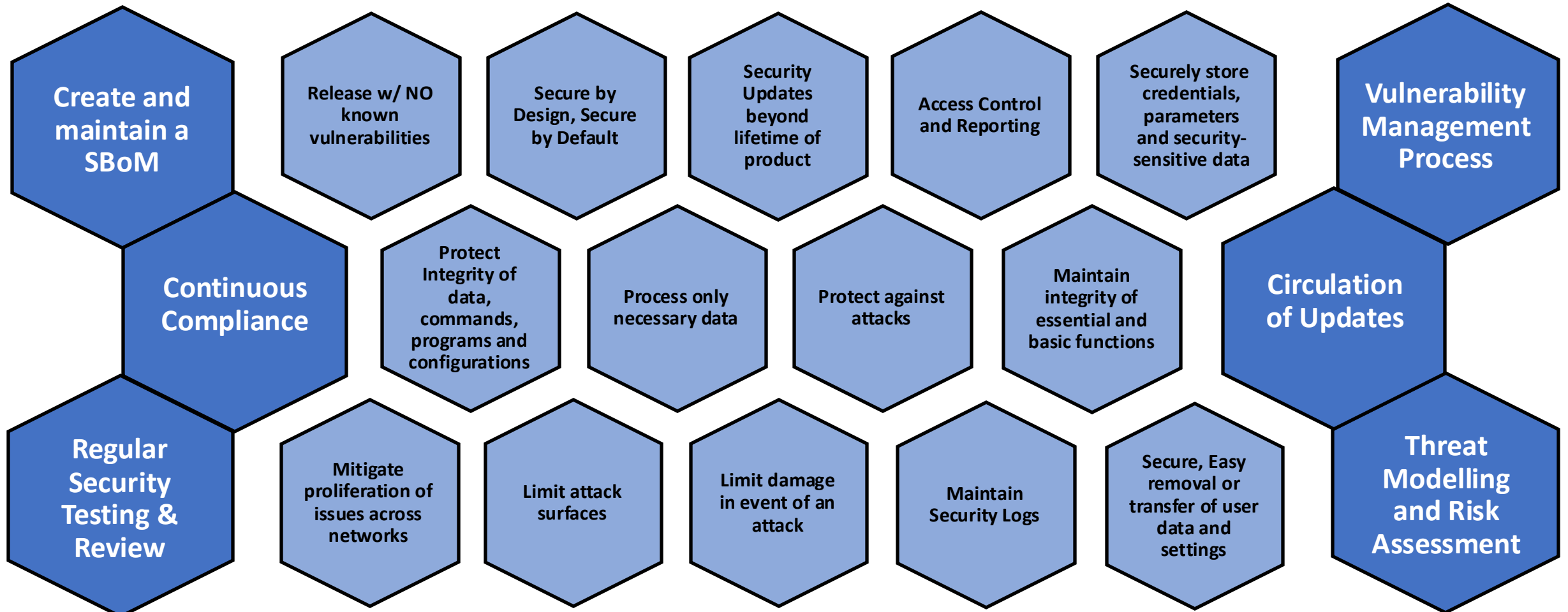
Q - Do Cyber Regulations present a significant change in design requirements and methods for product creators?

Let's start with a question



- Cyber Regulations present challenges in product design and methods
 - Improved planning, addressing cyber impacts over the entire product lifecycle
 - Long term support
 - Continuous integration with compliance testing
 - Rigorous documentation and reporting
 - Account for penalties and liabilities in event of compliance failures
- Requires phase shift in how we approach product development and management

Essential Requirements and Processes



Business/Design Impact



Business	Design	Market
• Cyber Security Culture • Mindset • Leadership • Full lifecycle Audit Trail • actions • changes • issues • Security Updates • Guaranteed period • Free of Charge	• Methodologies • Secure-by-Design • Meet product security legislation requirements • Full lifecycle • Threat Modelling and Risk Assessment • SBoM Generation • Vulnerability process • Security patch deployment	• Release to market • NO known vulnerabilities • Auditable documentation • Monitor compliance throughout lifecycle • Vulnerability reporting • Visibility of security updates

