Dow CREDIT UNION

Governance and Risk Management

Stakeholder Communication Planning

Mark Gandy
VP, Chief Information Officer

Contents

The Governance Organization

The Risk Management and Governance Processes

Examples

- Monthly Board Dashboard
- Quarterly Vendor and Info Sec Risk Management Executive Summary Dashboard
- Annual InfoSec Risk Management Executive Summary Dashboard

Organizational Profile

- Single Branch*
- SEG CU 74,000ish members*
- US$2B asset size (as of 12/31/2022)
- 160 employees

My Profile

- 4 years on the management team (after 20 years on Supervisory Committee)
- 29 years in global chemical manufacturing cyber and information security
- GO GREEN!

The Organization

Board and Committees

Board

9 Directors - Global Manufacturing Executives

- 2 IT Executives
- 1 Sarbanes Oxley Compliance Executive
- 1 Corporate Audit Executive

10 Meetings/Year

Supervisory Committee

3 Members

- 1 SOx Global Executive (ret)
- 1 Investment Executive
- 1 IT Architecture Executive

Quarterly

IS Review Cmte

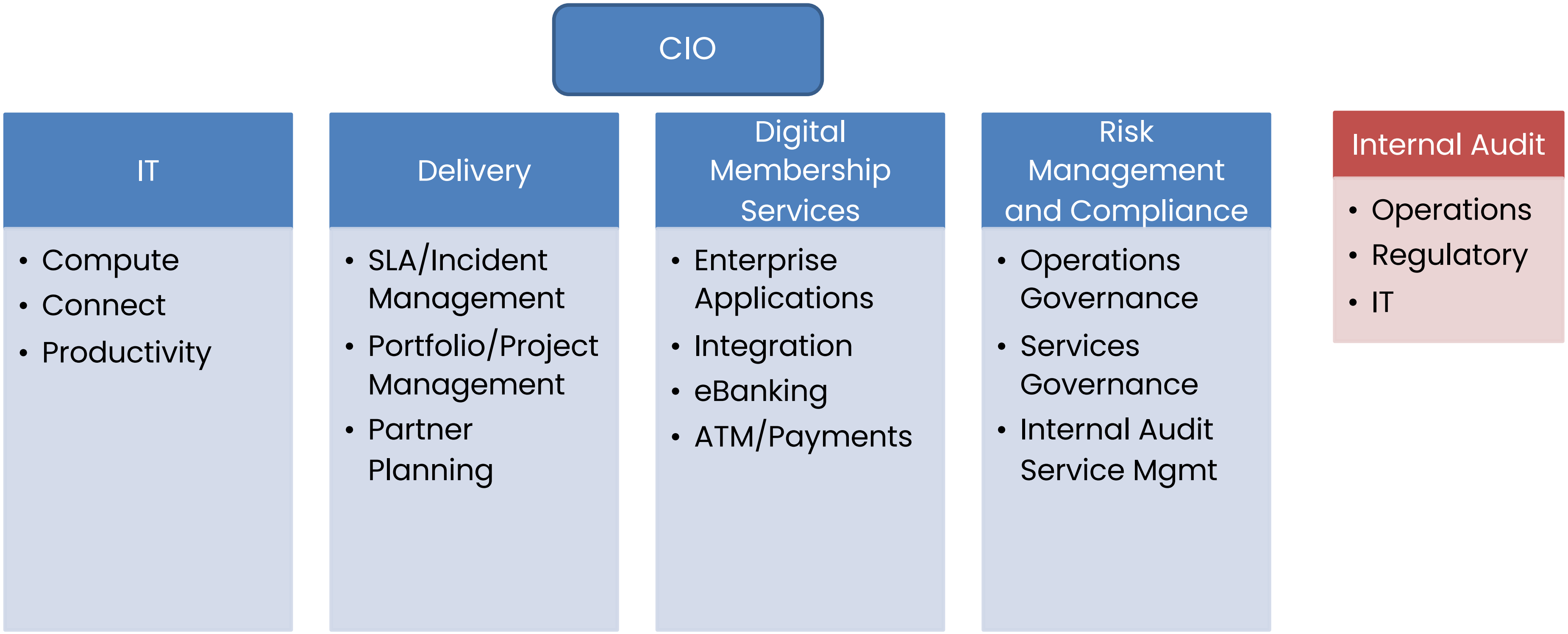
3 BoD, 1 SC Member

- 2 IT Executive
- 1 SOx Compliance Executive
- 1 IT Arch Exec from SC (*ex officio)*

