Case Study - The Business and Regulatory Value of Third Party Certification to the NIST Cybersecurity Framework

John DiMaria, MHISP, HISP, CSSBB, AMBCI, CERP
Global Product Champion, BSI Group
Ronald Tse; Founder and Chief Executive Officer
CalConnect Vice President and Director of External Relations
Ribose

UK Superbrands 2017

INVESTORS IN PEOPLE

By Royal Charter

59,000 different areas of collective best practice - created by industry, for industry

From tram tracks…

… to the Internet of Things

Tea

Information Security

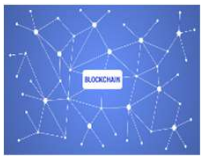
Connected and Autonomous Vehicles

Robot Ethics / Artificial Intelligence

Smart Cities / Building Information Modelling

bsi.

Where are we at today?



"The FBI reports that more than **4,000 ransomware attacks occur daily**, while other research sources state that **230,000 new malware samples** are produced every day."

"By the end of 2018, **one to two million cybersecurity jobs** could remain unfilled."

WORLD ECONOMIC FORUM

facebook

THE HOME DEPOT

Anthem

Privacy protection

Security breaches

Data Integrity

DDOS Attacks

Cyber Hacks & Attacks

Session Hijacking

Malicious Codes

Governance of cybersecurity risk

- Consider privacy implications of the cybersecurity program
- Responsible individuals report to appropriate management and are appropriately trained
- Top management support compliance of cybersecurity, privacy laws, regulations, and Constitutional requirements
- Continued assess implementation of the foregoing organizational measures and controls

Source: NIST

International Harmonization and Context

Information technology — Security techniques — Cybersecurity and ISO and IEC Standards

6 Concepts

6.1 Overview of cybersecurity frameworks

A cybersecurity framework captures a set of desired cybersecurity outcomes that are common across all sectors and organizations. A framework facilitates communication about implementation of these

desired outcomes and associated cybersecurity activities across the organization, from the executive level to the implementation and operations levels. The framework should consist of five functions, or high-level descriptions of desired outcomes, which are concurrent and continuous:

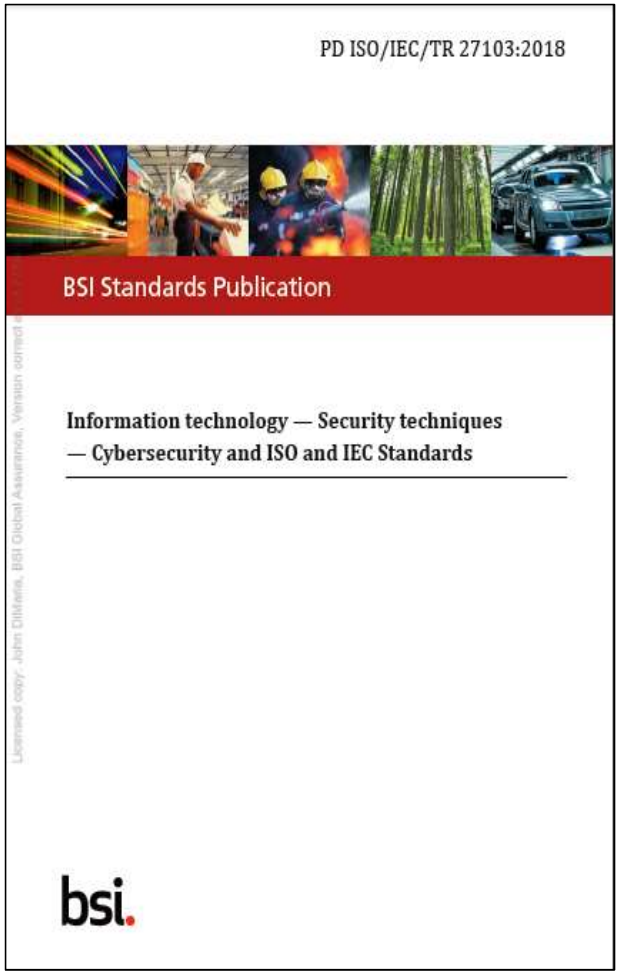
— Identify;

— Protect;

— Detect;

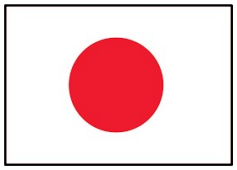
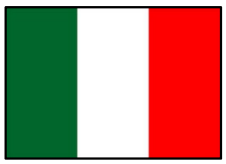
— Respond;

— Recover.

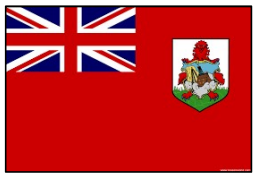


International Cybersecurity Framework Use







NTT
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

ONTARIO ENERGY BOARD

IMO INTERNATIONAL MARITIME ORGANIZATION

ISO IEC

Source: NIST

International Harmonization and Context

INSIDE CYBERSECURITY

DAILY NEWS

Japanese industry leader on cyber: NIST framework increasingly embraced overseas

July 25, 2017 | Charlie Mitchell

INSIDE CYBERSECURITY

DAILY NEWS

U.S. businesses urge Singapore to adopt NIST framework in cyber law

August 29, 2017 | Joshua Higgins

INSIDE CYBERSECURITY

DAILY NEWS

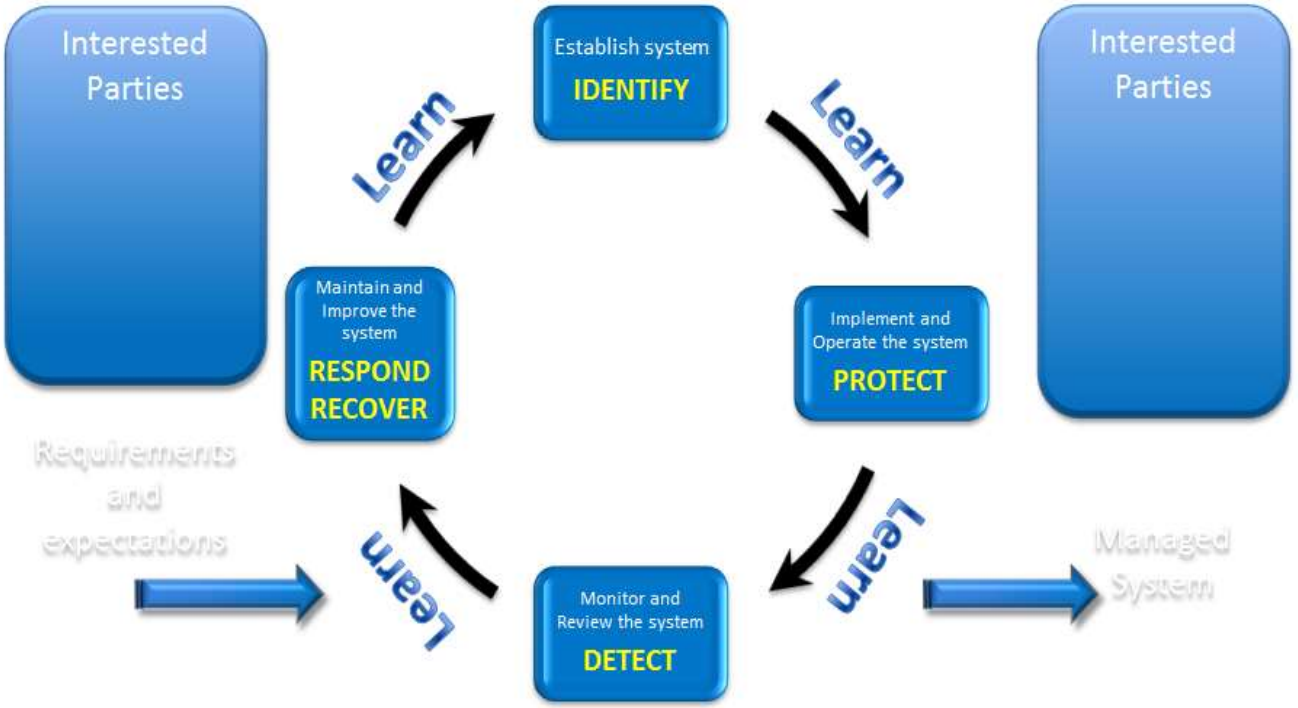
British vehicle cyber guides follow U.S. NHTSA approach to connected cars

