

DWA
Damian Walters & Associates, LLC
IT Audits, Assessments, and Test of Controls

#1 Thing …

The Board/Executives Can Do For IT
IT Can Do For The Board/Executives

Great Lakes Credit and Collection Association (GLCCA)

10th Annual Conference – CRAFTING THE FUTURE

05/07/2026

© Damian Walters & Associates

What Do We / DWA Do?

IT Audits, Assessments, and Tests of Controls (AAT)

80+ Credit Unions and Banks
3+ Collection Agencies
20+ Other regulated and non-regulated organizations
GLBA, HIPAA, PCI DSS

SOC 2 Type 1 & 2 Audits

Vulnerability Assessments and Penetration Testing

vISO Services and Consulting

© Damian Walters & Associates

Who We / DWA Are?

15+ years conducting AATs for financial organizations

500+ AATs conducted

Largest Credit Union IT AATers in Michigan …

… Soon, The World!

CUSO formed with NCA CU December 2024

Partnered with CU*Answers in August 2025

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do For IT?

i Business Impact Analyses (BIA) !

- **For *EVERY* Business Process *and* Resource**
- **Business Process / Resource Owner**
- **Criticality - Sensitivity (vs. Inherent Risk)**
- **Impact (financial, operational, reputational, regulatory/legal)**
- **Resumption Time / Point Objective (RTO / RPO)**
- **Max Allowable Downtime / Downpoint (MAD-T / MAD-P)**

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Business processes and resources?

- CRM - Retail services - payment and client portals
- ERP - Wholesale services – ARM applications / databases
- **Physical infrastructure (buildings)**
- **Staff (employees, consultants, service providers)**

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Business processes (cont)

- IT services:
  - **Authentication**
  - File
  - Database
  - **Collaboration**
  - **Network access**
  - Internet access
  - Remote access
  - **Backup and restore**

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Criticality - Sensitivity (vs. inherent risk)?

- **Criticality measures operational importance**

- **Sensitivity measures breach importance**

- Ranking =
  - Low
  - Medium
  - High
  - Extreme

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

RTO, RPO, MAD-T, MAD-P?

- Time objective = The maximum acceptable time loss.
- Point objective = The maximum acceptable transaction loss.
- Max allowable = The absolute maximum time / point before facing catastrophic consequences

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Per the FFIEC, examiners should review:

- Identification of critical business functions
- Identification of interdependencies across business units
- Identification and analysis of disruptive events
- **Reasonableness of recovery objectives**
- **Communication of BIA results throughout the entity**
- **Comprehensiveness of management's BIA review**

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Per the FFIEC, examiners should (cont)

- **Board expectations for overall business continuity capabilities**, including guidelines to achieve defined business continuity objectives

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Roles and Responsibilities?

Layer	Owns	Example
Board	**Unacceptable harm**	"Customer trust loss from prolonged outage is not tolerable"
Executives	**Risk posture translation**	"This implies same-day restoration for e-commerce"
Management / BIA	**Quantification**	"Revenue loss exceeds tolerance at 6 hours → RTO ≤ 4 hours"
Technology / Ops	**Delivery**	Architect DR to meet RTO

© Damian Walters & Associates

#1 Thing The Board/Executives Can Do (cont)

Why is the BIA so important?

- ***BIA -> Risk Assessments [see SPR below]***
- **BIA -> Data-Flow and Data-Loss Analyses**
- **BIA -> Authentication and Encryption Analyses**
- **BIA -> BC-DR and IR Testing**
- **BIA -> …**

© Damian Walters & Associates

#1 Thing IT Can Do For The Board/Executives?

i Security Program Reporting (SPR) To The Board !

Per the DIFS:

- **Information security program and status**
- **IT and infosec policies**
- **Information security risk assessment**
- **Vendor management results**
- **Security breaches or attempted breaches**

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

i Security Program Reporting (SPR) (cont)

- Business continuity plan-testing results
- Incident response plan-testing results
- **Insurance coverage for IT risks**
- **IT strategic plan (1- 3- 5-year)**
- **IT test results and remediation status**
- **Security-network performance metrics**

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

Insurance coverage for IT risks

The board should:

- Review, approve (sign), and **ensure sufficiency of insurance**

IT should:

- Review the board's review, and **ensure compliance with insurance requirements**

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

IT strategic plan = short- medium- and long-term goals

E.g.:

- **Migration of file services from on-premises servers to cloud services (Microsoft 365 Outlook, OneDrive-SharePoint, Teams)**

- **Implementation of full transmission inspection, including encrypted communications (data loss prevention)**

- **Transition from a fully outsourced IT department to a hybrid in-house and outsourced (? What is your MAD-T for IT ?)**

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

Per the FFIEC:

- Management should include the results of management assessments and reviews

- Management should include recommendations for updates to the information security program

- **Ensure the board provides a credible challenge to management by actively reviewing and questioning the information security program's effectiveness**

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

IT test results and remediation status

Of what?

i Controls !

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

Security and network performance metrics

Of what?

i Controls !

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

¿ Controls ?

The TTs and MMs employed to mitigate risks enumerated in risk assessments

© Damian Walters & Associates

#1 Thing IT Can Do (cont)

¿ Risk Assessments ?

The 1-3-5 likely and foreseeable risks that could negatively affect the CIA of

critical-sensitive business processes and resources [see BIA above]

© Damian Walters & Associates



Damian Walters, CISA

616-558-3917

dwalters@damianwaltersassociates.com

www.damianwaltersassociates.com

© Damian Walters & Associates