Cassandra Lalli

Cybersecurity Test and Validation Scheme

Table of Contents

Technical Controls

In contrast to HIPAA, the HITRUST CSF does not create broad buckets like Administrative and Security controls. The HITRUST CSF is divided into 19 different control domains In addition to the domains above, HITRUST also has 75 control objectives and 156 specific controls (Datica, 2019). With this said below is the following control domains that apply along with the specific controls that New York's Fines will be using for our security architecture, after reviewing all controls it is our understanding that each of these controls will keep our system safe and at low risk.

- Information Protection Program
    - SC-4: Information in Shared System Resources | Multilevel or Periods Processing
    - AC-4: Information Flow Enforcement
    - PM-11: Mission and Business Process
    - PL-2: Develop Security and Privacy Plans for the System
    - PM-7: Enterprise archutextur
    - PM-8:Critical Infrastructure Plan
- Endpoint Protection
    - SC-8:Transmission Confidentiality and Integrity
    - SC-12: Cryptographic Key Establishment and Management
    - SC-13: Cryptographic Protection

- Portable Media Security
    - IR-8: Incident Response Plan
    - MP-4: Media Storage

    - MP-6(3): Media Sanitization | Nondestructive Techniques
    - MP-7; Media Use
    - MP-5: Media Transport
- Mobile Device Security
    - AC-19: Access Controle for Moblie Devices
    - PL-4(1): Rules of Behavior | Social Media and External Site/ Application Usage Restrictions
    - AC-19(4): Access Control for Mobile Devices | Restrictions for Classified Information
    - AC-19(5): Access Control for Mobile Devices | Full Device or Container-Based Encryption
    - CM-2(2): Baseline Configuration| Automation Support for Accuracy and Currency

- Wireless Security
    - AC-2: Account Management
    - AC-3: Access Enforcement
    - CA-9: Internal System Connections
    - IA-2: Identification and authentication (Organizational Users)
    - IA-3: Device Identification and Authentication
    - IA-8: Identification and Authentication
    - PL-4: Riles of Behavior
    - SC-40: Wireless Link Protection

- SC-43: Usage Restriction
- SI-4: System Monitoring

- Configuration Management
  - SA-4(5); Acquisition Process | System, Component and Service Configuration
  - CM-3: Configuration Chang Controle
  - CM-9: Configuration Management Plan
  - SA-10: Developer Configuration Management

- Vulnerability Management
  - AC-17(4): Remont Access | Privileged Commands and Access
  - AC-6: Least Privilege
  - SC-12: Session Termination
  - SC-13: Supervision and Review-Access Controle

- Network Protection
  - CM-7: Least Functionality
  - AC-4(15): Information Flow Enforcement | Detection of Unsanctioned Information
  - AC-6(3): Least Privilege | Network Access to Privileged Commands
  - CS-10: Network Disconnection

- Transmission Protection
    - AC-12(2): Session Termination| Termination Message
    - SI-15: Information Output Filtering
    - AC-16(5): Security and Privacy Attributes| Attribute Displays on Objects to be Output
    - CA-3(6): Information Exchange | Transfer Authorizations
    - CM-6: Configurations Settings

- Password Management
    - IA-5: Authenticator Management
    - IA-5(1): Authenticator Management | Password-based Authentication
    - IA-5(8): Authenticator Management | Multiple System Accounts
    - IA-5(4): Authenticator Management | Automated Support for Password Strength Determination
    - IA-5(18): Authenticator Management | Password Managers
    - SI-11:Error Handling

- Access Control
    - AC-13: Supervision and Review — Access Control
    - AC-3(7) : Access Enforcement | Role-based Access Control
    - AC-6(2)-AC-6(10) : Least Privilege Controles

- Audit Logging & Monitoring

    - AC-11:
    - AC-17(1): Employ automated mechanisms to monitor and control remote access methods.
    - AU-12-AU-12(4) : Audit Record Generation

- Education, Training, and Awareness
    - PM-14: Testing, Training, and Monitoring
    - PM-16: Threat Awareness Program
    - PM-12: Insider Threat Program