August 08, 2017 | Joshua Higgins

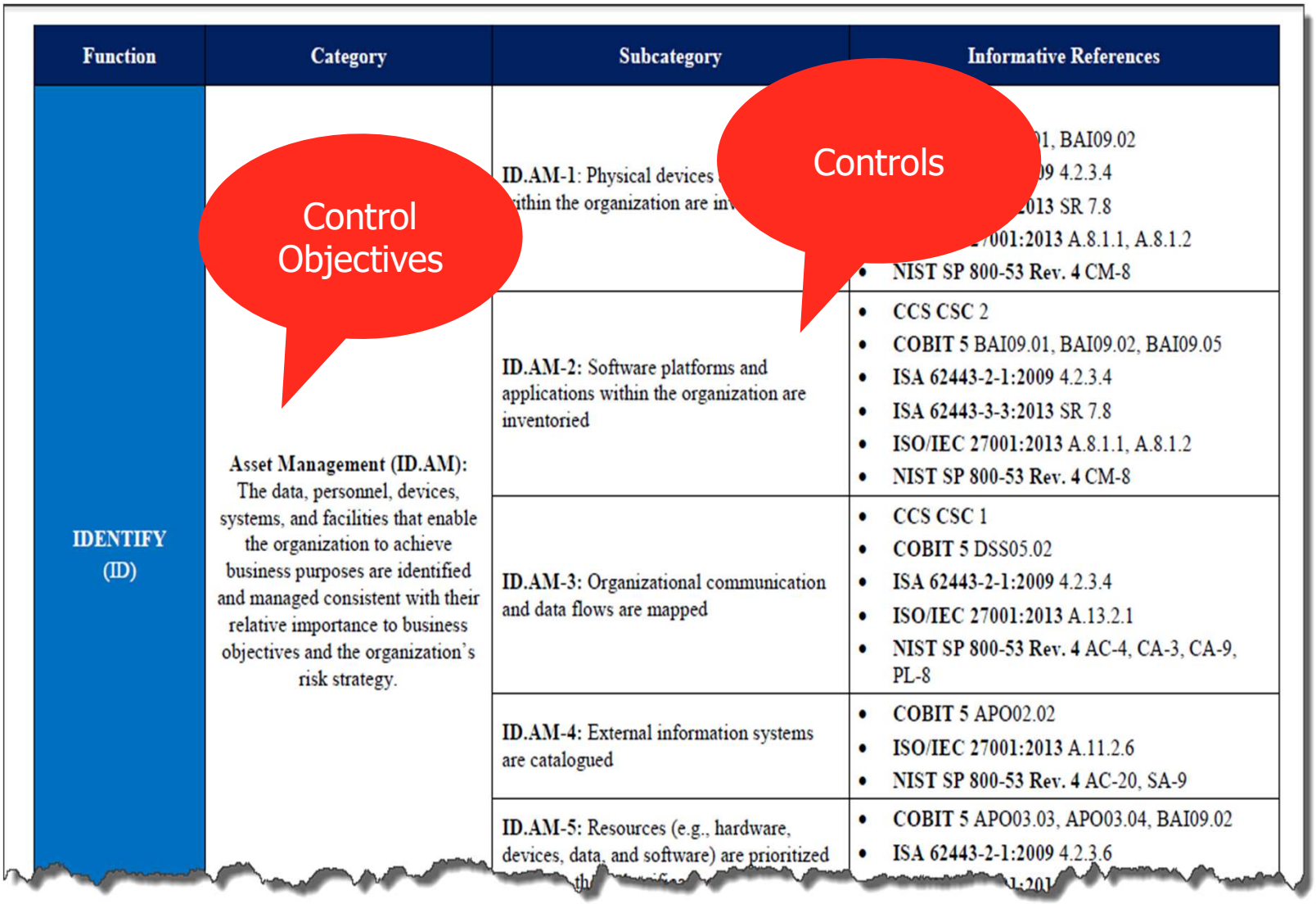
Common International Threads on how the Framework is being used

Addressing Gaps and Implementing Controls

Aligned with the PDCA Cycle



bsi.



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices ithin the organization are in	01, BAI09.02 09 4.2.3.4 013 SR 7.8 7001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• COBIT 5 APO02.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized th	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 1:201

bsi.

Organizational Tier Levels

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1**: Physical devices and systems within the organization are inventoried	• **CCS CSC** 1 • **COBIT 5** BAI09.01, BAI09.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	• **CCS CSC** 2 • **COBIT 5** BAI09.01, BAI09.02, BAI09.05 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISA 62443-3-3:2013** SR 7.8 • **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 • **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	• **CCS CSC** 1 • **COBIT 5** DSS05.02 • **ISA 62443-2-1:2009** 4.2.3.4 • **ISO/IEC 27001:2013** A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	• **COBIT 5** APO02.02 • **ISO/IEC 27001:2013** A.11.2.6

