The NIST Cybersecurity Framework – Measuring Compliance
What is the NIST Cybersecurity Framework?

Why YOU should care?

How would I apply it?

How would I measure my effectiveness?
Without a Security Framework...
The Survey Says...

Security Frameworks guide the way...
- 84% Leverage a security framework
- Broad range of company sizes

Wide Range of Frameworks Utilized
- 44% used more than one framework
- EOY 2016 - CSF (43%), CIS (44%) ISO (44%)

Best practice & requirements drive CSF adoption
- 70% adopted CSF because they consider it best practice
- 29% adopted CSF because a partner required it

Security Framework Adoption is a Journey
- Only 1 in 5 rank their organization as very mature
- More than half of CSF adopters require significant investment to fully conform

Survey conducted by Dimensional Research, March 2016
316 IT and Security Professionals interviewed in US
The National Institute of Standards (NIST) Cybersecurity Framework is...

- Repeatable
- Flexible
- Performance based
- Technology Neutral
- Cost Effective
- Measurable!

- Common Language

New & Improved

RSA Conference 2016 Singapore
Objectives of CSF in a nutshell

Communicate Risk

Describe Current Security Posture

Describe Target Security Posture

Assess Progress towards Target Posture

Continuous Improvement

IT WAS BAD ENOUGH FOR SISYPHUS BEFORE THE GODS ADDED A CIRCUS POODLE.
# RSAC

## Framework Profile
*(Where you are and where you want to go)*
- Defines (measures) current state
- Defines (measures) desired state

## Framework Implementation Tiers
*(How you view cybersecurity)*
- Tiers (4) that show how cybersecurity risks and processes are viewed within an organization
- Required Tier based on perceived risk/benefit analysis

## CSF Core
*(What it does)*
- Identify
- Protect
- Detect
- Restore
- Recover

---

The Cyber Security Framework at 40,000 feet...
CSF Component 1 – Framework Core

- Identify
- Detect
- Protect
- Recover
- Respond

Framework Core
## Structure

<table>
<thead>
<tr>
<th>Function Unique Identifier</th>
<th>Function</th>
<th>Category Unique Identifier</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.BE</td>
<td>Business Environment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.GV</td>
<td>Governance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RA</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.RM</td>
<td>Risk Management Strategy</td>
</tr>
<tr>
<td>PR</td>
<td>Protect</td>
<td>PR.AC</td>
<td>Access Control</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.AT</td>
<td>Awareness and Training</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.DS</td>
<td>Data Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.IP</td>
<td>Information Protection Processes and Procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.MA</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PR.PT</td>
<td>Protective Technology</td>
</tr>
<tr>
<td>DE</td>
<td>Detect</td>
<td>DE.AE</td>
<td>Anomalies and Events</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.CM</td>
<td>Security Continuous Monitoring</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DE.DP</td>
<td>Detection Processes</td>
</tr>
<tr>
<td>RS</td>
<td>Respond</td>
<td>RS.RP</td>
<td>Response Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.CO</td>
<td>Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.AN</td>
<td>Analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.MI</td>
<td>Mitigation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RS.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td>RC</td>
<td>Recover</td>
<td>RC.RP</td>
<td>Recovery Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.IM</td>
<td>Improvements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RC.CO</td>
<td>Communications</td>
</tr>
<tr>
<td>Function Unique Identifier</td>
<td>Function</td>
<td>Category Unique Identifier</td>
<td>Category</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>-----------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>ID</td>
<td>Identify</td>
<td>ID.AM-1</td>
<td>Asset Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ID.AM-2</td>
<td>Asset Management</td>
</tr>
</tbody>
</table>
Everything kinda looks the same...
Use CSF as ingredient to Custom Control Framework
Use CSF to “Normalize to Common Language”

Existing Frameworks

ISO/IEC 27001
CIS Critical Security Controls
ISA 62443
NIST Cybersecurity Framework

“Normalization Layer”
CSF Component 2 – Framework Implementation Tiers

- How cybersecurity risks and processes are viewed within organization

- Partial
- Risk Informed
- Repeatable
- Adaptable

Sophistication
CSF Component 3 – Framework Profile

- Presents overview of present and future cybersecurity posture
  - Business Requirements
  - Risk Tolerance
  - Resources

- Used to define current state and desired state
  - Can help measure progress...
Common Language for All Levels

Executive Level
Focus: Organizational Risk
Actions: Risk Decision/Priority

Process Level
Focus: Risk Management
Actions: Select Profile, Allocate budget

Operations Level
Focus: Risk Management
Actions: Secure Infrastructure, Implement Profile

- Implementation Progress
- Vulnerabilities, Threats, Assets
- Framework Profile
- Priorities Risk Appetite Budget

RSA Conference 2016 Singapore
Process

Prioritize and Scope
- Business Objectives
- Priorities
- Strategy

Orient
- Related Systems
- Assets
- Regulations

Risk Assessment
- Exposure
- Tolerance

Create Current Profile
- Where you are now

Create Target Profile
- Where you need to be

Gap Analysis
- Delta between Current/Target

Action Plan
- MEASURE
How is CSF Different?

