BAKER TILLY

HITRUST CSF™ Version 9: Updates and impacts for certification

HITRUST™ announced that version 9 of the HITRUST CSF™ is now available. The updated version of the HITRUST CSF™ includes 75 controls required for HITRUST CSF™ Certification, an increase of nine controls from the 66 previously required under version 8.1.

Taking a closer look at the increase in the controls required for HITRUST CSF™ Certification, HITRUST™ has actually removed 10 controls that were previously required for certification under version 8/8.1 and then added 19 controls as required that were previously not required.

Summary of HITRUST CSF™ Version 9 control changes

Newly required (+19 controls)

- ✕ **01.l** Remote Diagnostic and Configuration Port Protection
- ✓ **03.d** Risk Evaluation
- ✓ **05.h** Independent Review of Information Security
- ✓ **05.j** Addressing Security with Customers
- ✓ **06.c** Protection of Organizational Records
- ✓ **06.h** Technical Compliance Checking
- ✓ **09.b** Change Management
- ✓ **09.k** Controls Against Mobile Code
- ✓ **09.l** Backup
- ✓ **09.v** Electronic Messaging
- ✓ **09.x** Electronic Commerce Services
- ✓ **09.y** Online Transactions
- ✓ **09.ad** Administrator and Operator Logs
- ✓ **10.a** Security Requirements Analysis and Specification
- ✓ **10.k** Change Control Procedures
- ✓ **11.d** Learning from Information Security Incidents
- ✓ **12.b** Business Continuity and Risk Assessment
- ✓ **12.d** Business Continuity Planning Framework

No longer required (-10 controls)

- ✕ **01.a** Access Control Policy
- ✕ **01.f** Password Use
- ✕ **01.i** Policy on Use of Network Services
- ✕ **01.r** Password Management System
- ✕ **03.a** Risk Management Program Development
- ✕ **05.b** InfoSec Coordination
- ✕ **09.g** Managing Changes to Third Party Services
- ✕ **09.ac** Protection of Log Information
- ✕ **09.af** Clock Synchronization
- ✕ **10.g** Key Management

BAKER TILLY

Drivers and impact of HITRUST CSF™ version 9 updates

Version 9 now integrates several additional regulatory requirements and industry frameworks, the most notable being the option to complete a NIST Cybersecurity Framework (CsF) assessment. The NIST CsF assessment allows an organization to assess against 185 control requirements, which align with HITRUST CSF™ control requirements, that are required to address the NIST CsF Core Subcategories. The addition of the NIST CsF assessment option will likely be the most globally applicable and relevant of the changes incorporated into version 9, as cybersecurity continues to be a highly scrutinized area for all organizations, regardless of organization size or industry.

Version 9 also incorporates additional updates to address the following specific requirements:

- Federal Financial Institutions Examination Council (FFIEC) Information Security Examination Handbook
- Federal Risk and Authorization Management Program (FedRAMP) for Infrastructure as a Service (IaaS) providers
- Department of Homeland Security (DHS) Critical Resilience Review (CRR) cybersecurity criteria
- Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11) for the Food and Drug Administration (FDA) requirements for electronic records and electronic signatures
- Office of Civil Rights' (OCR) Audit Protocol v2 to help demonstrate HIPAA Security Rule compliance

What HITRUST CSF™ version 9 means for your organization

Organizations that are currently in the process of certifying may continue to submit their validated assessment against version 8.1 for another six months (February 2018). However, organizations that have not already created their validated assessment object within MyCSF, or that will not be completed with their procedures and ready to submit to HITRUST™ within the six-month timeframe, will now generate their assessment and control requirements using version 9.

Baker Tilly can help organizations determine the impact of the version 9 release to their HITRUST™ CSF assessment scope and certification timelines.

For further assistance with your organization's HITRUST™ efforts, please contact our HITRUST services advisors.