TIER 1
Partial

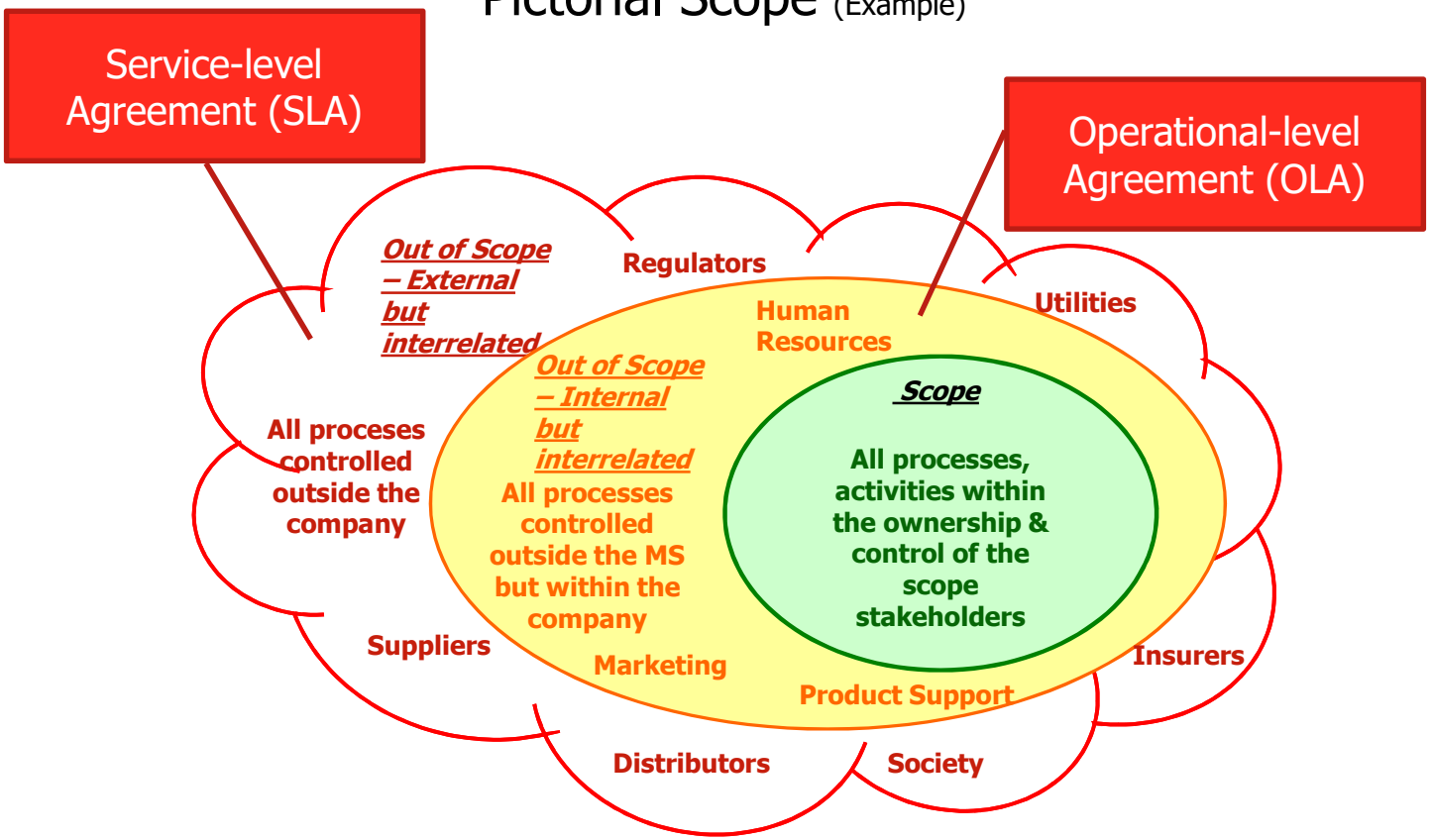
Tier 2
Risk Informed

Tier 3
Repeatable

TIER 4
Adaptive

bsi.

Pictorial Scope (Example)



Why ISO/IEC 27001?

Why did we chose ISO/IEC 27001?

Information Resilience

Information Security
ISO/IEC 27001

Cloud security
- Security controls for cloud services ISO/IEC 27017
- CSA STAR Certification

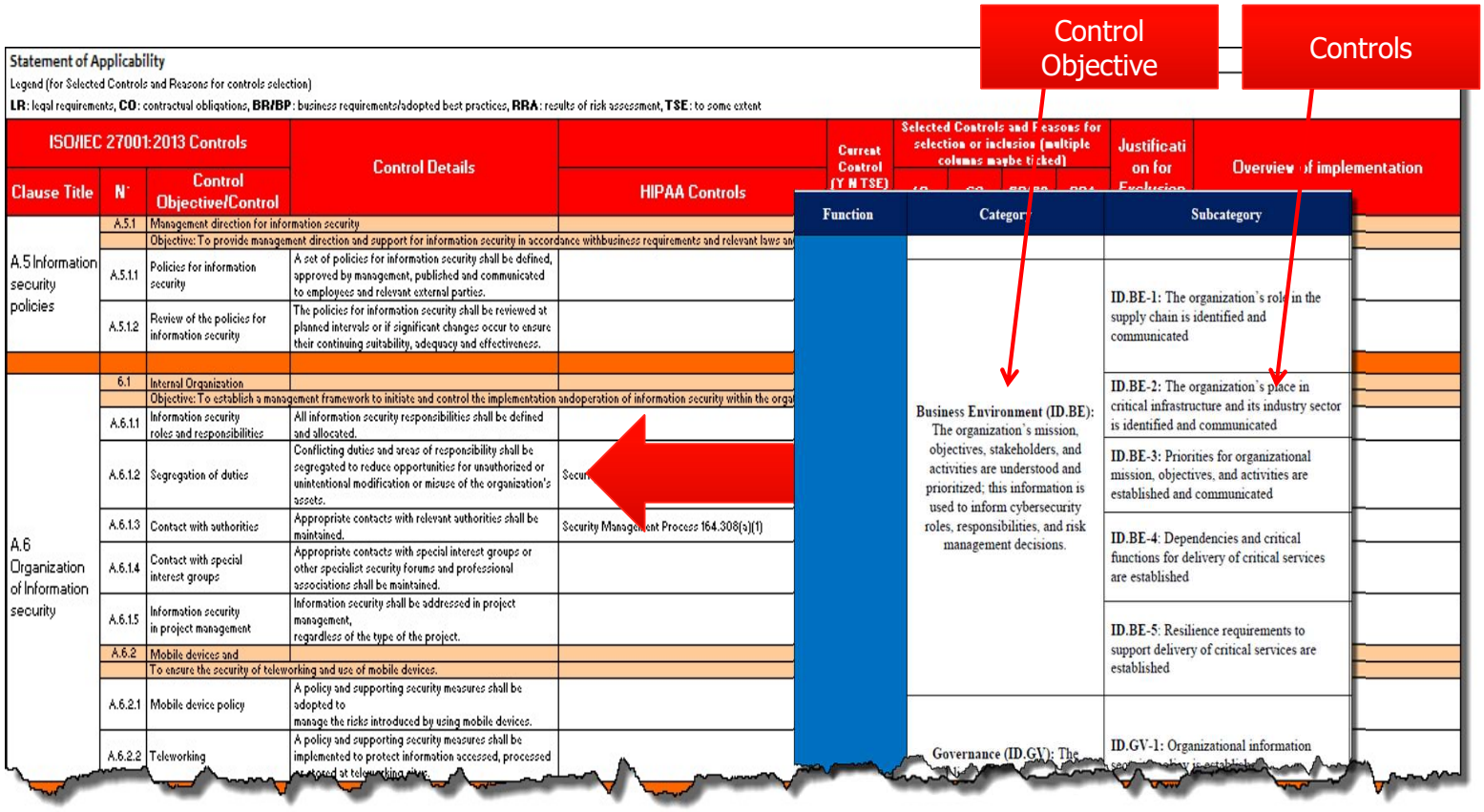
Privacy
- Privacy gap analysis
- Personal Information Management BS 10012
- Personally Identifiable Information Protection ISO/IEC 29151
- Personally Identifiable Information in the cloud ISO/IEC 27018

Network/system/application security
- Vulnerability Scanning
- Secure Digital Devices and Transactions Kitemark
- Penetration Testing
- Cyber Essentials/ Cyber Essentials Plus

Specialist information security
- NIST Cybersecurity Framework
- Payment Card Industry Data Security Standard PCI DSS
- Information Security Management System Kitemark
- Security Awareness: Wombat

bsi.