- Expresses cybersecurity activities in a common language

- Leverages existing standards – does not reinvent the wheel – can map existing processes/guidelines into CSF

- Provides crucial guidance for reinforcing security controls while maintaining a focus on business objectives

- Provides a vehicle to effectively measure cybersecurity effectiveness independent of existing framework
How does CSF help you?

CSF helps you to do all these great things...

- Reduce chance of breach, liability
- Ability to know status “on the fly”
- Communicate adherence to business, business partners, customers and auditors
- Meet contractual obligations
- Prioritize, evaluate security investments
- Reduce resource drain and impact of multiple audits
The CSF is an absolute minimum of guidance for new or existing cybersecurity risk programs...

*Gartner webinar: Using the NIST Cybersecurity Framework, https://www.gartner.com/user/registration/webinar?resId=3163821*
By 2020, more than 50 percent of organizations will use the NIST Cybersecurity Framework, up from the current 30 percent in 2015.

To MEASURE, you need DATA...
...and MORE DATA...
Ingredients to Measuring Compliance

- Endpoint Assessment
- Network Monitoring
- Event Monitoring
- Analytics
Continuous Monitoring

Complete Visibility of all Assets, all the Time
<table>
<thead>
<tr>
<th>Assurance Report Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSF DETECT. Continuous Monitoring (DE.CM)</td>
</tr>
<tr>
<td>CSF IDENTIFY. Governance (ID.GV)</td>
</tr>
<tr>
<td>CSF Network Defense (PR.AC and PR.PT)</td>
</tr>
<tr>
<td>CSF PROTECT. Access Control (PR.AC)</td>
</tr>
</tbody>
</table>

RSA Conference 2016 Singapore
Assurance Report Cards

**CSF DETECT: Continuous Monitoring (DE.CM)**

**CSF IDENTIFY: Governance (ID.GV)**
- 1. At least 95% of actively and passively detected systems have been scanned for compliance in the past 90 days
- 2. Less than 25% of compliance checks failed on Windows, Linux, Solaris and Mac OS machines
- 3. Less than 5% of secure configuration compliance checks failed
- 4. Less than 5% of anti-malware compliance checks failed
- 5. Less than 5% of data protection compliance checks failed
- 6. Less than 5% of login configuration compliance checks failed
- 7. Less than 5% of default account/password compliance checks failed
- 8. Less than 5% of least privilege compliance checks failed
- 9. Less than 5% of database compliance checks failed
- 10. Less than 5% of web server compliance checks failed
- 11. Less than 5% of remote access compliance checks failed
- 12. Less than 5% of removable media and USB compliance checks failed
- 13. Less than 5% of wireless compliance checks failed

**CSF Network Defense (PR.AC and PR.PT)**

**CSF PROTECT: Access Control (PRLAC)**
<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Family</th>
<th>Severity</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000001</td>
<td>7.1.1 Set Password Expiration Days</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000002</td>
<td>7.1.2 Set Password Change Minimum Number of Days</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000018</td>
<td>1.1.2 Set noexec option for /tmp Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000019</td>
<td>1.1.3 Set nosuid option for /tmp Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000020</td>
<td>1.1.4 Set noexec option for /tmp Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000021</td>
<td>1.1.5 Create Separate Partition for /var</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000022</td>
<td>1.1.6 Bind Mount the /var/tmp directory to /tmp</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000027</td>
<td>1.1.11 Add noexec Option to Removable Media Partitions</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000030</td>
<td>1.1.14 Add nosuid Option to /dev/shm Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000031</td>
<td>1.1.15 Add nosuid Option to /dev/shm Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
<tr>
<td>1000032</td>
<td>1.1.16 Add noexec Option to /dev/shm Partition</td>
<td>N/A</td>
<td>High</td>
<td>7</td>
</tr>
</tbody>
</table>
## 1.1.3 Set nosuid option for /tmp Partition (1000019)

### Solution
Edit the /etc/fstab file and add nosuid to the fourth field (mounting options). See the fstab(5) manual page for more information.

### Audit File
auditFile.CSIsexoy

### Information
The nosuid mount option specifies that the filesystem cannot contain set userid files.

### Rationale
Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create set userid files in /tmp.

### Policy Value

<table>
<thead>
<tr>
<th>Actual Value:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The file <code>/etc/fstab</code> does not contain <code>^([^a-zA-Z0-9])</code></td>
<td></td>
</tr>
</tbody>
</table>
CSF: Malware
Combating malware on the network often seems to be a never-ending battle. Network defenders need to use a defense-in-depth approach to both protect against malware infections and also discover and address any malware that gets through the defenses. This dashboard aligns with the NIST Cybersecurity Framework (CSF) subcategories that deal with malware, unauthorized mobile code, and the improvement of network defenses.

Updated: Mar 24, 2016

CSF: User Access and Least Privilege
User account management, access control, and enforcement of least privilege are critical to effective network security. Without these, the risk of network invasion and compromise, insider activity, and data loss is increased. This dashboard aligns with the NIST Cybersecurity Framework (CSF) subcategories that deal with user account management, credential management, and least privilege.

