My framework analysis is based on the Heilmeier Catechism.

**An idea is worth pursuing if:**

1. **What are you trying to do?**

**Reduce the probability of material impact due to a cyber event over the next three years.**

**(Source: Cybersecurity First Principles by Rick Howard)**

1. **How is it done today, and what are the limits of the current practice?**

**Pros of the ISO 27001:**

1. **International recognition:** The ISO 27001 framework is recognized and respected around the world, which can be beneficial for organizations that operate globally or that want to attract international customers and partners.
2. **Comprehensive coverage:** The ISO 27001 framework covers a wide range of controls related to information security, including confidentiality, integrity, and availability. This can help organizations identify and address potential vulnerabilities in their systems and processes.
3. **Continuous improvement:**The PDCA cycle at the heart of the ISO 27001 framework encourages organizations to regularly review and improve their controls, which can help them stay ahead of emerging threats and maintain the effectiveness of their ISMS over time.
4. **Establishes a strong foundation for information security:**The ISO 27001 framework provides a comprehensive set of controls that cover all aspects of information security, from risk assessment and management to access controls and incident response. This helps organizations establish a strong foundation for their information security efforts.
5. **Improves security posture:**By implementing the controls in the ISO 27001 framework, organizations can significantly improve their security posture and reduce the risk of data breaches, cyber attacks, and other security incidents.
6. **Demonstrates commitment to information security:** Adopting the ISO 27001 framework demonstrates to customers, partners, and regulatory bodies that an organization is committed to information security and has taken the necessary steps to protect sensitive information.
7. **Improves efficiency:**Implementing the controls in the ISO 27001 framework can help organizations streamline their security processes and improve efficiency by eliminating duplication and inefficiencies.

# Cons of the ISO 27001:

1. **Cost:** Adopting the ISO 27001 framework can be a time- and resource-intensive process, especially for organizations that are starting from scratch. This can include the cost of training personnel, conducting assessments, and implementing new controls.
2. **Complexity:**The ISO 27001 framework is comprehensive, which can make it complex to understand and implement. This can be especially challenging for smaller organizations that may have limited resources and expertise in information security.
3. **Inflexibility:**The ISO 27001 framework is a prescriptive standard, which means that it specifies specific controls that organizations must implement. This can be inflexible for organizations that have unique security requirements or that want to tailor their controls to their specific business needs.
4. **Can be time-consuming and resource-intensive:**Adopting the ISO 27001 framework can be a complex and time-consuming process, requiring the allocation of significant resources to implement and maintain the necessary controls.
5. **Requires ongoing maintenance:**The ISO 27001 framework is based on the PDCA cycle, which means that organizations must continually review and update their controls to ensure that they are effective and aligned with the latest best practices. This requires ongoing maintenance and resources.

**(Source:** [**https://www.songer.pro/iso-27001-pros-and-cons/**](https://www.songer.pro/iso-27001-pros-and-cons/)**)**

1. **What is new in your approach and why do you think it will be successful?**

## Key Updates in CSF 2.0

* **Broadened Scope & Universal Relevance:** One of the most significant updates in CSF 2.0 is broadening its scope to apply to all organizations, including small businesses and higher education institutions. By removing language specific to critical infrastructure, the framework becomes more universally relevant and accessible.
* **New Governance Function:**Introducing a new Govern Function focuses on organizational context, risk management strategy, policies, procedures, and roles. This addition positions cyber risks alongside enterprise risks like financial stability threats and highlights the importance of cybersecurity governance.
* **Inclusion of Supply Chain Risk Management:** The updated framework introduces cybersecurity supply chain risk management outcomes, addressing cybersecurity's crucial but often overlooked aspect. This reflects the growing reliance on external partners, suppliers, and service providers for various aspects of an organization's operations and the potential cyber threats that can originate from or propagate through these third parties.
* **Technology Infrastructure Resilience:** The Protect Function now stresses the importance of resilient technology infrastructure. This update reflects the growing recognition that organizations must prioritize not only the protection of their information assets but also the resilience of the underlying infrastructure that supports these assets. This involves ensuring that technology infrastructure can withstand, recover from, and adapt to cyber threats, incidents, and disruptions.
* **New Focus on Forensics & Learning from Incidents:** The updated framework highlights the significance of incident forensics and response management through new Categories in the Respond and Recover Functions. This increased focus on forensics emphasizes the need for organizations to analyze, learn from, and improve their defenses based on the findings from these investigations.
* **Enhanced Measurement and Assessment:** More guidance on measurement and assessment has been added, providing a common taxonomy and lexicon to communicate the outcome of an organization's measurement and assessment efforts, regardless of the underlying risk management process.
* **Improved Alignment to Other Frameworks:** CSF 2.0 aims to better align with other NIST and non-NIST security programs, such as the Risk Management Framework and Workforce Framework for Cybersecurity. This improved alignment seeks to streamline the adoption of security controls and enable more effective resource allocation.
* **International collaboration:** Recognizing the global nature of cybersecurity threats, NIST aims to increase international collaboration and encourage other countries to adopt the framework in whole or in part, recognizing the global nature of cybersecurity threats and promoting a standardized and widely-accepted set of guidelines and best practices.