Typical ISO/IEC 27001 Statement Of Applicability (SOA)



BSI's Journey in development of Certification to the Cyber Security Framework

bsi.

Objectives

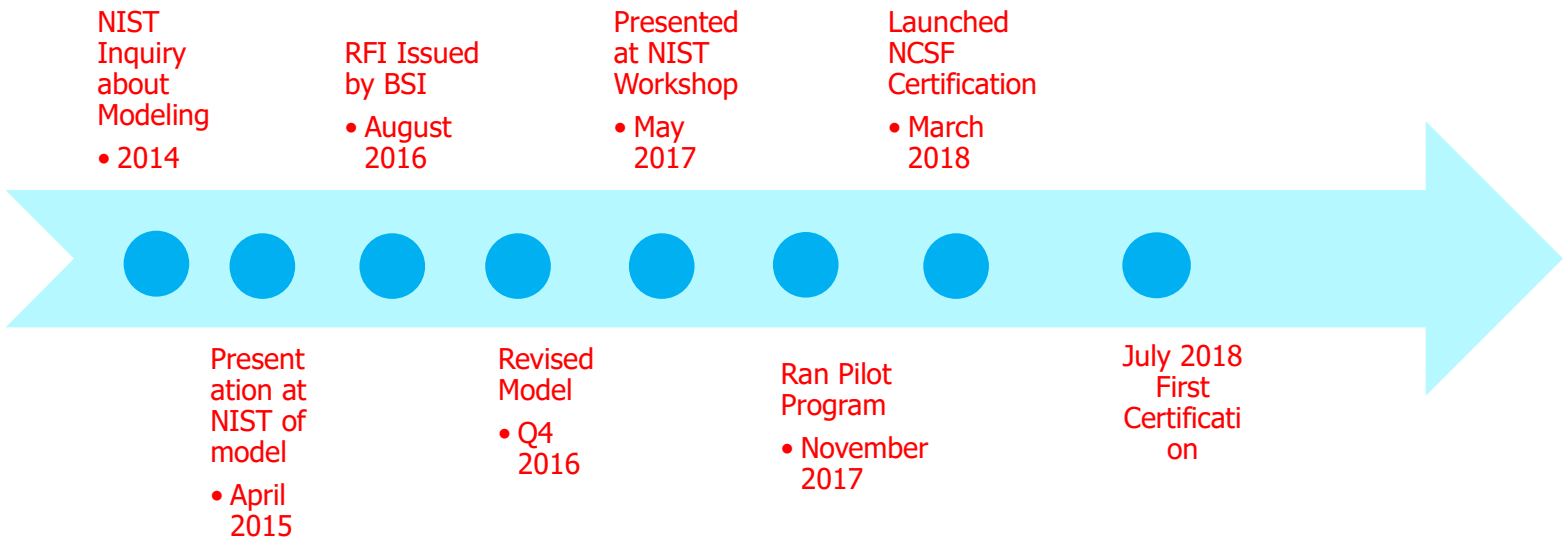
There are an increasing number of organisations claiming they are compliant to the CSF. However it is unclear what confidence can be placed on the statement of 'compliance'.

The CSF was intended to manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

Therefore the Framework relies on a variety of existing standards, guidelines, and practices to enable critical infrastructure providers to achieve resilience. These should be recognised in any certification scheme.

bsi.

Development Timeline



bsi.

Mapping ISO 27001 to CSF

Risk assessment/management

- There exists a risk management approach in ISO 27001 that meet many the requirements of the CSF

Core

- Many of these map to ISO 27001. Those are relatively easily be added during an ISO 27001 assessment and have already been mapped

Tiers

- It will be hard to state or even verify the tier selected but we assess the process by which the organisation evaluated the tier and validate effectiveness of the process

Profile

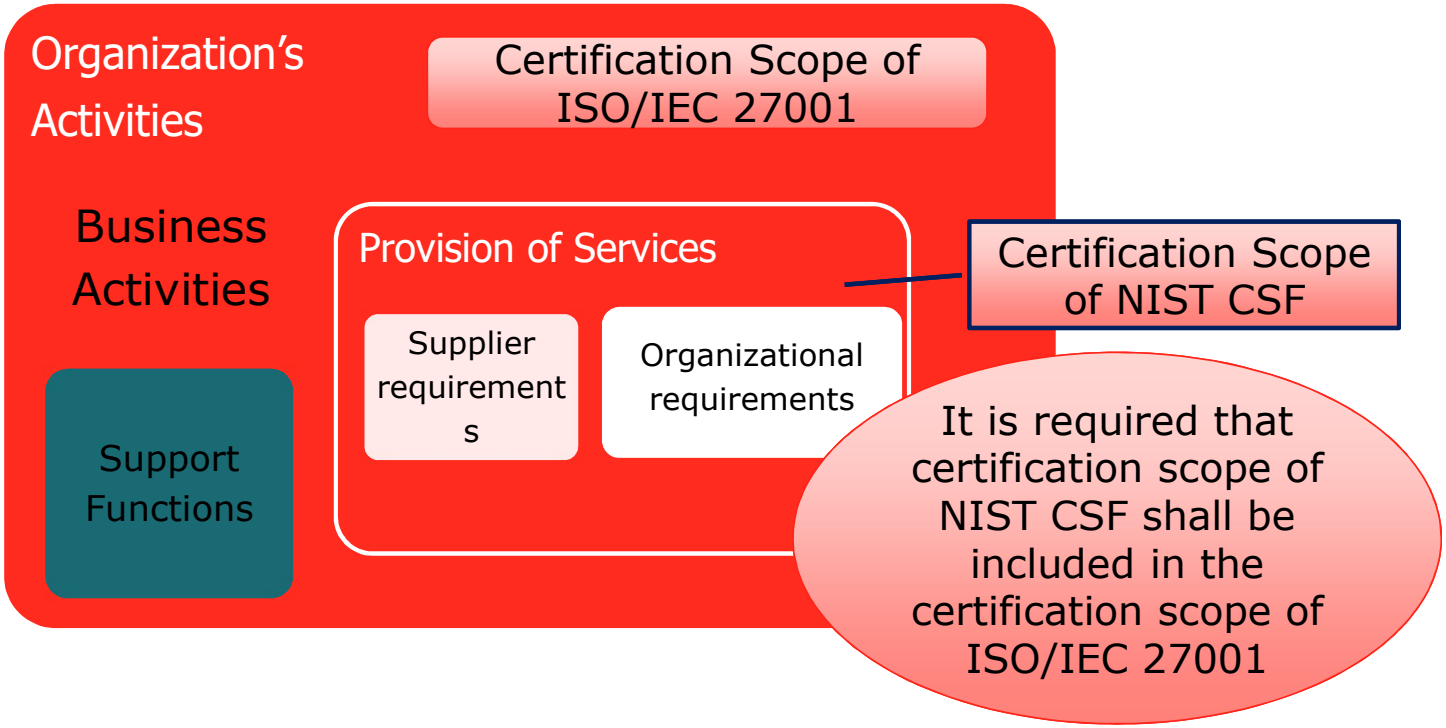
- Current state is well covered by control selection process in ISO 27001 plus a process for assessing the tier
- Will be expanded by a number of additional clauses to create a future state
- A requirement that the profiles be documented

