Prompt: I need a one-page synopsis of the differences between the NIST Cybersecurity Framework 1.1 and 2.0

The NIST Cybersecurity Framework (CSF) 2.0 introduces several important changes and enhancements compared to version 1.1, with a focus on broader applicability, governance, and practical implementation guidance.

Framework Structure

- CSF 1.1 consisted of five core functions: Identify, Protect, Detect, Respond, and Recover.
- CSF 2.0 refines these five and adds a sixth, "Govern," emphasizing comprehensive governance and executive involvement in cyber risk management.
- The new structure makes the framework more intuitive and user-friendly, with clearer outcomes for each function.

Emphasis on Governance

- Version 1.1 was mostly outcome-focused with less emphasis on who manages cybersecurity risks.
- The new Govern function in 2.0 highlights the importance of integrating cybersecurity into overall organizational governance and strategic risk management.
- Roles, responsibilities, authorities, and policies for cybersecurity are now clearly addressed, supporting organization-wide engagement beyond IT.

Broader Applicability and Integration

- CSF 1.1 primarily targeted U.S. critical infrastructure.
- CSF 2.0 is designed for all organizations worldwide, regardless of size, industry, or sector, reflecting universal threats and global best practices.
- Guidance on integrating the CSF with other frameworks (such as NIST SP 800-53, NIST Privacy Framework, and Secure Software Development Framework) has been expanded.

Implementation Guidance and Usability

- CSF 1.1 provided general recommendations for cybersecurity practices.

Commented [AE1]: This change was needed to highlight the importance of governance in an organization dealing with cyber threats. Since cybersecurity is more than just a technical issue, it needs to be focused on by more than just IT in an organization. This structure plainly emphasizes that expectation.

Commented [AE2]: This change added an increased emphasis on who owns different aspects of cybersecurity in an organization. Strong leadership from the executive level is needed to ensure proper security in a business. This component gives buy-in from other arms of a business, while also emphasizing its importance.

Commented [AE3]: This change helped to diversify the use of the CSF. Rather than expecting its use to be limited to American needs and any adaptations on other groups, this is ready out of the box. By making the CSF less specialized, it increases adoption worldwide, strengthening security and making attacks more difficult.

- CSF 2.0 introduces “Implementation Examples” and detailed, sector-specific case studies to help organizations apply the framework more effectively to their specific needs.
- The framework’s language and guidance have been clarified, making it more actionable and easier to use.

Supply Chain and Privacy

- CSF 2.0 places increased focus on supply chain risk management and privacy within the governance and identify functions.
- It encourages thorough assessment and monitoring of third-party risks and better alignment with evolving privacy requirements.

Continuous Improvement

- Both versions acknowledge ongoing improvement, but CSF 2.0 expands this focus with new categories, referencing tools like NIST SP 800-55 for performance measurement, and supporting the cycle of assessment, learning, and enhancement.

Key Comparison Table

Aspect	CSF 1.1	CSF 2.0
Core Functions	Identify, Protect, Detect, Respond, Recover	Govern, Identify, Protect, Detect, Respond, Recover
Governance Focus	Limited	Dedicated “Govern” function, executive & board oversight
Target Audience	U.S. critical infrastructure	Global, all orgs & sectors
Integration Guidance	Minimal	Enhanced framework integration guidance
Supply Chain/Privacy	Limited in scope	Explicitly included and strengthened
Implementation Support	General	Detailed examples/case studies, clarity
Continuous Improvement	Acknowledged	Expanded and explicit guidance

Commented [AE4]: This change helped to make implementation easier for organizations. This makes the barrier of entry to being properly secured lower, and provides support to ensure that the CSF is working in the best way possible. This ease of use further encourages adoption of the CSF.

Commented [AE5]: This change brings awareness to supply chain security that was largely neglected. Lessons learned previously show that supply chain security is just as necessary as first party security to prevent compromises and disruptions. A large organization keeping a supplier accountable in their cyber practices keeps both organizations protected.

Commented [AE6]: This change helps to emphasize continuous improvement in organizations since cybersecurity is an ever-evolving field. New threats are developed daily and an organization is never fully protected if improvements are not made periodically. A cycle of assessment, learning, and enhancement make sure that security does not lapse due to ignorance.