April, August, November

The Organization

Management



CIO

IT

- Compute
- Connect
- Productivity

Delivery

- SLA/Incident Management
- Portfolio/Project Management
- Partner Planning

Digital Membership Services

- Enterprise Applications
- Integration
- eBanking
- ATM/Payments

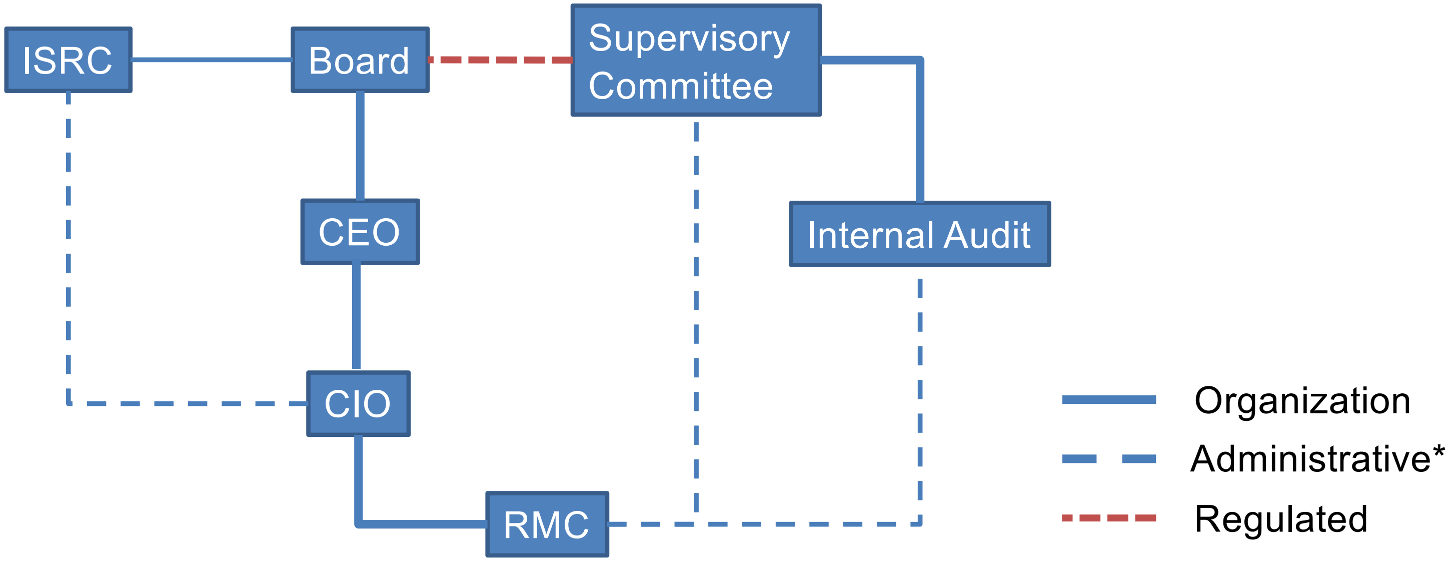
Risk Management and Compliance

- Operations Governance
- Services Governance
- Internal Audit Service Mgmt

Internal Audit

- Operations
- Regulatory
- IT

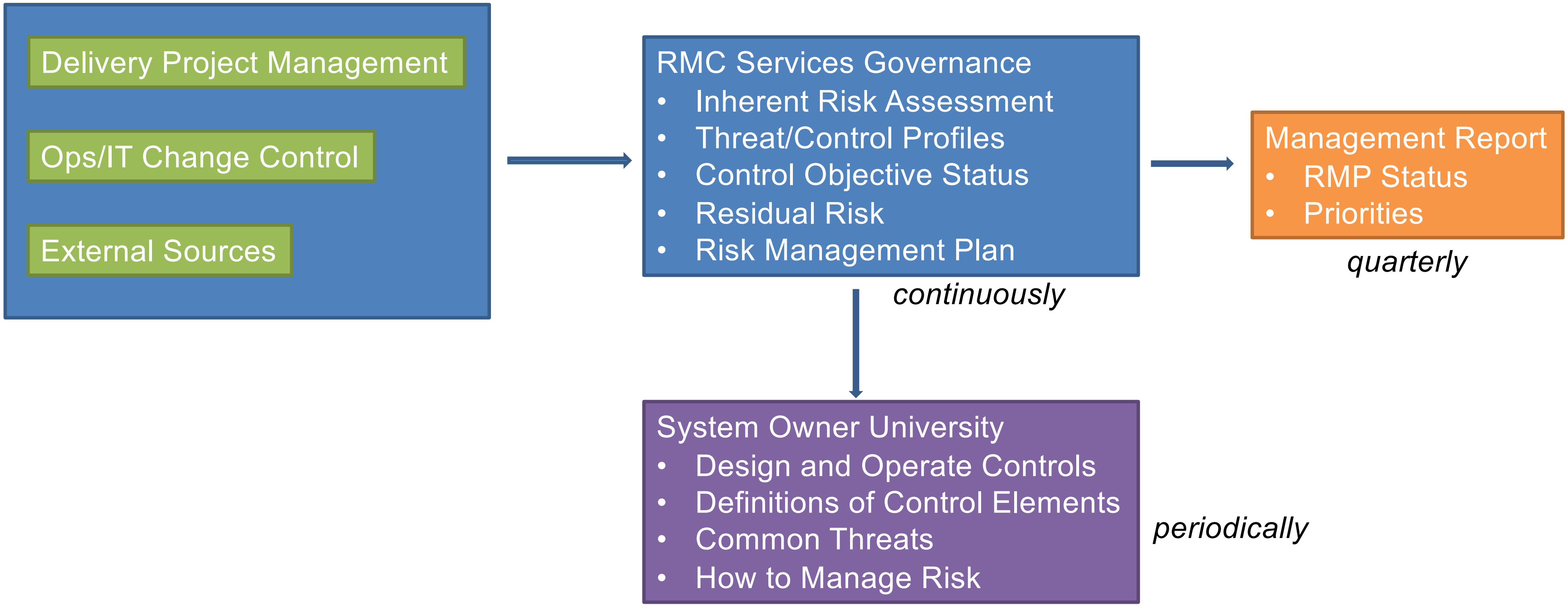
Governance Reporting Lines



**Meets directly with for independent communications*

Management Activities