- Third-Party Assurance
    - SC-7: Boundary Protection
    - SR-6: Resource Availability

- Incident Management
    - IR-4(1)- IR-4(15) : Incident Handling

- Business Continuity & Disaster Recovery
    - CP-2(1): Contingency Plan | Coordinate with Related Plans
    - CP-4(1): Contingency Plan Testing | Coordinate with Related Plans
    - CP-8(4): Telecommunications Services | Provider Contingency Plan
    - IR-3(2): Incident Response Testing | Coordination with Related Plans
- Risk Management

- PM-4: Plan of Action and Milestones Process
- PM-7: Enterprise Architecture
- PM-9: Risk Management Strategy

- Physical & Environmental Security
  - PE-23: Facility Location

- Data Protection & Privacy
  - SA-8(18): Security and Privacy Engineering Principles | Trusted Communications Channels
  - SC-8: Transmission Confidentiality and Integrity
  - SC-12:Cryptographic Key Establishment and Management | PKI Certificates
  - SC-13: Cryptographic Protection | FIPS-validated Cryptography

Cases Study

The following case study was made by the New Yorks Fines cybersecurity team, in this test we have reached a strong maturity, the number represents the order in which the test was performed, the name represents the control domain that was tested (please see above for which specific controls were tested in their respective domain). Technique stands for the method with which each domain was tested, and lastly the pass or fail criteria in which the test final results are displayed below.

#	Name	Technique	Test Result

1	Information Protection Program	Social Engineering Documentation Review	Pass
2	Endpoint Protection	Penetration Testing	Fail
3	Portable Media Security	Documentation Review	Pass
4	Mobile Device Security	Documentation Review	Pass
5	Wireless Security	Penetration Testing	Pass
6	Configuration Management	Ruleset and Security Configuration Review	Pass
7	Vulnerability Management	Password Cracking Social Engineering	Pass
8	Network Protection	Penetration Testing	Pass
9	Transmission Protection	Penetration Testing	Pass
10	Password Management	Password Cracking Social Engineering	Pass
11	Access Control	Ruleset and Security Configuration Review	Pass
12	Audit Logging & Monitoring	Penetration Testing Social Engineering	Pass

		Documentation Review	
13	Education, Training, and Awareness	Social Engineering	Pass
14	Third-Party Assurance	Social Engineering Documentation Review	Pass
15	Incident Management	Social Engineering	Pass
16	Business Continuity & Disaster Recovery	Documentation Review	Pass
17	Risk Management	Password Cracking Social Engineering Documentation Review	Pass
18	Physical & Environmental Security	Social Engineering Documentation Review	Fail
19	Data Protection & Privacy	Penetration Testing Social Engineering	Pass

New Yorks Finest hospital is proud of the hard work in which the cyber team has put in. There were only 2 critical points of failure in the Endpoint Protection and Physical & Environmental Security domain of our architecture. It is our responsibility to make sure our system as a whole can pass with every domain, and will be revising the controls in these areas.

References

Datica. (2019, November 11). *What Are HITRUST Requirements?* Datica. https://datica.com/blog/what-are-hitrust-requirements#:~:text=The%20HITRUST%20CSF%20is%20a,to%20achieve%20and%20maintain%20compliance.

HITrust. (2019). *Risk Analysis Guide for HITRUST Organizations & Assessors* . https://hitrustalliance.net/. https://hitrustalliance.net/uploads/RiskAnalysisGuide.pdf.

Information Technology Laboratory Computer Security Division. (2020). *Release Search - NIST Risk Management Framework: CSRC*. CSRC. https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/controls?version=5.1.

NIST. (2008). *Archived NIST Technical Series Publication* . govinfo. https://www.govinfo.gov/content/pkg/GOVPUB-C13-6c7a70faefc0886fd6368ad878f7487e/pdf/GOVPUB-C13-6c7a70faefc0886fd6368ad878f7487e.pdf.

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008, September 30). *Technical Guide to Information Security Testing and Assessment*. CSRC. https://csrc.nist.gov/publications/detail/sp/800-115/final.