Description of Decision Making and Information Flows (no specific requirements)

- Reasonably well covered by the core clauses of 27001 (High Level Structure). Some additional documentation requirements are assessed

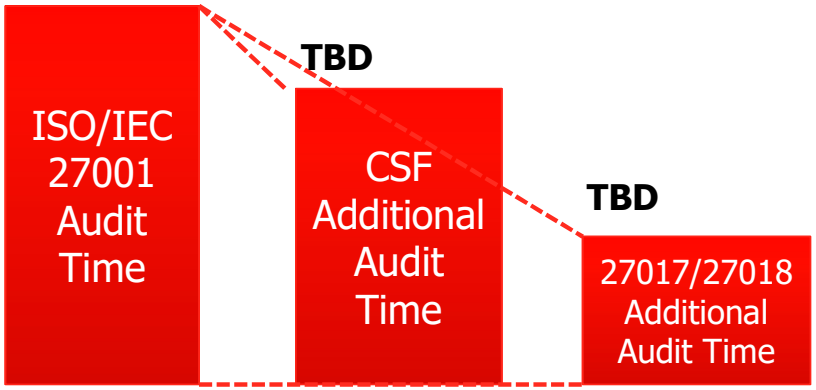
bsi.

Certification Scope of NIST CSF



Additional audit durations for NIST CSF

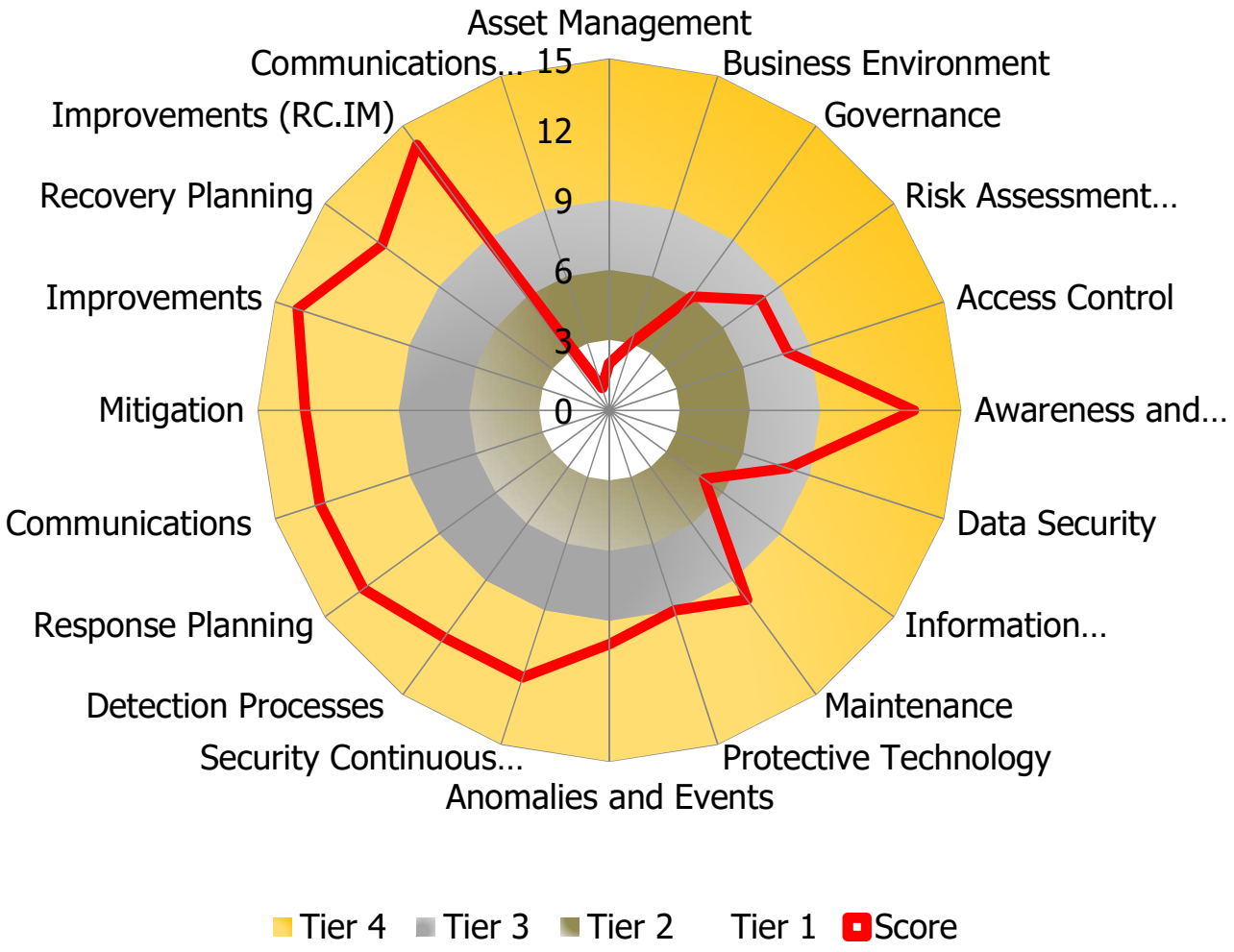
The additional audit time for subsequent NIST CSF audit is calculated based on the audit time for ISO/IEC 27001 audit.