Integrating Cyber/Info Sec Risk Management into the organization



Delivery Project Management

Ops/IT Change Control

External Sources

RMC Services Governance

- Inherent Risk Assessment
- Threat/Control Profiles
- Control Objective Status
- Residual Risk
- Risk Management Plan

continuously

Management Report

- RMP Status
- Priorities

quarterly

System Owner University

- Design and Operate Controls
- Definitions of Control Elements
- Common Threats
- How to Manage Risk

periodically

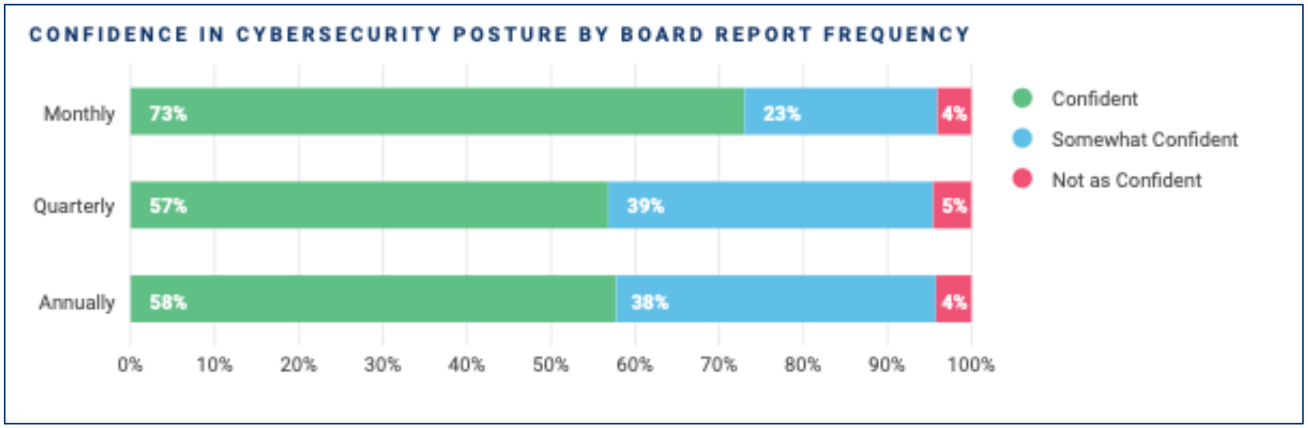
Industry Perspectives – Effective Board Governance

