HITRUST CSF® v11.3.0 Summary of Changes

Version 11.3.0

HITRUST®

April 2024

HITRUST is committed to keeping the CSF current to meet the needs of organizations by regularly updating the CSF to integrate and normalize industry standards, requirements, and other authoritative sources.

The addition of several key authoritative sources in the CSF framework is an important part of the HITRUST cyber threat-adaptive approach to keep the framework relevant and up-to-date to reduce risk by proactively updating the control library. In addition, the power of AI in the CSF development toolkit enables adding and mapping new authoritative sources faster and more accurately than ever.

Benefits of Adding Authoritative Sources to the HITRUST CSF:

- To remain current with evolving industry standards and regulations.
- To keep the CSF comprehensive so it meets multiple organizational needs.
- To include and harmonize emerging standards and mappings to stay ahead of cyber threats.
- To satisfy market demand for additional HITRUST Insights Reports.

The HITRUST CSF v11.3.0 release contains the following enhancements:

Authoritative Source updates:

- Added FedRAMP r5 mapping and selectable Compliance factor, “FedRAMP r5”
- Added StateRAMP r5 mapping and selectable Compliance factor, “StateRAMP r5”
- Added TX-RAMP r5 mapping and selectable Compliance factor, “TX-RAMP r5”
- Added FFIEC CAT mapping and selectable Compliance factor, “FFIEC CAT”
- Added CIS v8 mapping and added a selectable Compliance factor, “CIS v8”
    - The existing CIS v7.1 Compliance factor, “CIS CSC v7.1” will not be selectable as of v11.3.
- Added MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) Mitigations [MITRE ATLAS]
- Added OWASP AI Exchange mapping and added a selectable Compliance factor, “OWASP AI Exchange”
- Added: NIST SP 800-172 “Enhanced Security Requirements for Protecting Controlled Unclassified Information”
- Added HHS Cybersecurity Performance Goals mapping and added a selectable Compliance factor, “HHS Cybersecurity Performance Goals”
- Added PCI DSS v4 mapping and selectable Compliance factor, “PCI DSS v4”
    - The existing PCI DSS v3.2.1 Compliance factor, “PCI DSS v3.2.1” will not be selectable as of v11.3.

- Added 23 NYCRR 500 Second Amendment mapping and selectable Compliance factor, “23 NYCRR 500 Second Amendment”
    - The existing 23 NYCRR 500 Compliance factor, “23 NYCRR 500” will not be selectable as of v11.3.
- Added HICP 2023 edition mapping and selectable Compliance factor, “HICP 2023”
    - The existing HICP Compliance factor, “HICP” will not be selectable as of v11.3.
- Refreshed GDPR mapping and selectable Compliance factor, “GDPR”
- Refreshed Singapore PDPA mapping and selectable Compliance factor, “PDPA (Singapore)”
- Additionally, minor enhancements were made to the NIST SP 800-53 R5 mapping based on NIST SP 800-53 Release 5.1.1, which included one new control (IA-13) and three control enhancements.

Relevant Notes:

- The addition of NIST SP 800-172, “Enhanced Security Requirements for Protecting Controlled Unclassified Information” is included in the CSF v11.3.0 because it contains highly rigorous controls to further safeguard organizations that are at the highest level of risk within their HITRUST r2 Assessment tailoring.
- In light of recent cyber threat events, the addition of stringent NIST SP 800-172 standards is another example of HITRUST taking the initiative to keep our framework cyber threat-adaptive to help healthcare and other segments safeguard critical infrastructure.

  NIST SP 800-172 inclusion also lays important groundwork for addressing new CMMC Level 3 requirements, which will be based on this standard.
- The “RAMP” authoritative sources provide a standardized approach and are included to ensure that assessed entities doing business with the government comply with applicable information security requirements.
- The inclusion of MITRE ATLAS as a selectable factor will enable the inclusion of key AI security requirements that are fundamental to the mitigation of techniques that target AI systems.
- HHS Cybersecurity Performance Goals are a voluntary subset of cybersecurity practices healthcare organizations can prioritize to strengthen cyber preparedness, and HICP 2023 is an update with best practices for managing cyber threats to safeguard patient safety.

Reduces r2 Assessment Effort

In addition to the Authoritative Source updates, HITRUST is continuing our consolidation effort to reduce requirement statement redundancy within the CSF. As a result of our control reference level coverage analysis, CSF v11.3.0 has moved 47 requirements out of Levels 2 and 3 and into segments. This significant change reduces the average r2 assessment size without impacting overall control coverage.

Additional Information:

- r2 assessments can still be generated in v11.2.0 despite the release of v11.3.0.
- Effective April 16, 2024, the ability to create new e1 and i1 assessment objects, including i1 rapid recertification assessments, in MyCSF using CSF v11.2 has been disabled.
- Existing e1 and i1 assessments using CSF v11.2 can continue to be submitted after April 16, 2024.
- There will be no impact on an existing assessment unless the organization and assessor firm determine that the modifications to certain requirement statements and illustrative procedures in v11.3.0 are appropriate for the scope and requirements of the assessed entity.
- A reason an organization would move to v11.3.0 is to take advantage of the authoritative source enhancements (r2 only).

Download the HITRUST CSF v11.3.0.

THANK YOU

855.HITRUST (855.448.7878)

www.HITRUSTAlliance.net

HITRUST®