The Assurance Framework Document



Comprehensive list of ~300 requirements for 15 facets of Product Security

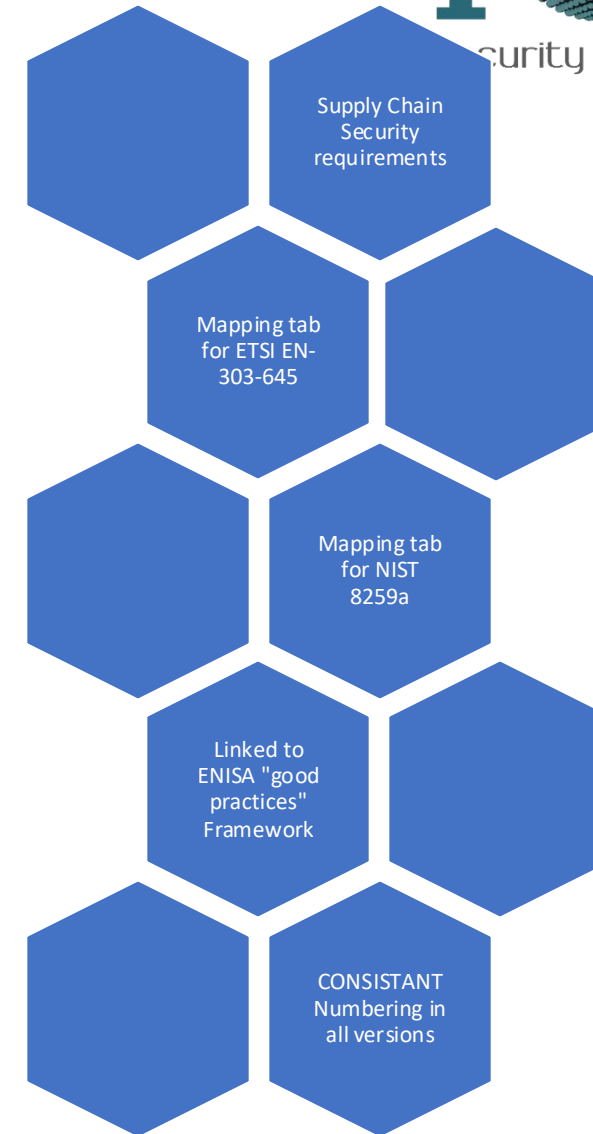
How to use this document

- Introduction to threat-based Security Risk Assessments
- Example Projects

Over 50 cross references to international publications.

- List of Resources for security practitioners

Widely Cited in other documents

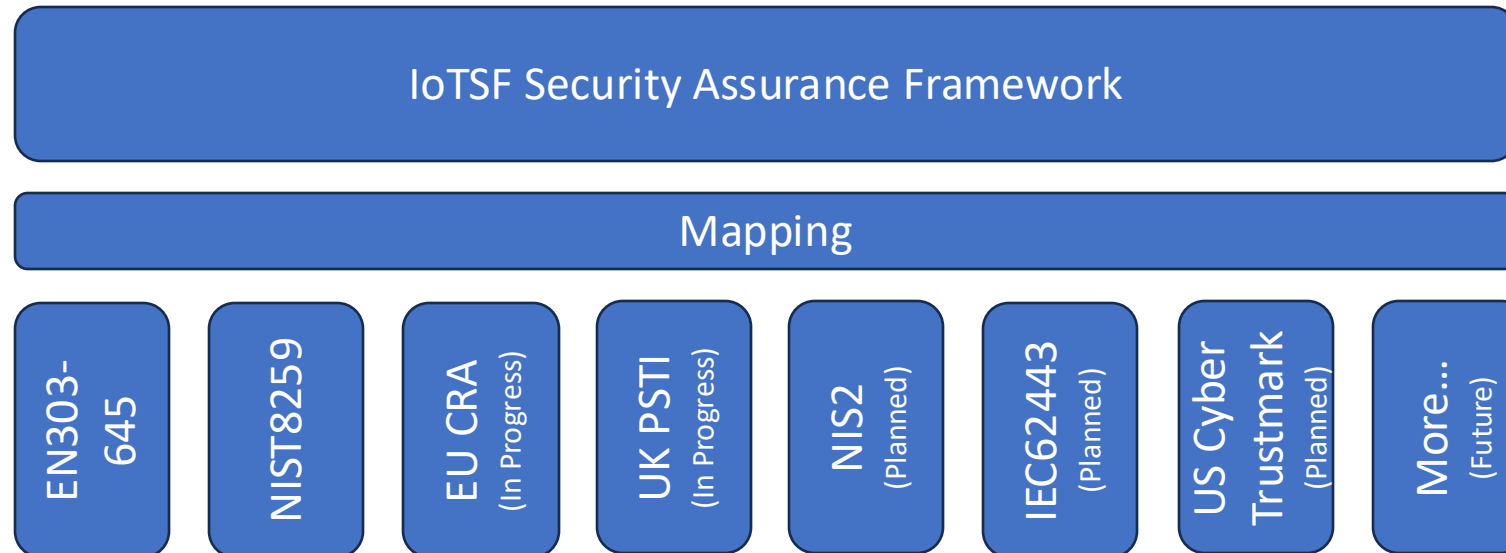


How does the Assurance Framework help?