2022 The State of Cyber Security in the Financial Institution Industry - Tandem

THE STATE OF CYBER SECURITY IN THE FINANCIAL INSTITUTION INDUSTRY 2022 SURVEY REPORT

Tandem

Dow Credit Union's Information Security Programs (Vendor, Cyber/Info Security, Business Continuity) are continuously improving with timely and intentional stakeholder reporting to improve the confidence in the value and effectiveness of the governance activities..



Monthly:

- *Board Dashboard*

Quarterly:

- *Information Security Risk Assessment*
- *IT Internal Audits*

Annually

- Management Annual Report

Timely Communications

Reports by Management to Governance Stakeholders

Board Dashboard – Monthly

ISRC Governance Report – 3x/year

- Risk Assessments and Strategic Planning

Supervisory Committee – Quarterly

- Audit Management and Governance Topics
- Note: IA attends and receives management risk assessments for planning consideration.

Annual Report to the Board – Yearly

- Strategic, Operational, and Audit year in review and look ahead

Timely Communications

Reports by Management to Governance Stakeholders

Board Dashboard – Monthly

- Threat Environment
- Security Operations (IoC’s)
- Phishing Analysis
- Employee Phish Testing
- Vulnerability Management
- Audit/Exam Responses
- Employee (Board) Training Topics
- Notes for the Period

ISRC Governance Report – 3x/year

- Vendor Management
- Management Cyber/Info Sec Risk Assessment

Supervisory Committee – Quarterly

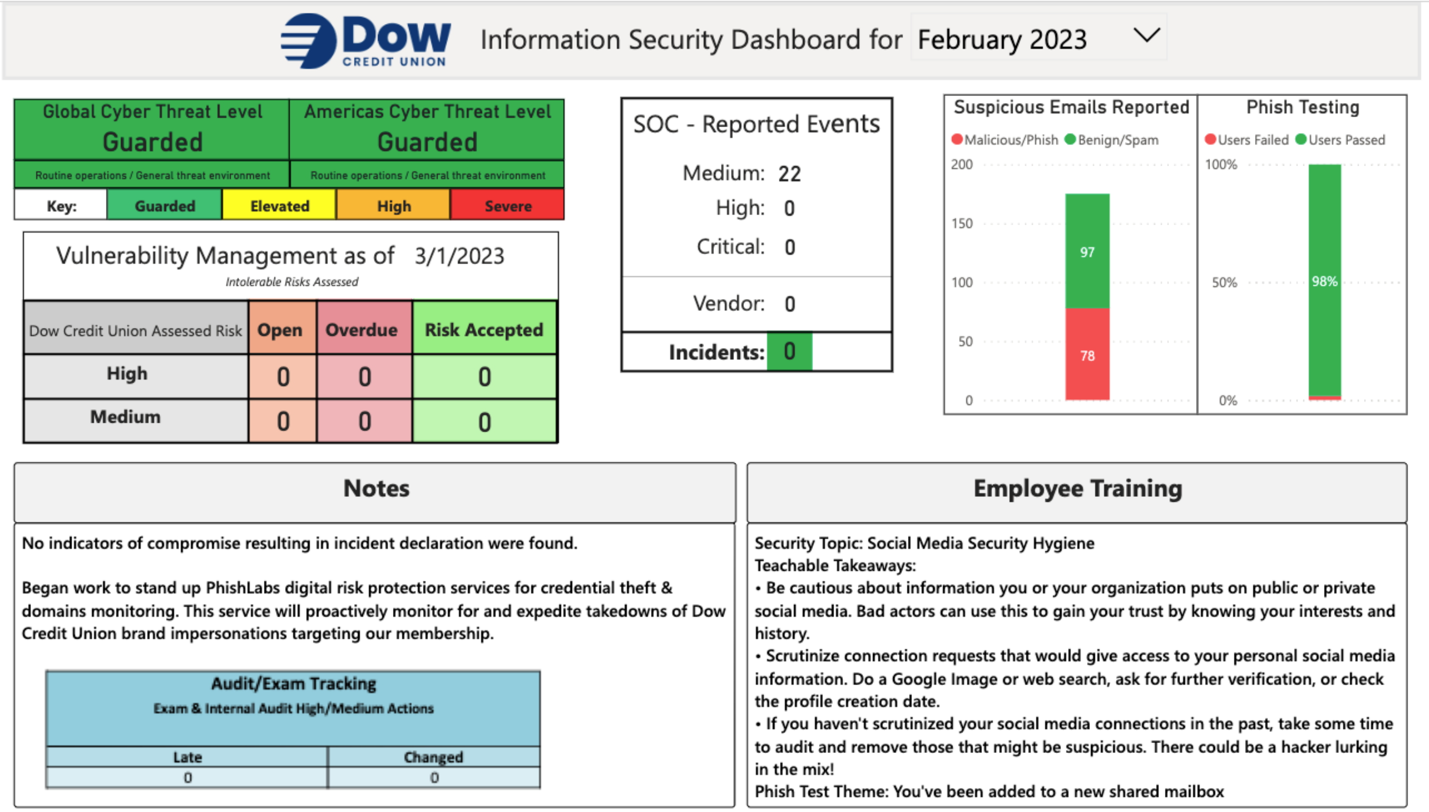
- Internal Audit Risk Assessment and Audit Planning
- Exam/Audit Reports with Management Responses
- Regulatory Updates
- Status of Planned Audits and Open Responses