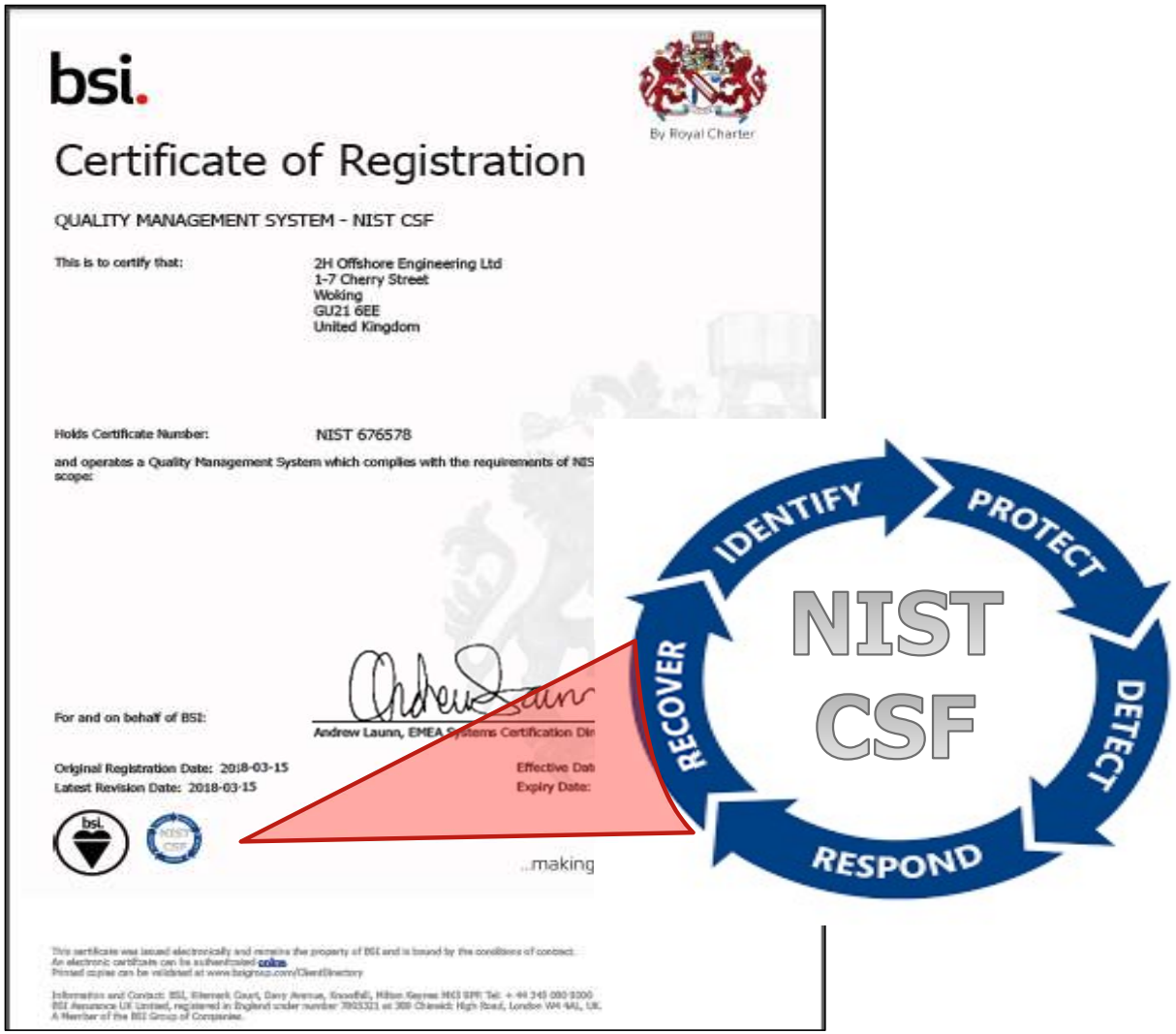


Audit type	Audit Time for NIST CSF
Extension to NIST CSF in conjunction with ISO/IEC 27001 IA, CAV or RA	Initial Certification Audit Time for ISO/IEC 27001 x
Special Audit to extend to NIST CSF	Plus X day to the above
Subsequent RA for NIST CSF	RA Audit Time for ISO/IEC 27001 x
Subsequent CAV for NIST CSF	CAV Audit Time for ISO/IEC 27001 x

bsi.

Score	1 to 3	4 to 6	7 to 9	10 to 12	12 to 15
	No formal approach	Partial	Risk Informed	Repeatable	Adaptive
Evidence / Definition	1. There is some evidence of a system in place to manage the control area.	4. There is evidence of a system in place to cover to key operations in the control area. Where required, the system is documented.	7. There is evidence of a robust system in place that covers all routine operations in the control area	7. There is evidence the system for managing the control area is capable of managing contingency events as well as routine activity.	13. Control area owners actively share best practice to support development in other areas of the organization based on their experience in this control area.
Managed	2. There is some evidence of either a documented system or an accepted way of working is in place.	5. There is a clearly identified owner for the control area who understands their scope of responsibility.	8. There is evidence that the control area is actively monitored and measured and actions evaluated based on the evidence.	11. Input from a variety of sources is considered to decide how to manage risk and improve operations in this control area.	14. Control area owners can demonstrate that they actively review best practice from their industry and across their organisation and apply it to the control area.
Followed / Effective	3. There is some evidence of an accepted way of working that is broadly understood and followed.	6. There is evidence the system is understood and routinely followed.	9. There is evidence that critical people operating in the control area are appropriately trained / skilled to manage routine operations in the control area.	12. There is evidence that inputs form a range of stakeholders and monitoring and measure systems has been taken into account when improving operations in the control area.	15. Changes in the control area are evaluated against the strategic objectives of the organization.


Asset Management
Business Environment
Governance
Risk Assessment…
Access Control
Awareness and…
Data Security
Information…
Maintenance
Protective Technology
Anomalies and Events
Security Continuous…
Detection Processes
Response Planning
Communications
Mitigation
Improvements
Recovery Planning
Improvements (RC.IM)
Communications…
15
12
9
6
3
0
Tier 4
Tier 3
Tier 2
Tier 1
Score



bsi.

By Royal Charter

Certificate of Registration

QUALITY MANAGEMENT SYSTEM - NIST CSF

This is to certify that:

2H Offshore Engineering Ltd
1-7 Cherry Street
Woking
GU21 6EE
United Kingdom

Holds Certificate Number: NIST 676578

and operates a Quality Management System which complies with the requirements of NIS
scope:

For and on behalf of BSI:

Andrew Launn, EMEA Systems Certification Dir

Original Registration Date: 2018-03-15
Latest Revision Date: 2018-03-15

Effective Dat
Expiry Date:

...making

This certificate was issued electronically and remains the property of BSI and is bound by the conditions of contract.
An electronic certificate can be authenticated online.
Printed copies can be validated at www.bsigroup.com/ClientDirectory

Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Ribose Case Study

Integrating the NIST Framework into the organizational culture and proving effectiveness

bsi.

Ribose is defined by the universal pursuit of freedom and liberty

Our mission:
"To allow individuals and organizations alike to *freely communicate and achieve productivity for the greater good*."

We achieve our mission through focusing on:

- Security and privacy
- Open standards, transparency and interoperability

Everything we do relate to these goals.

And this is why the **NIST CSF** fits us.

bsi.

Rising Star
Technology Fast 20
2017 Hong Kong
Deloitte.

