Equity Credit Union

Cybersecurity Update

25 January 2023

bakertilly
now, for tomorrow.

Agenda

1. Overview
2. IT Actions and Improvements
3. Compliance Models

Review Objectives

- Equity Credit Union requested Baker Tilly staff review the currently applied Information Technology controls and vendor provided compliance status.

- Provide the Leadership Team with an updated understanding of the current state of Cybersecurity practices applied by Horn IT.

- Provide the Leadership Team with an update regarding the compliance status and/or controls applied by core vendors, Smart Solutions and Hub Creative.

- Provide an Overview of potential compliance models

Note: System auditing, verification and tests of controls were not completed as part of this review, all information regarding controls and practices were provided by Equity CU staff and their vendors. This summary is for management discussion purposes only and cannot be relied upon by third parties.

Interim IT Reviews 2020 - 2022

Baker Tilly

- Completed and IT General Controls Review During Audit - 2022
- Executive Summary Issued for Website/Application Security Project - 2021

Smart Solutions

- Completed SOC Audits in 2021
- SOC 2 Audit for 2022 in Progress

Hub Creative

- Website, Application and Support Solutions Upgrade
- Applied Security Best Practice Standards

IT Actions & Improvements

2020 - Proposed Actions

Governance

- Improve Policies
- Disaster Recovery

Technical

- Vulnerability Scanning
- Enhanced VPN
- Open DNS
- Software Controls
- Improve Policies
- Disaster Recovery

2022 - Completed Actions

IT CONTROL IMPROVEMENTS SINCE 2020 REPORTING PERIOD

Cyber Control	Security Benefit
Rapid 7 Vulnerability Scanning	Daily scanning of assets for vulnerabilities
Ninja RMM	Improved Monitoring and Control of Endpoints Automatic Patching; Software Control; Reporting; Management
CrowdStrike	Enhanced Anti-Virus, Endpoint Intrusion Detection, Response & Reporting (EDR) (replaced BitDefender and Carbon Black)
CISCO Umbrella	Provides Web monitoring and control
NetExtender Remote Access	Upgrade to VPN (virtual private network) to better secure access with 2FA (2 factor authentication)
W10 Upgrades and Patching	Regular and reported patch cycle to mitigate vulnerabilities
Reporting	Revised Monthly Status and Vulnerability Reports

2022 - Completed Actions

IT CONTROL IMPROVEMENTS SINCE 2020 REPORTING PERIOD

Cyber Control	Security Benefit
Disaster Recovery Site	Provides off site teller location for Disaster Recovery
Local Administrative Access	Access Restricted to Reduce Attack Surface and Escalation Attacks
Software Lockdown	EDR and Umbrella establish whitelisting and browser controls
Email	Migrated to Microsoft 365 – improved Security and Data Leakage Prevention.
Website	Upgraded Security on Platform and Webform Authentication Controls

2022 - Vendor Compliance

IT CONTROL IMPROVEMENTS SINCE 2020 REPORTING PERIOD

Vendor	Compliance
Smart Solutions	SOC 2 Compliance
Hub Creative	SOC 2 Compliance for WP Engine WordFence Premium Service for Security

CIS Controls Alignment

Basic

		Controls
1	Inventory and Control of Hardware Assets	- MSP, Ninja RMM
2	Inventory and Control of Software Assets	- MSP, Ninja RMM, CrowdStrike EDR
3	Continuous Vulnerability Management	- CrowdStrike EDR & AntiVirus; Rapid7 Scans
4	Controlled Use of Administrative Privileges	- MSP monitoring - Local Controls, 2FA, RBAC
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	- MSP; Patching; EDR
6	Maintenance, Monitoring and Analysis of Audit Logs	- MSP; RMM; Firewall etc. - Universa; HubCreative

Observations

BASED ON OUR REVIEW THE FOLLOWING AREAS OF OBSERVATION PRESENT ELEVATED RISK.