## Practical Takeaways

Now that we've explored the key updates in the NIST CSF 2.0 draft let's focus on the practical takeaways that can help your organization strengthen its cybersecurity posture.

* **Assess Your Cybersecurity Governance:** Reevaluate your governance structure and risk management strategies to align with the updated framework.
* **Strengthen Supply Chain Security:**Evaluate your supply chain risk management practices and identify areas for improvement, as these can be potential weak points in your cybersecurity defense.
* **Prioritize Continuous Improvement:**Stay ahead of evolving cyber threats by regularly reviewing and updating your cybersecurity policies and practices.
* Focus on Resilient Infrastructure: Invest in robust technology infrastructure and develop strategies for maintaining resilience in the face of cyber threats.
* **Enhance Incident Response:**Develop and maintain a comprehensive incident response plan that includes incident forensics, mitigation, and recovery, as emphasized by the new Categories in the Respond and Recover Functions.

## ****Conclusion****

The NIST CSF 2.0 draft offers organizations a comprehensive set of guidelines to enhance their cybersecurity posture. Staying informed and proactive is the key to navigating the ever-changing landscape of digital threats. Lastly, remember that the NIST CSF 2.0 is still in development. Your organization can engage in the update process (if it hasn't already) and provide valuable feedback to improve this framework.

**(Source:** [**https://www.linkedin.com/pulse/quick-analysis-nist-csf-20-draft-kris-kimmerle**](https://www.linkedin.com/pulse/quick-analysis-nist-csf-20-draft-kris-kimmerle)**)**

**NIST Cybersecurity Framework (CSF) 2.0 Reference Tool:** [**https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters**](https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters)

**Cybersecurity First Principles:** [**https://firstprinciples.thecyberwire.com/cybersecurityfirstprinciplesbook**](https://firstprinciples.thecyberwire.com/cybersecurityfirstprinciplesbook)

1. **Who cares? If you are successful, what difference will it make?**

**Primary Business Drivers and Needs**

**What is the Treasury’s core business?**

**How is Treasury’s success measured?**

**Concerns, Questions, etc.**

**How might elements of your program feel as though they work against Treasury’s core mission and values?**

**Might elements of your program feel as though they take focus from areas that Treasury is measured against?**

**Benefits if the program is successful**

**How might elements of your program make the Treasury Department look good?**

**How might elements of your program make the Treasury Department perform better?**

**How might elements of your program help the Treasury Department link to the State’s mission and goals?**

1. **What are the risks?**

**Table 7.4 Linking KRIs with KPIs Source (The CISO Evolution pgs. 223-224)**

|  |  |  |
| --- | --- | --- |
| **KPI (Input)** | **KRI(Output)** | **Implication/Business Impact** |
| Number of identified regulations, policy, or process violations | Percentage of incidents involving customer personal data | This indicates a failure to meet compliance obligations and might lead to scrutiny from regulators or media, adversely impact the reputation of the Treasury. |
| Number of security-related service downtimes | Number of services cancelled or delayed as a result of security-related service downtimes | Security incidents impacting critical systems potentially cause service interruption or degradation. |
| Number of business applications/systems not supported by a backup plan. | Percentage of business applications/systems not supported by a backup plan | Lack of data backup for business applications/systems leads to data loss and adversely affects service continuity in case of any interruption. |
| Percentage of nonconformities detected in security tests/audits, but not resolved within the timeframe planned | Number of nonconformities detected in security tests/audits remaining unresolved beyond the planned timeframe | Delay in remediating vulnerabilities detected in security tests/audits makes the organization an easy target for malicious attacks. |
| Inadequate third-party management | Number of security incidents attributed to vulnerabilities in third-party systems/employees | The organization’s information can be exposed to risk by third parties with inadequate information security management. |
| Lack of adequate time frame for scheduled downtime of systems | Number of systems without up-to-date patches | Delay in patching the systems makes the organization an easy target for malicious attacks. |
| Lack of review of risk management processes | Lack of effective reporting of key risk | In the absence of a review of risk management processes, these processes may continue to be ineffective, resulting in nonidentification of vulnerabilities/risk. |

1. **How much will it cost?**
2. **How long will it take?**

**Present findings to Treasury Security leadership by 01/15/2024 with a recommendation of which framework will be best for Treasury and why.**

**In the remaining IPP period, running from approximately 02/01/2024 – 08/31/2024, work to implement the chosen framework within the Treasury department.**

1. **What are the mid-term and final “exams” to check for success?**

**Mid-Term**

1. Research the current Cyber Security Frameworks to be considered to replace the current framework.

2. Develop a pros and cons list evaluating each framework

3. Research implementation guidelines

4. Analyze any costs that may be associated with the frameworks

5. Present findings to Treasury Security leadership by 01/15/2024 with a recommendation of which framework will best for Treasury and why

**Final exam**

In the first quarter of employment a Cyber Security Framework was chosen. In the remaining IPP period, running from approximately 02/01/2024- 08/31/2024, work to implement the chosen framework within the Treasury department.

1. Document the process of applying the framework to a control and a test.
2. Create a control document in the relating it to the Treasury environment.
3. Create a test case that can demonstrates adherence to the control.
4. Review the control and test case with Security leadership.
5. Create a schedule for control review and testing the control.