- Note: IA attends and receives management risk assessments for planning consideration.

Annual Report to the Board – Yearly

- Board Responsibilities and Delegations to Management
- Threat and Governance Environment
- Management Reports (VDD, InfoSec, BCP/DR, IR)
- Audit/Exam Results
- GLBA Compliance
- ACET Risk Assessment Results
- Prior Year/Current Year Priority Updates

Monthly Board Dashboard



Information Security Dashboard for February 2023

Global Cyber Threat Level	Americas Cyber Threat Level
Guarded	Guarded
Routine operations / General threat environment	Routine operations / General threat environment

Key:	Guarded	Elevated	High	Severe

Vulnerability Management as of 3/1/2023

Intolerable Risks Assessed

Dow Credit Union Assessed Risk	Open	Overdue	Risk Accepted
High	0	0	0
Medium	0	0	0

SOC - Reported Events

Medium:	22
High:	0
Critical:	0
Vendor:	0
Incidents:	0

Suspicious Emails Reported
● Malicious/Phish ● Benign/Spam
200
150
100
50
0
97
78
Phish Testing
● Users Failed ● Users Passed
100%
50%
0%
98%

Notes

No indicators of compromise resulting in incident declaration were found.

Began work to stand up PhishLabs digital risk protection services for credential theft & domains monitoring. This service will proactively monitor for and expedite takedowns of Dow Credit Union brand impersonations targeting our membership.

Audit/Exam Tracking

Exam & Internal Audit High/Medium Actions

Late	Changed
0	0

Employee Training

Security Topic: Social Media Security Hygiene
Teachable Takeaways:

- Be cautious about information you or your organization puts on public or private social media. Bad actors can use this to gain your trust by knowing your interests and history.
- Scrutinize connection requests that would give access to your personal social media information. Do a Google Image or web search, ask for further verification, or check the profile creation date.
- If you haven't scrutinized your social media connections in the past, take some time to audit and remove those that might be suspicious. There could be a hacker lurking in the mix!