Mapping to Standards



- Cyber regulations are global – need a global best practice view
- Mapping of the Assurance Framework to range of international standards
- Allows developers to follow a single framework and meet range of geo requirements



Assurance Framework

Evolution - Background



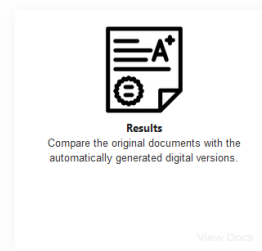
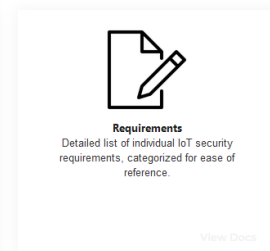
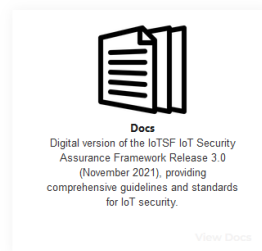
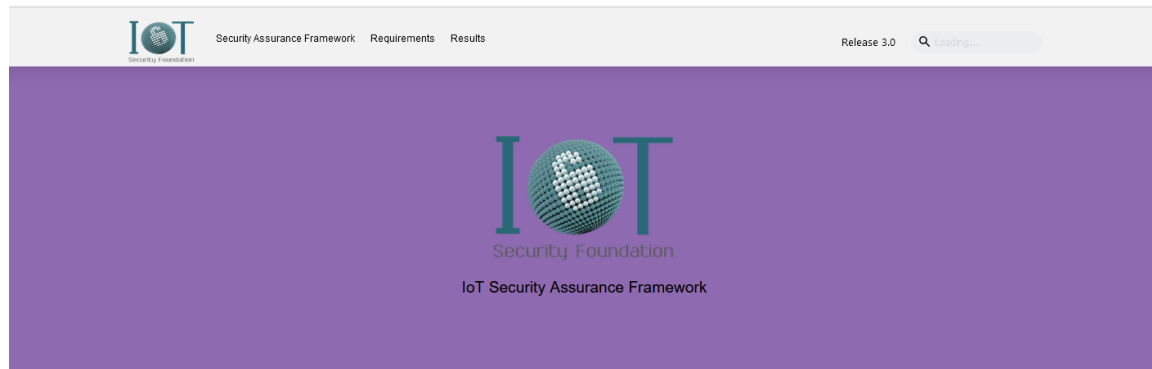
- Security never stops
 - Security needs to manage **Out of Spec** operation
 - Updates, Vulnerabilities, Attacks, product changes all occur **post** 'Certification'
 - Cyber Regulations and Standards require compliance is maintained post certification
 - Need to manage changes over the lifecycle to maintain 'Continuous Assurance' status
 - Provide proof/evidence of continuous compliance
 - Vulnerability Management, Regular Testing, SBoM, Documentation
- Net result - more complex product lifecycle
 - Secure by Design is more complex than current non-secure product development

The Security Assurance Framework Website Evolution



A fully referenceable Web version of the **IoTSF Security Assurance Framework**

<https://af.iotsf.org>



Quick Tour

The Assurance Framework Website



- Security Assurance Framework

The screenshot shows the IoT Security Assurance Framework website. The header includes the IoT Security Foundation logo, navigation links for 'Security Assurance Framework', 'Requirements', and 'Results', and a 'Release 3.0' indicator. A search bar is also present. The left sidebar contains a list of navigation items, with 'The-Process' highlighted. The main content area is titled 'The-Process' and '2.1 The Process'. It contains a paragraph explaining the framework's purpose and a diagram showing the process steps: 'Conduct Risk Analysis on the Product in the Target Environment' and 'Determine Assurance Class Applicable to the Product'.