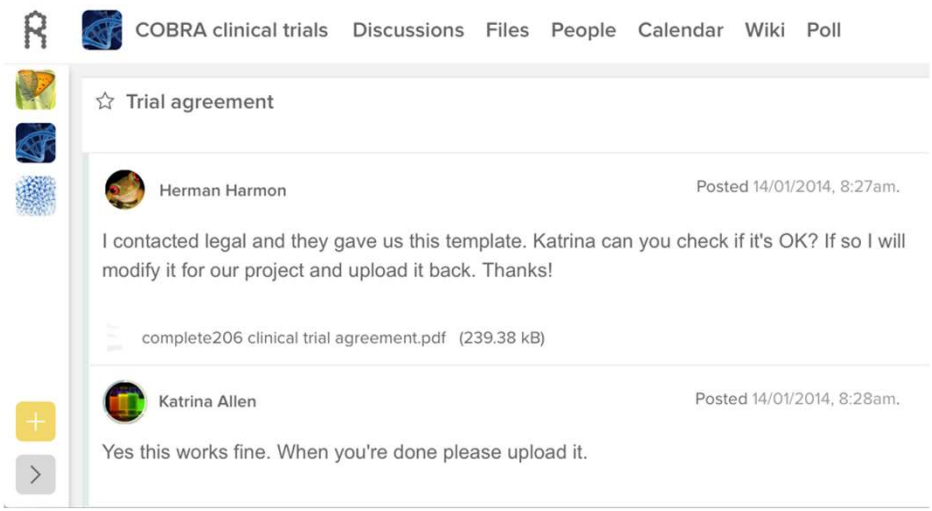
CSA APAC
Enterprise Awards
Security Innovation of the Year

RED HERRING GLOBAL 100 WINNER

Our offerings demonstrate we practice what we preach

Ribose, the secure collaboration platform

- Provider-opaque security
- Hierarchically-managed data
- Proprietary security technologies



Related open technologies

- RNP: high-performance OpenPGP suite
- Nereon: universal configuration
- Riffol: secure initialization system
- Retrace: application integrity monitoring and active interception

Heavy contributions to third-party projects

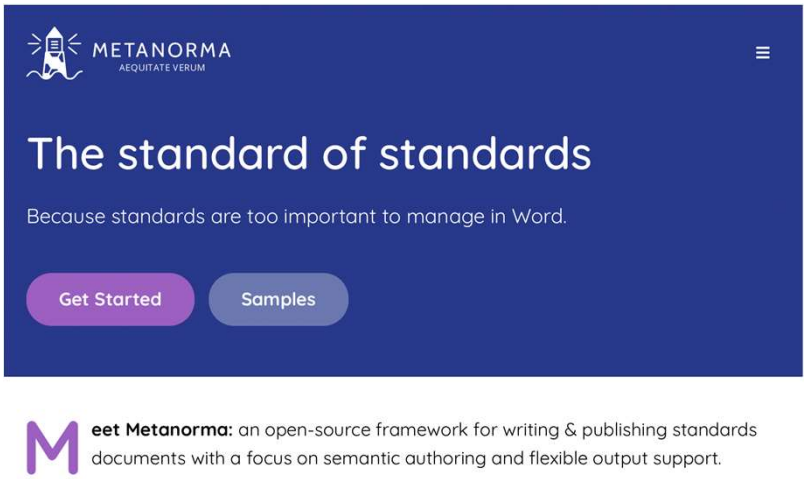
- OpenSSL
- Botan
- Terraform

bsi.

Our open technologies form the basis of international standards

Metanorma, the open-source publishing toolchain

- Author-to-paper publishing flow
- Separates content and presentation concerns



Related open technologies

- Metanorma StandardDoc: standardized standardization documents
  - Adopted by authors of **ISO**, **IETF**, **CalConnect**, **CSA**, **UNECE**, **M3AAWG** documents
- Engyon: secure documents
- Relaton: interoperable citations

bsi.

Advancing the world with open international standards, one at a time

Security

- ISO/PWI Information security -- Vulnerability assessment process
- CSA SaaS security guidelines for cloud customers
- CSA Agile security

Standardization documents

- ISO 36001 Standardization documents -- Metanorma -- Document metamodel
- ISO 36002 Standardization documents -- Metanorma -- Representation in XML

Information exchange

- ISO 19160-6 Addressing -- Digital addresses
- ISO 56001 Directory -- Common profile -- Personal and organization information (vCard v4 successor)

Core data

- ISO 8601-1/2 Date and time -- Representation for information interchange (FDIS)
- ISO 34000 Date and time -- Concepts and vocabulary
- ISO 34002 Date and time -- Timezones
- ISO 34003 Date and time -- Codes for calendars

bsi.

We strongly advocate cybersecurity assessments, and do them for good reasons

Regional

World's first Singapore MTCS (highest Level 3)

bsi. SS 584 Multi-tiered Cloud Computing Security

First non-China-based C-STAR

CSA C-STAR

Cloud

First SaaS

bsi. ISO/IEC 27017 Security Controls for Cloud Services

bsi. ISO/IEC 27018 Protection of Personally Identifiable Information

Only CSP triple-assured by CSA

World's first STAR Attestation

CSA STAR CERTIFICATION

CSA STAR ATTESTATION

First cloud provider

bsi. Secure Digital Transactions KITEMARK™

... and more security

AICPA SOC

AICPA SOC 3

CHECK IT Health Check Service

bsi.

Independent auditors are the true value in third-party certification

"The (audit) journey is the reward."

The audit report is **not** where value lies.

Rationale

- "You can't improve what you can't **measure**"
- Measurements have to be **interpreted**
- **Independence** helps in interpretation of measurements

Facts

- **Independent and competent external auditors** can provide expert insights about your security stance.
- They have a keen sense in **finding problems** and can **signal potential improvements.**
- They do more audits than you think, their **experience** will **allow everyone involved in the process to learn**.

bsi.

The business value of a certification is in self-improvement

Value of dynamic interactions

- Going to school vs reading textbooks at home?
- In-person course vs self-taught option?
- You wanted to **learn the subject** well!
  - Helps you understand the topic with a **broader view and depth**
  - Immediate **feedback**
- A little **pressure** also helps you get there
  - **Motivation** from peers compassionate with your cause and familiar with your context

A way to **get better**

- Third-party auditors are your **sparring partners** in information security management.
- A certification is a (paid) continuous commitment to improve one's information security stance. This **external pressure applies to all involved** in the organization.
- Serves a **consistent reminder** that the "good enough" bar for information security is an **ever-raising** one.

That said, a shiny badge is a useful extra.

bsi.

Business rationale for Ribose's certification

International harmonization

- Philosophy of "Implement once, certify many"
- Harmonization for us means "**highest bar**", not "lowest common" or "average"
- Want to demonstrate to customers we can **do the right thing**:
  - Raison d'être of "best practices"
  - Doing the right thing means doing it everywhere!
    - (i.e. there is only one Internet)

Operational benefits

- Better **align** organizational **goals and risks** with operational controls.
- Push our existing system and **fill in any gaps**
  - We realized better ways of doing things with every extra security standard we comply with
  - Continuously improve on efficiency and effectiveness
- Applicable control for continuous improvement!

bsi.

