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
From tram tracks... to the Internet of Things

- Tea
- Information Security
- Connected and Autonomous Vehicles
- Robot Ethics / Artificial Intelligence
- Smart Cities / Building Information Modelling

59,000 different areas of collective best practice - created by industry, for industry
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.”
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
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 outcomes and associated cybersecurity activities across the organization, from the executive level to the implementation and operations level. 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

Source: NIST
International Harmonization and Context

Japanese industry leader on cyber: NIST framework increasingly embraced overseas
July 25, 2017 | Charlie Mitchell

U.S. businesses urge Singapore to adopt NIST framework in cyber law
August 29, 2017 | Joshua Higgins

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

- **Identify** (Establish system)
- **Protect** (Implement and operate the system)
- **Detect** (Monitor and review the system)
- **Respond** (Maintain and improve the system)

**Learn**

**Interested Parties**

**Managed System**

**Requirements and expectations**
<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY (ID)</td>
<td>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.</td>
<td>ID.AM-1: Physical devices within the organization are inventoried</td>
<td>NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
</tbody>
</table>
| | | 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 | • COBIT 5 APO03.03, APO03.04, BAI09.02  
• ISA 62443-2-1:2009 4.2.3.6 |
Organizational Tier Levels

<table>
<thead>
<tr>
<th>Function</th>
<th>Category</th>
<th>Subcategory</th>
<th>Informative References</th>
</tr>
</thead>
<tbody>
<tr>
<td>TIER 1</td>
<td>Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIER 2</td>
<td>Risk Informed</td>
<td>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.</td>
<td>CCS CSC 1&lt;br&gt;COBIT 5 BAIO 01, BAIO 02&lt;br&gt;ISA 62443-2:1:2009 4.2.3.4&lt;br&gt;ISA 62443-3:3:2013 SR 7.8&lt;br&gt;ISO/IEC 27001:2013 A.8.1.1, A.8.1.2&lt;br&gt;NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td>TIER 3</td>
<td>Repeatable</td>
<td>ID.AM-1: Physical devices and systems within the organization are inventoried</td>
<td>CCS CSC 2&lt;br&gt;COBIT 5 BAIO 01, BAIO 02, BAIO 05&lt;br&gt;ISA 62443-2:1:2009 4.2.3.4&lt;br&gt;ISA 62443-3:3:2013 SR 7.8&lt;br&gt;ISO/IEC 27001:2013 A.8.1.1, A.8.1.2&lt;br&gt;NIST SP 800-53 Rev. 4 CM-8</td>
</tr>
<tr>
<td>TIER 4</td>
<td>Adaptive</td>
<td>ID.AM-2: Software platforms and applications within the organization are inventoried</td>
<td>CCS CSC 1&lt;br&gt;COBIT 5 DSS05.02&lt;br&gt;ISA 62443-2:1:2009 4.2.3.4&lt;br&gt;ISO/IEC 27001:2013 A.13.2.1&lt;br&gt;NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, FL-8</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-3: Organizational communication and data flows are mapped</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-4: External information systems are categorized</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

bsi.
Pictorial Scope (Example)

Service-level Agreement (SLA)

Operational-level Agreement (OLA)

Out of Scope – External but interrelated

Out of Scope – Internal but interrelated

All processes, activities within the ownership & control of the scope stakeholders

All processes controlled outside the MS but within the company

All processes controlled outside the company

Scope

Regulators

Utilities

Insurers

Human Resources

Marketing

Product Support

Society

Suppliers

Distributors

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators

Pictorial Scope

(Society)

Out of Scope

– External

but

interrelated

All processes,
activities within
the ownership &
control of the
scope

out of

control

stakeholders

All processes
controlled
outside the MS
but within the
company

All processes
controlled
outside the
company

Society

Distributors

Suppliers

Insurers

Utilities

Human Resources

Marketing

Product Support

Regulators
Why ISO/IEC 27001?
Why did we choose ISO/IEC 27001?

Information Resilience

Knowledge Solutions
Assessment Services
Training
Product Certification
Medical Devices
Supply Chain Solutions
EHS Solutions
Cybersecurity and Information Resilience

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
Typical ISO/IEC 27001 Statement Of Applicability (SOA)

### Statement of Applicability

Legend (for selected Control Objective and Control selection)
- **Current Control:** Critical in the current environment
- **Selected Controls:** Critical in the current environment
- **Justification:** Critical in the current environment
- **Overview of Implementation:** Critical in the current environment

#### IS/IEC 27001:2013 Controls

<table>
<thead>
<tr>
<th>Clause Title</th>
<th>N</th>
<th>Control Objective/Control</th>
<th>Control Details</th>
<th>HIPAA Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS Information security policies</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5.1.1 Policy for information security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5.2.2 Response to incidents or breaches</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.5.3 Business continuity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### A.6 Organization of IS governance

<table>
<thead>
<tr>
<th>Clause Title</th>
<th>N</th>
<th>Control Objective/Control</th>
<th>Control Details</th>
<th>HIPAA Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.6.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6.1.1 Role and responsibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6.1.2 Organizational objectivity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6.2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6.2.1 Hardware security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.6.2.2 Software security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### A.7 Information security management

<table>
<thead>
<tr>
<th>Clause Title</th>
<th>N</th>
<th>Control Objective/Control</th>
<th>Control Details</th>
<th>HIPAA Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.7.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.7.1.1 Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.7.1.2 Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### A.8 Information security management

<table>
<thead>
<tr>
<th>Clause Title</th>
<th>N</th>
<th>Control Objective/Control</th>
<th>Control Details</th>
<th>HIPAA Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.8.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.8.1.1 Information security management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Function