Observation	Description	Risk Rating
Response and Recovery	WebFence Reporting for <1hr response service is not enabled, currently response services would need to be engaged post incident. Incident Reporting, Response and Recovery actions require integration with vendor processes to ensure coverage and reporting.	**High**
Protective Technical Controls	Protective controls such as use of MFA, Local Endpoint Encryption, Media Controls and Web Response Controls require review. (DMARC is now enabled on outgoing email.)	**Medium/High**
Detective Technical Controls	Data Leakage Protection, monitoring, alerting and auditing is applied at a basic level.	**Medium**
IT Governance and IT Security Policies.	Policies related to IT Governance, including: IT risk and response categorization; Data security, retention and destruction; vendor management; and controls audit and assurance; are not aligned.	**Medium**
Data Classification & Protection	The PII, Financial and other sensitive data are classified but locations and workflows are not catalogued, which impacts on the ability to apply technical controls and effectively protected against unauthorized disclosure. Outsourcing policies and agreements need to include security requirements.	**Medium/Low**
Vulnerability & Risk Management	A Vulnerability Management program is not established, and reporting to management is not completed on a regular basis.	**Medium/Low**

Compliance Models

IT Governance Framework (ITGF)

- Assurance that IT is providing value and is mitigating risks.
- Effective and efficient use of IT resources
- Maximizes the cost savings and the benefits of IT
- Ensures investments are consistent with business strategy.

DICO IT Governance Framework (ITGF)

Built on industry best practices:

- NIST CSF
- ISACA (COBIT)
- ISO 38500 / 27001

- Establishes 42 Controls Areas

- FSRA Has Not Reissued Framework

Other Compliance Models

BCFSA – BC Financial Services Authority

- Framework for Credit Unions
- NIST Based, 72 Questions

CIS Controls

- Technical Best Practices (not GRC focused)
- 20 Control Areas

NIST

- GRC Focus
- Privacy and Supply Chain can be included

NIST Cybersecurity Framework

THE FOLLOWING IS CONTEXTUAL INFORMATION ABOUT THE NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework (CSF) originated in 2013.

- Designed for the assessment and protection of critical government infrastructure.
- Comprehensive nature of the NIST CSF has led to the widespread adoption throughout the cybersecurity industry as best practices.
- The NIST CSF expands beyond other frameworks by being more than a simple listing of cyber controls.
- Focus on using business drivers to guide security activities and considering cyber risks as part of the organization's risk management processes.

NIST CSF takes a true risk-based approach to cybersecurity.