Updated: Feb 24, 2016

CSF: Continuous Monitoring
How do you know what’s happening on your network? Continuous network monitoring helps an organization maintain ongoing awareness of its network and security. This dashboard aligns with the multiple NIST Cybersecurity Framework (CSF) subcategories that deal with continuous monitoring, anomaly detection, and log correlation and analysis.

Updated: Feb 24, 2016

CSF: Compliance and Device Hardening
Compliance and regulatory changes can be challenging for any organization to manage effectively. Not only do organizations have to keep systems updated with the latest patches, systems also need to be hardened to reduce the attack surface. This dashboard aligns with the NIST Cybersecurity Framework (CSF) PRP-1, PRI-7, and ID.003-3 subcategories, which provide a series of system configuration, compliance, and device hardening checks, along with specific industry standards and regulation checks.

Updated: Feb 24, 2016

CSF: Secure Development
Vulnerabilities in applications and application development can be a great risk to an organization. Development tools that are accessible in insecure locations could allow an intruder to modify code and functionality for malicious purposes. This dashboard aligns with the NIST Cybersecurity Framework (CSF) subcategory PRP-2 that deals with secure development and life cycle management.

Updated: Feb 24, 2016
CSF: Compliance and Device Hardening

Compliance and regulatory changes can be challenging for any organization to manage effectively. Not only do organizations have to keep systems updated with the latest patches, systems also need to be hardened to reduce the attack surface. This dashboard aligns with the NIST Cybersecurity Framework (CSF) PR. IP-1, PR. IP-7 and ID. GV, subcategories, which provide a series of system configuration, compliance, and device hardening checkpoints to strengthen information security frameworks within organizations.
CSF IDENTIFY: Governance (ID.GV)

With the increase in governance and compliance regulations, establishing a strong policy to address legal and regulatory compliance requirements is a must. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a set of objectives that address compliance standards, guidelines, and best practices across multiple regulations. This Assurance Report Card (ARC) aligns with the CSF category IDENTIFY: Governance (ID.GV), which recommends understanding, managing, and ultimately applying legal and regulatory cybersecurity requirements to systems within an organization.

- 1. At least 95% of actively and passively detected systems have been scanned for compliance in the past 90 days
- 2. Less than 20% of compliance checks failed on Windows, Linux, Solaris, and Mac OS machines
- 3. Less than 5% of secure configuration compliance checks failed

Plus 10 more statements

CSF PROTECT: Access Control (PR.AC)

Access control is a critical part of every network security plan. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of objectives that allow an organization to build a comprehensive security plan to protect against security threats. This Assurance Report Card (ARC) addresses the user access and least privilege aspects of the NIST Cybersecurity Framework category PROTECT: Access Control (PR.AC), which provides accurate information on the access control measures in use and identifies potentially vulnerable areas that may need to be addressed.

- 1. At least 95% of systems report active user statistics
- 2. Less than 10% of systems using administrative accounts over the network
- 3. Less than 5% of password compliance checks failed

Plus 4 more statements

CSF PROTECT: Data Security (PR.DS)

Data security aims to protect the confidentiality, integrity, and availability of an organization’s information. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of objectives that allow an organization to build a comprehensive security plan to protect against security threats. This Assurance Report Card (ARC) aligns with the data leakage and protection aspects of the NIST Cybersecurity Framework category PROTECT: Data Security (PR.DS), which provides accurate information on the data leakage concerns within the network and potential sources of vulnerability or exposure.

- 1. No data leakage has been detected
- 2. No systems with data leakage events have exploitable vulnerabilities
- 3. No systems with data leakage events communicate outside the network

Plus 7 more statements

CSF PROTECT: Information Protection (PR.IP)

Organizations must ensure that proper processes and procedures are in place to manage protection of information systems and assets. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a set of objectives that allow an organization to build a comprehensive security plan to protect against security threats. This Assurance Report Card (ARC) aligns with the NIST Cybersecurity Framework category PROTECT: Information Protection Processes and Procedures (PR.IP), which will assist an organization in measuring the effectiveness of and improving protection processes and procedures.

- 1. At least 95% of actively and passively detected systems have been audited in the past 90 days
- 2. Less than 20% of compliance checks failed on Windows, Linux, Solaris, and Mac OS machines
- 3. Less than 5% of secure configuration compliance checks failed

Plus 8 more statements
Three Year Action Plan Tool...

http://www.tenable.com/whitepapers/nist-csf-implementation-planning-tool
Apply...

- Automate as much of compliance measurement as possible
- Leverage all possible sources to measure compliance
  - Scan, sniff & log all have something to say
- Consider using CSF as a “common language” for expressing and measuring security up and down within the organization
Contact me:
dbussiere@tenable.com

Website
http://www.tenable.com

blog.tenable.com

tenable.com/podcast

youtube.com/tenablesecurity
discussions.nessus.org