Implementer's view: CSF takes a more holistic approach than ISO/IEC 27001

	ISO/IEC 27001	**NIST CSF**
Orientation	Process-oriented	Outcome-oriented
Action drivers	Risk-driven control requirements	Focused on risk mitigation
Approach	Prescriptive, management system	Adaptive, risk-driven
	Rule-based	Open to prioritization, improvise
Mantra	**"What you have to do"**	**"What you want achieved"**

SMBs often find ISO/IEC 27001 too complex to apply.
CSF gives them a good start.

bsi.

CSF subcategories are worded to allow possibilities

ID.AM-2
Software platforms and applications within the organization are inventoried.

Straightforward, outcome-oriented, yet literally **open-ended** specification:

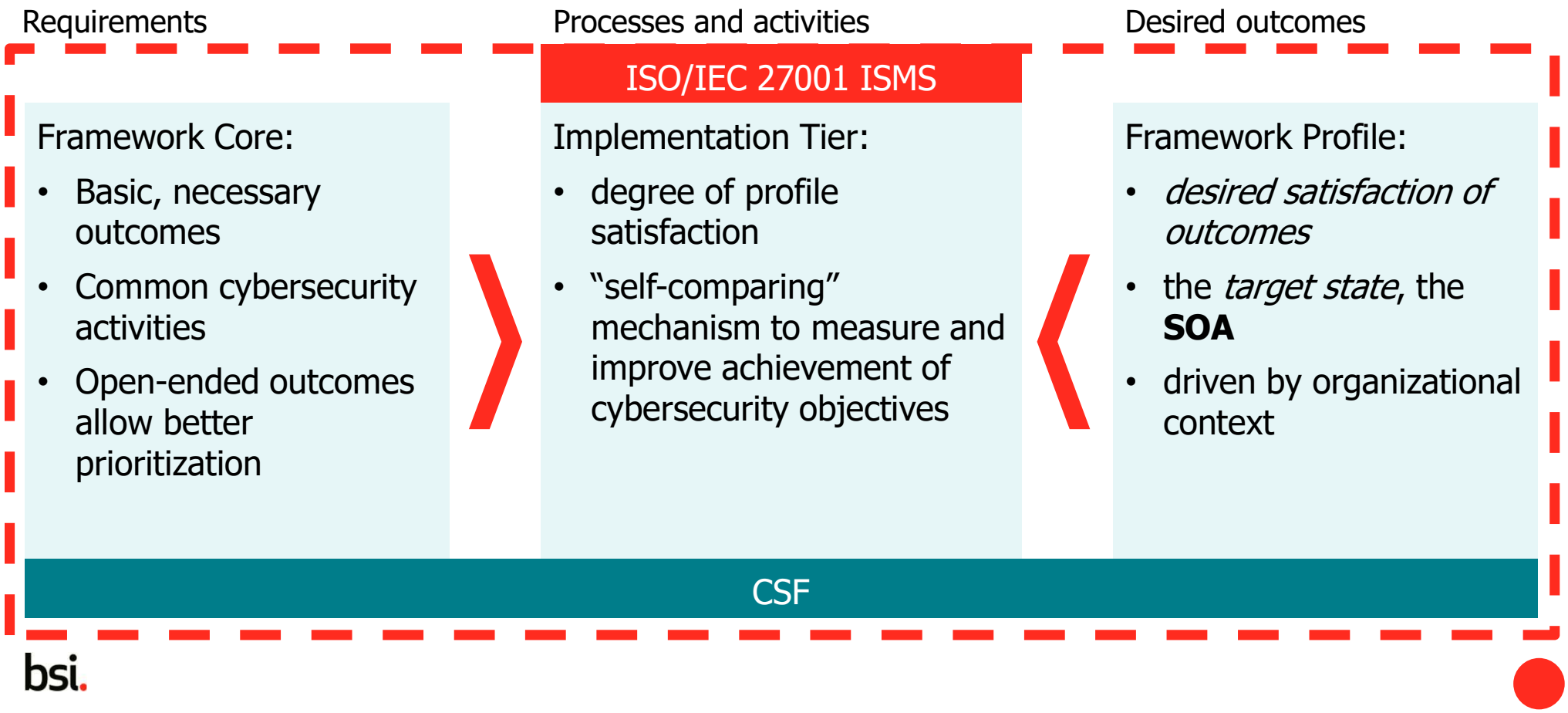
- *Software platforms*
- *applications*
- *within the organization*
- *inventoried*

In the ISO/IEC 27001 family, this involves at least:

- Change management
- Release management
- Service management
- Configuration management
- Audit management

bsi.

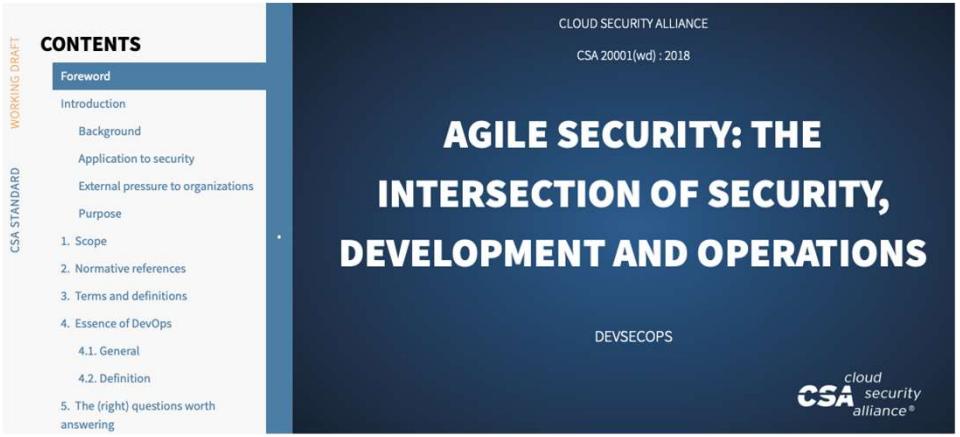
We found CSF useful for setting *context* for ISMS: risk and desired outcomes



bsi.

CSA DevSecOps WG's "six pillars" of Agile Security facilitates CSF alignment

DevSecOps: achievement of information security through DevOps practices.



Page:
- https://riboseinc.github.io/csand-devsecops-whitepaper/

Feedback:
- https://github.com/CloudSecurityAlliance/csand-devsecops-whitepaper/

bsi.

10.1. **Collectively responsible**
- Everyone is responsible of the security stance

10.2. **Collaborate**
- Culture of working together

10.3. **Pragmatic**
- Prioritize and demonstrate value of security

10.4. **Integrate**
- Vertical and horizontal

10.5. **Automate**
- Put humans in charge of what they do best

10.6. **Measure**
- Evidence-based improvement

Takeaway: how are YOU going to live the CSF?

> *Organizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances.*

> *The Framework is not a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure.*

-- NIST Cybersecurity Framework 1.1

This was never about the CSF.

It's about how you **live and breath** it!

bsi.

Thank You!

Address: BSI Group America Inc.

12950 Worldgate Drive, Suite 800

Herndon, VA 20170

Main Office Telephone: 888-429-6178

Fax: 703 437 9001

Email: Inquiry.msamericas@bsigroup.com

Links: http://www.bsiamerica.com

bsi.