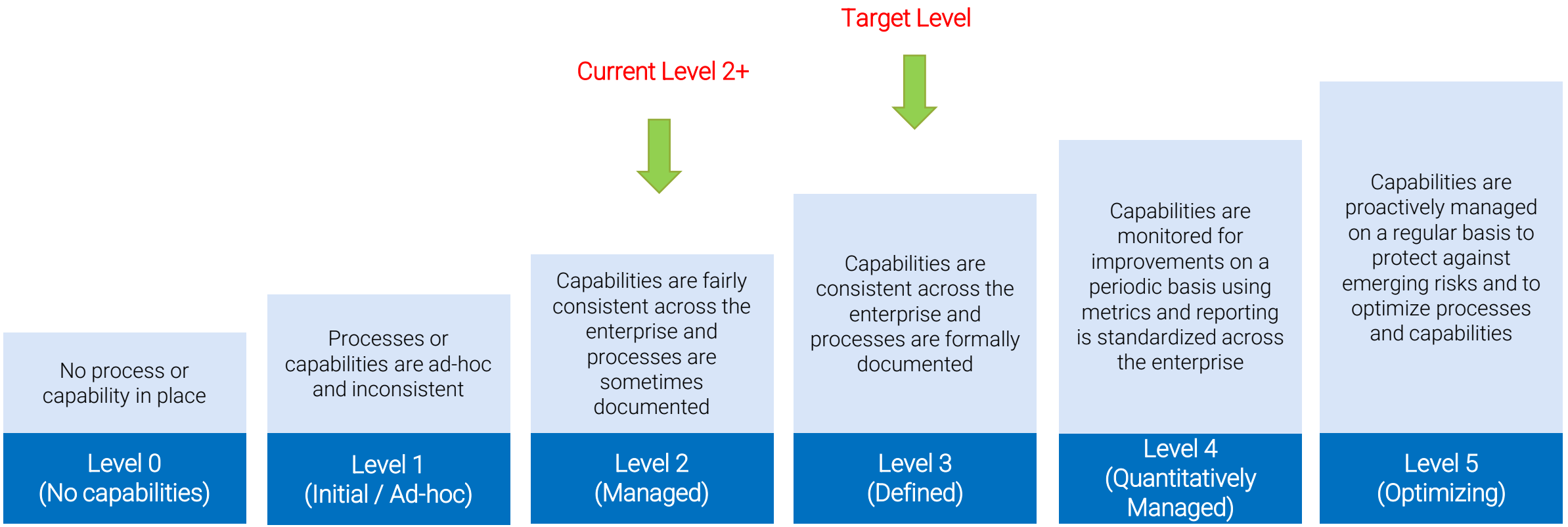
NIST CSF

THE NIST CYBERSECURITY FRAMEWORK (CSF) IS THE FOUNDATION FOR THE CYBERSECURITY CAPABILITY ASSESSMENTS.

Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets and capabilities.
Protect	Develop and implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event
Respond	Develop and implement the necessary activities to take action as a result of a detected cybersecurity event
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore capabilities after a cybersecurity event

Capability Maturity

BAKER TILLY USES A SLIGHTLY MODIFIED CMMI RATING SCALE



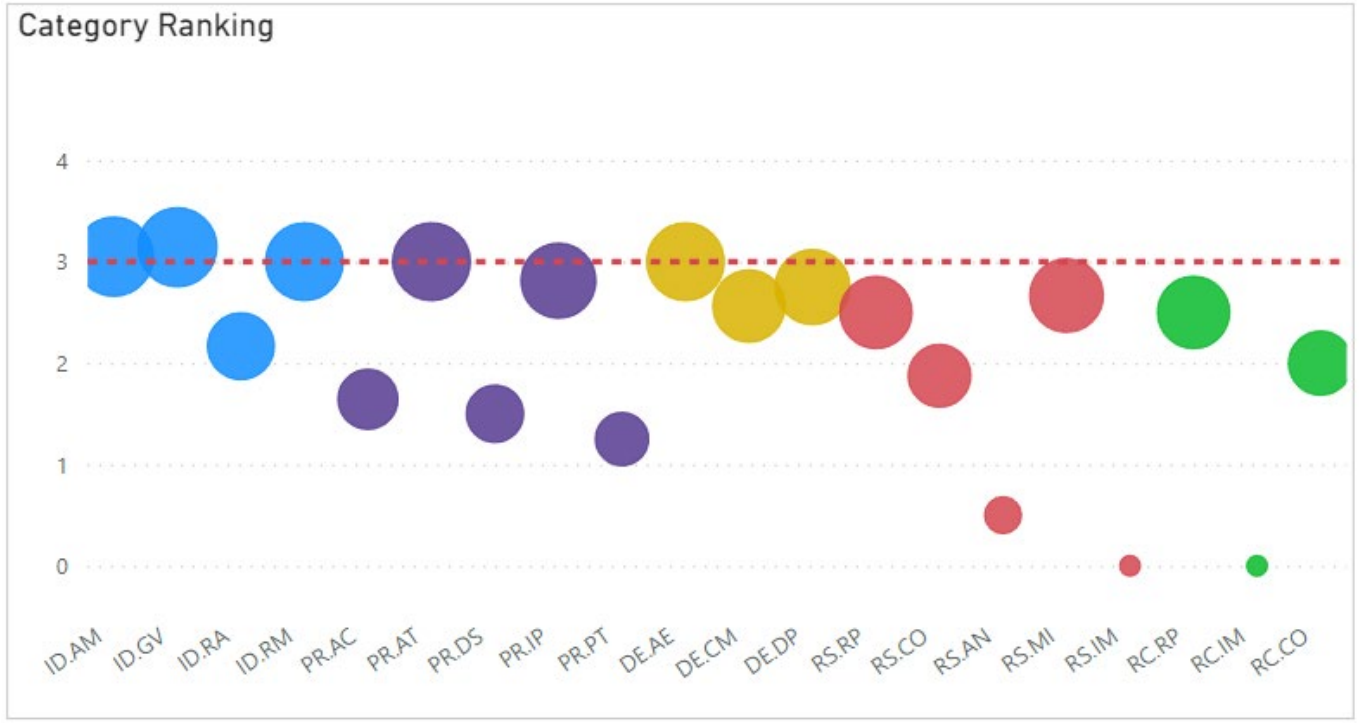
Note: For illustrative purposes only. This is a high-level executive summary based upon the general information provided by Equity and their vendors, a formal audit and review of controls was beyond scope.