IoT Security Assurance Framework

Acknowledgements

Intent-And-Purpose >

IoT-Security-Assurance-Framework >

The-Process

Assurance-Class

Using-The-Assurance-Questionnaire

Assurance-Terminology-And-Applicability

Assurance-Applicability >

References-And-Abbreviations >

Appendix-A-Risk-Assessment >

Appendix-B-Introduction-To-Supply-Chain-Security-Requirements >

IoT Security Assurance Framework

Security Assurance Framework Requirements Results

Release 3.0

Search Loading...

The-Process

2.1 The Process

The Framework sets out a comprehensive set of security requirements for aspects of the organisation and product. A response to each requirement needs to be recorded, with supporting statements or evidence. The Assurance Questionnaire is available to IoTSF Members to facilitate evidence collation. For requirements deemed "not applicable", an explanation must be provided as to why. Any alternative countermeasures to reduce any security risk should also be listed.

The assurance process breaks down into a number of steps:

```
graph TD; A[Conduct Risk Analysis on the Product in the Target Environment] --> B[Determine Assurance Class Applicable to the Product];
```

- Create Risk Register
- Determine CIA-Triad Security Objectives
- See Risk Assessment Appendix A for guidelines

- Assurance Class based on security objectives
- Documented Product Environment

Quick Tour

The Assurance Framework Website



- Requirements

IoT Security Foundation

Security Assurance Framework Requirements Results

Release 3.0

Q Loading...

Individual Requirements

2.4.3 Business-Process

2.4.3 Business Processes

Requirements

2.4.4 Device-Hardware

2.4.5 Device-Software

2.4.6 Device-Os

2.4.7 Device-Interfaces

2.4.8 Authentication-& Authorisation

2.4.9 Encryption-& Key-Management

2.4.10 Web-User-Interface

2.4.11 Mobile-Application

2.4.12 Privacy

2.4.13 Cloud-And-Network-Elements

2.4.14 Secure-Supply-Chain-Production

2.4.15 Configuration

2.4.16 Device-Ownership-Transfer

2.4.3 Business Processes

This section's intended audience is those personnel who are responsible for governance of a business developing and deploying IoT Devices. There must be named executive(s) responsible for product security, and privacy of customer information. There are several classes of requirements, which have been identified by a keyword. Each class should be allocated to a specified person or persons for the product being assessed. Further guidance is available from the IoTSF Best Practice Guidelines [ref 44]¹. The applicability of each requirement is defined as Advisory or Mandatory for the assessed risk level of any device, the default is Advisory.

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy.	Mandatory for all classes	Business	Responsibility
2.4.3.2	There is a person or role, who takes ownership for adherence to this compliance framework process.	Mandatory for all classes	Business	Responsibility
2.4.3.3	Intentionally left blank to maintain requirement numbering	-		
2.4.3.4	The company follows industry standard cyber security recommendations.	Mandatory for all classes	Business	Policy
2.4.3.5	A policy has been established for interacting with both internal and third party security researcher(s) on the products or	Mandatory for	Business	Policy

Quick Tour

The Assurance Framework Website



- Requirements



Security Assurance Framework [Requirements](#) [Results](#)

Release 3.0

Individual Requirements

- [2.4.3 Business-Process](#) ▼
 - 2.4.3 Business Processes
 - [Requirements](#) ▼
 - 2.4.3.1**
 - 2.4.3.2
 - 2.4.3.3
 - 2.4.3.4
 - 2.4.3.5
 - 2.4.3.5.1
 - 2.4.3.6
 - 2.4.3.7
 - 2.4.3.8
 - 2.4.3.9
 - 2.4.3.9.1

2.4.3.1

Req No	Requirement	Compliance Class And Applicability	Primary Keyword	Secondary Keyword
2.4.3.1	There is a person or role, accountable to the Board, who takes ownership of and is responsible for product, service and business level security, and mandates and monitors the security policy.	Mandatory for all classes	Business	Responsibility

Previous
« [2.4.3 Business Processes](#)