Phish Test Theme: You've been added to a new shared mailbox

Information Risk Assessment

Summary Dashboard as of 12/31/2022

Systems by CIA Composite Inherent Risk (n=257)

High	Medium	Low
31	138	88

Risk Management Plans Count by Residual Risk (IRP = High/Medium) ‡

⬇ Residual Risk	Mitigate Further	Accept
High:	0	0
Medium:	5	6

‡ All High IRP systems assessed annually. Medium IRP systems assessed on best-effort basis

Highest Inherent Risk Systems (C/I/A all rated as High)

System	Description	RA Last Approved
JHA Banno	Online banking platform	4/11/22
Co-Op Desktop Director	ATM and Debit card services	12/23/22
Encompass/Consumer Connect (FKA EllieMae)	Mortgage origination system	12/20/22
JHA Enterprise Payment Solutions (EPS)	Remote Deposit check capture & ACH loan payment system	4/11/22
FedLine Web	Fed services including cash & check processing	12/28/22
FedLine Advantage	ACH, wire, and securities transfer system	12/28/22
FICS – Financial Industry Computer Systems	Mortgage servicing system	12/21/22
JHA Image Center	item processing system	12/28/22
JHA Symitar EASE	Core processing system	6/30/22
Dell Storage	Datacenter storage system	9/30/22

Vendor Risk Management

Summary dashboard as of 12/31/2022

	Vendor Service Risk Profiles (n=399)									
Vendors (n=316)	Critical (15)			Significant (70)			Non-Essential (209)			TBD[1] (22)
Services	30			96			236			37
Residual Risk	*0*	*0*	*30*	*0*	*0*	*96*	*0*	*0*	*236*	*37*
	High	Medium	Low	High	Medium	Low/TBD	High	Medium	Low/TBD	TBD

Critical Vendors

Those vendors with service(s) that are vital to operations AND would require significant time/resources to replace.

Vendor Risk Management Plans by Residual Risk (High/Medium only)[2]		
Vendor Significance	**Mitigate Further**	**Accept**
Critical	0	0
Significant	0	0

Residual Risk: Sign-off/Reporting
Low: Gandy Review/Annual
Medium: Gandy sign-off/Quarterly
High: Goad sign-off/Monthly

(1) TBD=Non-critical vendor services migrated from previous program that are queued for updated risk assessments with best effort
(2) Information Risk Assessment RMP's are reported with the service's related systems
(3) Includes vendor services that are Pending Active status, but have been onboarded

Information Risk Assessment

Summary of Risk Management Activities for year end 2022

Management
1st/2nd Line Internal Controls

Policy 901

- Know where the inherent risks are by CIA
- Manage Cyber and Information Risks appropriately

Systems by CIA Composite Inherent Risk (n=257)		
High	**Medium**	**Low**
31	**138**	**88**

Risk Appetite

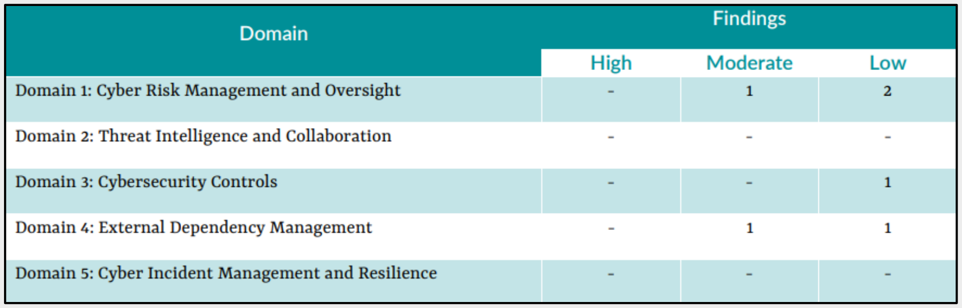
- Assess High/Medium Inherent Risk assets for expected controls (ISSP)
- Communicate management identified risks

	Mitigate Further	**Accept**
High: (CEO Owner)	**0**	**0**
Medium: (Exec Owner)	**5**	**6**

Internal Audit
3rd Line Assurance

Risk Based Internal Audit Plan

	Threat/Controls				
Inherent Risk	Identity	Configuration	Data Protection	Monitor	3rd Party
High	Annually				
Medium	Entity Annual, common control, Management discretion				
Low					



Domain	Findings		
	High	Moderate	Low
Domain 1: Cyber Risk Management and Oversight	-	1	2
Domain 2: Threat Intelligence and Collaboration	-	-	-
Domain 3: Cybersecurity Controls	-	-	1
Domain 4: External Dependency Management	-	1	1
Domain 5: Cyber Incident Management and Resilience	-	-	-

- Plante Moran – Dow Credit Union 2022 Information Security Audit

Questions?

Thank you!

Mark Gandy
mgandy@dowcreditunion.org