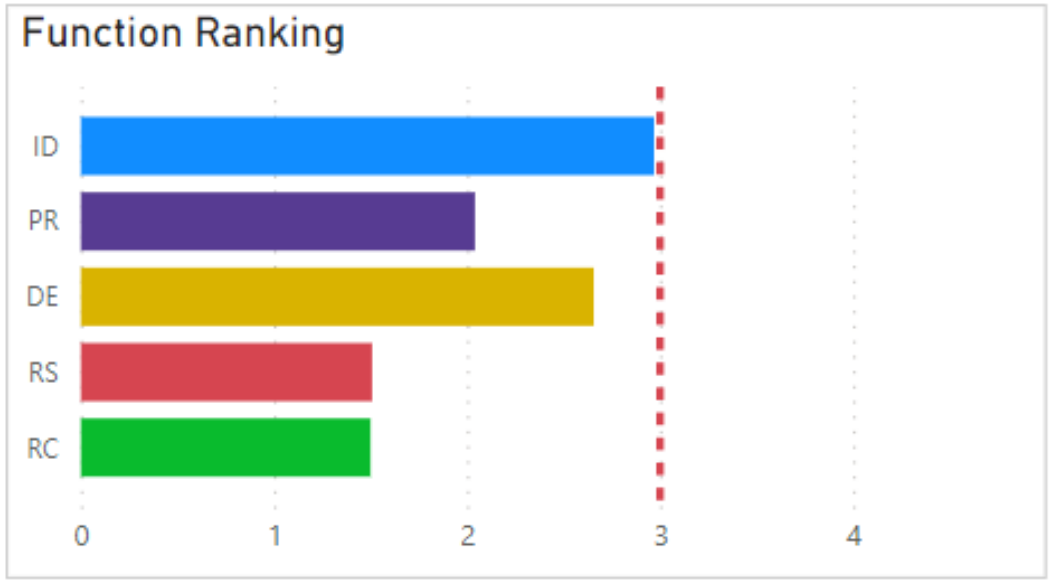
Equity CU Cybersecurity Maturity Overview

BELOW IS CLIENT'S CURRENT STATE MATURITY RATINGS

Current State Cybersecurity Maturity: 2+

CMMI Maturity Ratings		
0	No capabilities	No process or capability in place.
1	Initial/ad Hoc	Processes or capabilities are ad-hoc and inconsistent.
2	Managed	Capabilities are fairly consistent across the enterprise and processes are sometimes documented.
3	Defined	Capabilities are consistent across the enterprise and processes are formally documented.
4	Quantitatively Managed	Capabilities are monitored for improvements on a periodic basis using metrics and reporting is standardized across the enterprise.
5	Optimizing	Capabilities are proactively managed on a regular basis to protect against emerging risks and to optimize processes and capabilities.





Priority 1 and 2 Control Areas – IT and Privacy

Note: For illustrative purposes only. This high-level executive summary is based upon the general information provided by Equity and their vendors, a formal audit and review of controls was beyond scope.

Appendices to Presentation

The following Appendices support this report.

- Web Upgrade Project Executive Summary
- Web SOC Reports
- Smart Solutions SOC Reports
- Horn IT Monthly Report

Discussion