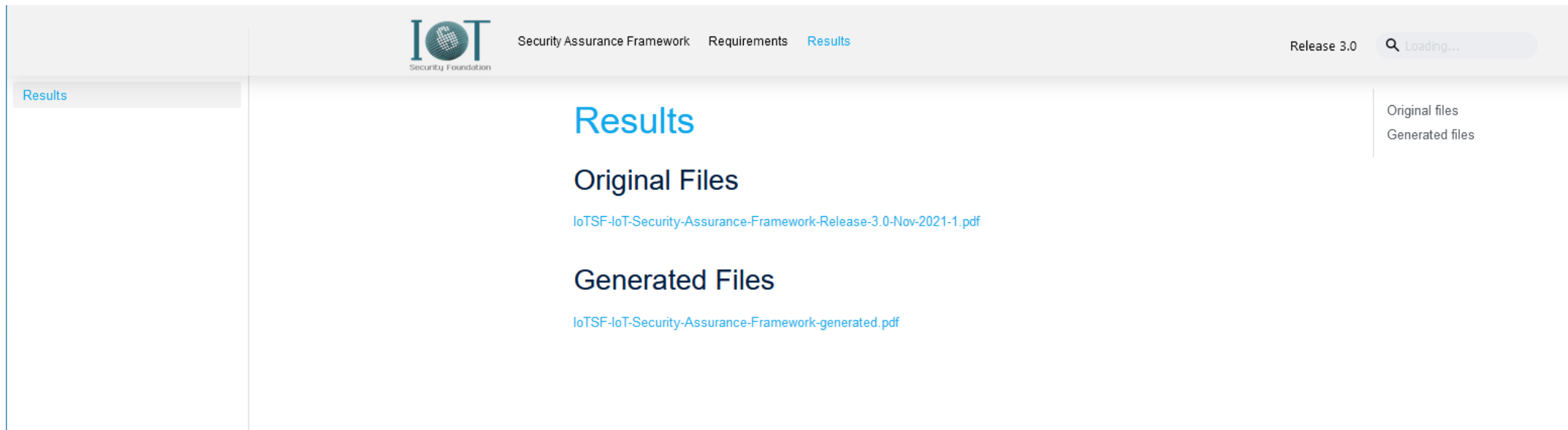
Next
[2.4.3.2](#) »