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance (GD)</td>
<td></td>
</tr>
<tr>
<td>ID-GV: Organizational information</td>
<td></td>
</tr>
</tbody>
</table>

#### Controls

- ID-BE: The organization's role in the supply chain is identified and communicated
- ID-BE-2: The organization's role in the supply chain is identified and communicated
- ID-BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
- ID-BE-4: Dependencies and critical functions for delivery of critical services are established
- ID-BE-5: Resilience requirements to support delivery of critical services are established
BSI’s Journey in development of Certification to the Cyber Security Framework
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.
Development Timeline

- **2014**
  - NIST Inquiry about Modeling
- **April 2015**
  - Presentation at NIST of model
- **August 2016**
  - RFI Issued by BSI
- **May 2017**
  - Presented at NIST Workshop
- **Q4 2016**
  - Revised Model
- **November 2017**
  - Ran Pilot Program
- **March 2018**
  - Launched NCSF Certification
- **July 2018**
  - First Certification
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
Certification Scope of NIST CSF

It is required that certification scope of NIST CSF shall be included in the certification scope of ISO/IEC 27001.
### 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.

<table>
<thead>
<tr>
<th>Audit type</th>
<th>Audit Time for NIST CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extension to NIST CSF in conjunction with ISO/IEC 27001 IA, CAV or RA</td>
<td>Initial Certification Audit Time for ISO/IEC 27001 x</td>
</tr>
<tr>
<td>Special Audit to extend to NIST CSF</td>
<td>Plus X day to the above</td>
</tr>
<tr>
<td>Subsequent RA for NIST CSF</td>
<td>RA Audit Time for ISO/IEC 27001 x</td>
</tr>
<tr>
<td>Subsequent CAV for NIST CSF</td>
<td>CAV Audit Time for ISO/IEC 27001 x</td>
</tr>
<tr>
<td>Score</td>
<td>1 to 3</td>
</tr>
<tr>
<td>-------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>No formal approach</td>
</tr>
<tr>
<td>Evidence / Definition</td>
<td>1. There is some evidence of a system in place to manage the control area.</td>
</tr>
<tr>
<td>Managed</td>
<td>2. There is some evidence of either a documented system or an accepted way of working is in place.</td>
</tr>
<tr>
<td>Followed / Effective</td>
<td>3. There is some evidence of an accepted way of working that is broadly understood and followed.</td>
</tr>
</tbody>
</table>
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

Holder Certificate number: NIST 676578

and operate a Quality Management System which complies with the requirements of NIST
accreditation.

For and on behalf of BSI:

Andrew Lawson, EMEA Systems Certification Dir

Original Registration Date: 2019-02-15
Latest Revision Date: 2020-03-15

Effective Date: 2019-02-15
Expiry Date: 2022-02-15

NIST CSF
IDENTIFY PROTECT RECOVER
DETECT RESPOND

This certificate was issued electronically and remains the property of BSI and is issued by the controller of copyright.
An electronic certificate can be viewed at www.bsi-global.com/BSI-Certificate

BSI Assurance Ltd, registered in England under number 0906565 at 10a Chancery Lane, London WC2A 1LS, UK.
A Member of the BSI Group of Companies.
Ribose Case Study

Integrating the NIST Framework into the organizational culture and proving effectiveness
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.
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
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
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

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

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

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

Regional

**World’s first Singapore MTCS**
(highest Level 3)

First non-China-based C-STAR

Cloud

First SaaS

Only CSP triple-assured by CSA

World’s first STAR Attestation

First cloud provider

... and more security
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.
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.
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!
Implementer’s view: CSF takes a more holistic approach than ISO/IEC 27001

<table>
<thead>
<tr>
<th>Orientation</th>
<th>ISO/IEC 27001</th>
<th>NIST CSF</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Process-oriented</td>
<td>Outcome-oriented</td>
</tr>
<tr>
<td>Action drivers</td>
<td>Risk-driven control requirements</td>
<td>Focused on risk mitigation</td>
</tr>
<tr>
<td>Approach</td>
<td>Prescriptive, management system</td>
<td>Adaptive, risk-driven</td>
</tr>
<tr>
<td></td>
<td>Rule-based</td>
<td>Open to prioritization, improvise</td>
</tr>
<tr>
<td>Mantra</td>
<td>“What you have to do”</td>
<td>“What you want achieved”</td>
</tr>
</tbody>
</table>

SMBs often find ISO/IEC 27001 too complex to apply. CSF gives them a good start.
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
We found CSF useful for setting *context* for ISMS: risk and desired outcomes

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Processes and activities</th>
<th>Desired outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Framework Core:</strong></td>
<td><strong>ISO/IEC 27001 ISMS</strong></td>
<td><strong>Framework Profile:</strong></td>
</tr>
<tr>
<td>• Basic, necessary outcomes</td>
<td>• degree of profile satisfaction</td>
<td>• <em>desired satisfaction of outcomes</em></td>
</tr>
<tr>
<td>• Common cybersecurity activities</td>
<td>• “self-comparing” mechanism to measure and improve achievement of cybersecurity objectives</td>
<td>• the <em>target state</em>, the SOA</td>
</tr>
<tr>
<td>• Open-ended outcomes allow better prioritization</td>
<td></td>
<td>• driven by organizational context</td>
</tr>
</tbody>
</table>

*CSF*
CSA DevSecOps WG’s “six pillars” of Agile Security facilitates CSF alignment

DevSecOps: achievement of information security through DevOps practices.

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!
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