Quick Tour

The Assurance Framework Website



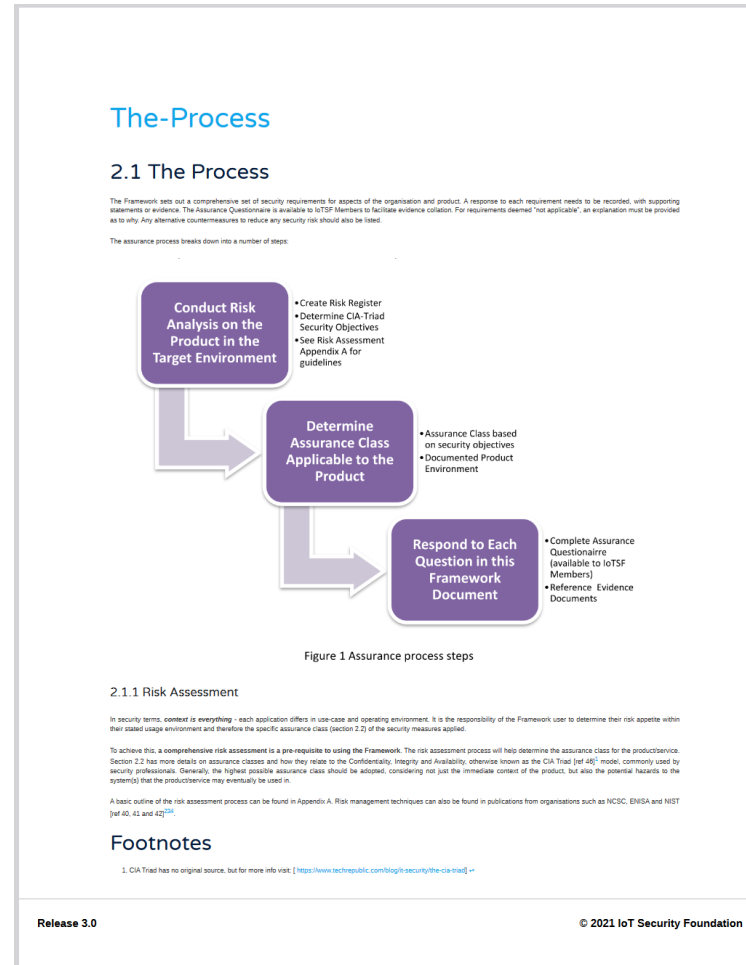
- Results



Quick Tour The Assurance Framework Website



- Output File

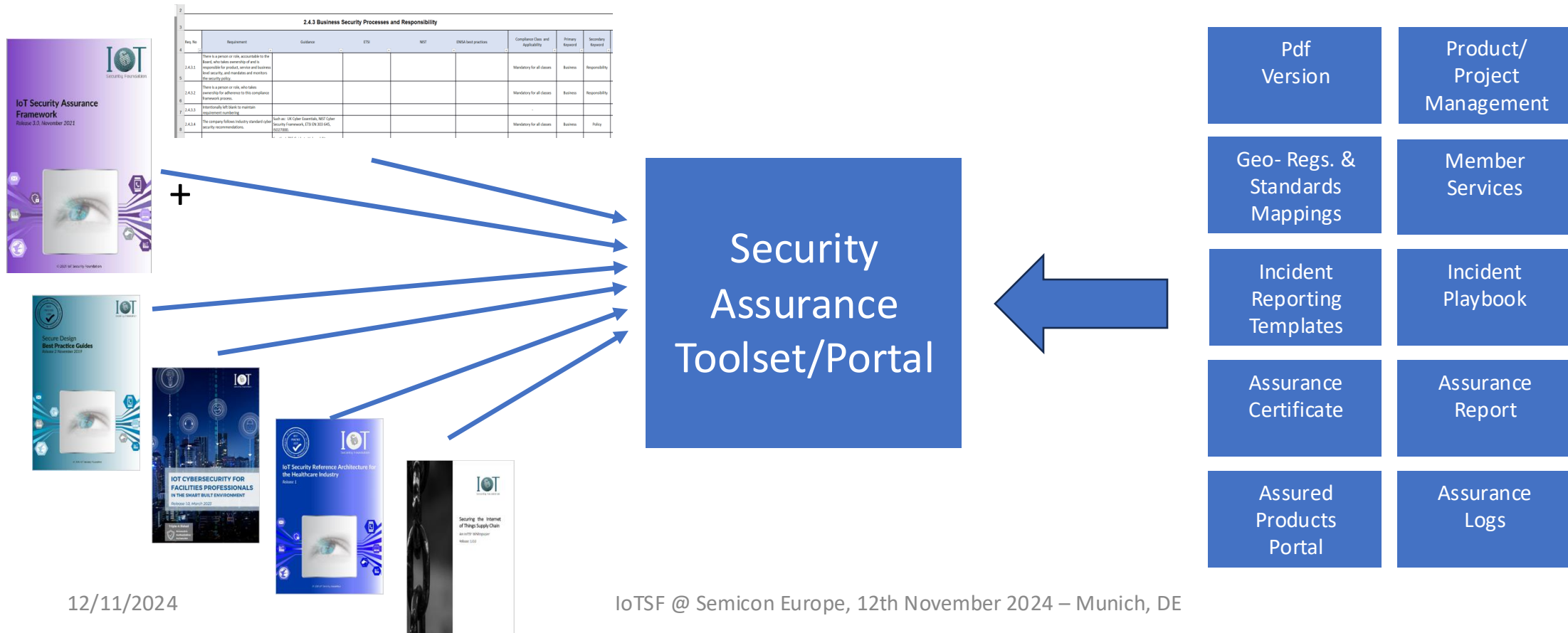


Assurance Framework

Continuous Evolution



- Focal point for best and next practices
- New medium gives broad scope for new features, extensions, interfaces



Status



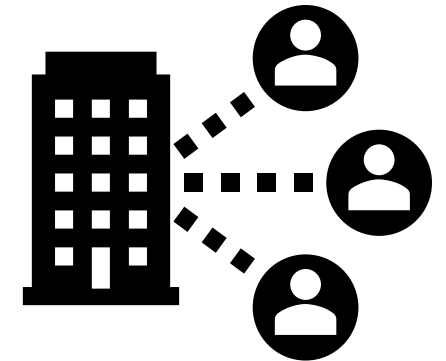
- First phase (DONE!)
 - Physical to Digital Medium conversion
 - Increases options and flexibility
 - Minimal changes to Assurance Framework v3.0 document
- Phase 2+Updates
 - Assurance Framework-WG now refining/updating the content
 - Historic/scheduled amendments
 - Clarification of Requirements
 - New material

Assurance Framework

Call to Action



- Participate
 - Use the Assurance Framework for your product designs
 - You can help: Further Contributions to the Working Group invited
 - Expertise from members and stakeholders –absolutely-needed
- Invite stakeholder input so we can deliver tools that work for users
 - SME's thro' Global Mega Corp
 - Make sure we get the right features



Thank You



SECURITY FIRST

Designed in at the start

FIT FOR PURPOSE

Right-sized for application

RESILIENCE

Through operating life