

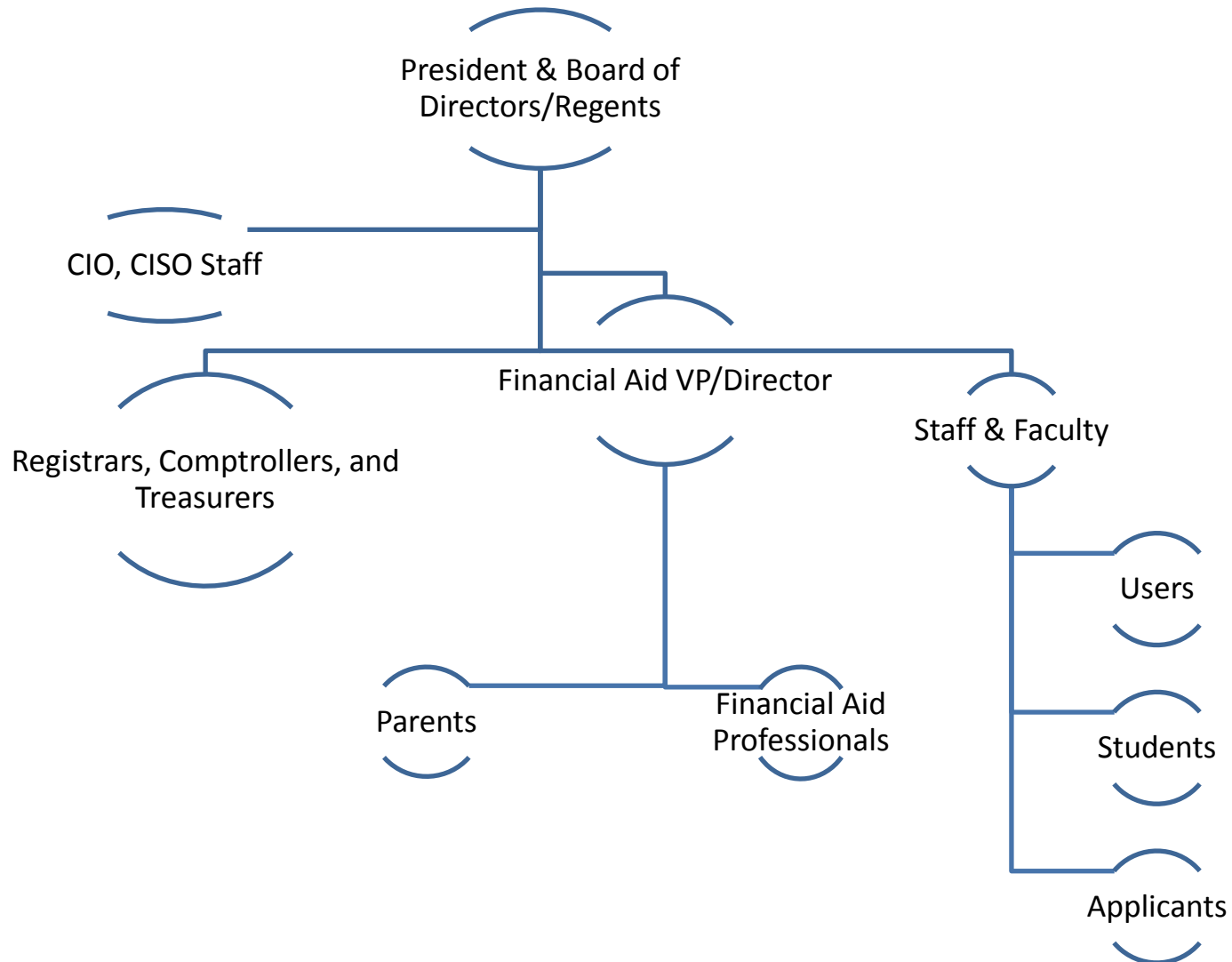
Post-Secondary Institution Data-Security Overview and Requirements

Tiina K.O. Rodrigue, EdDc, CISSP, CISM, PMP, CSM,
CEA, ITIL, ISC2 Compliance Mapper, A+
Senior Advisor – Cybersecurity - 2017

Agenda

- Who needs to worry about data security?
- Why do I need to worry about data security?
- What are the data security requirements?
- What is a breach?
- When do I report a breach?
- How do I report a breach?
- How can you help me with data security?
- What are my next steps?

Who needs to worry about data security?

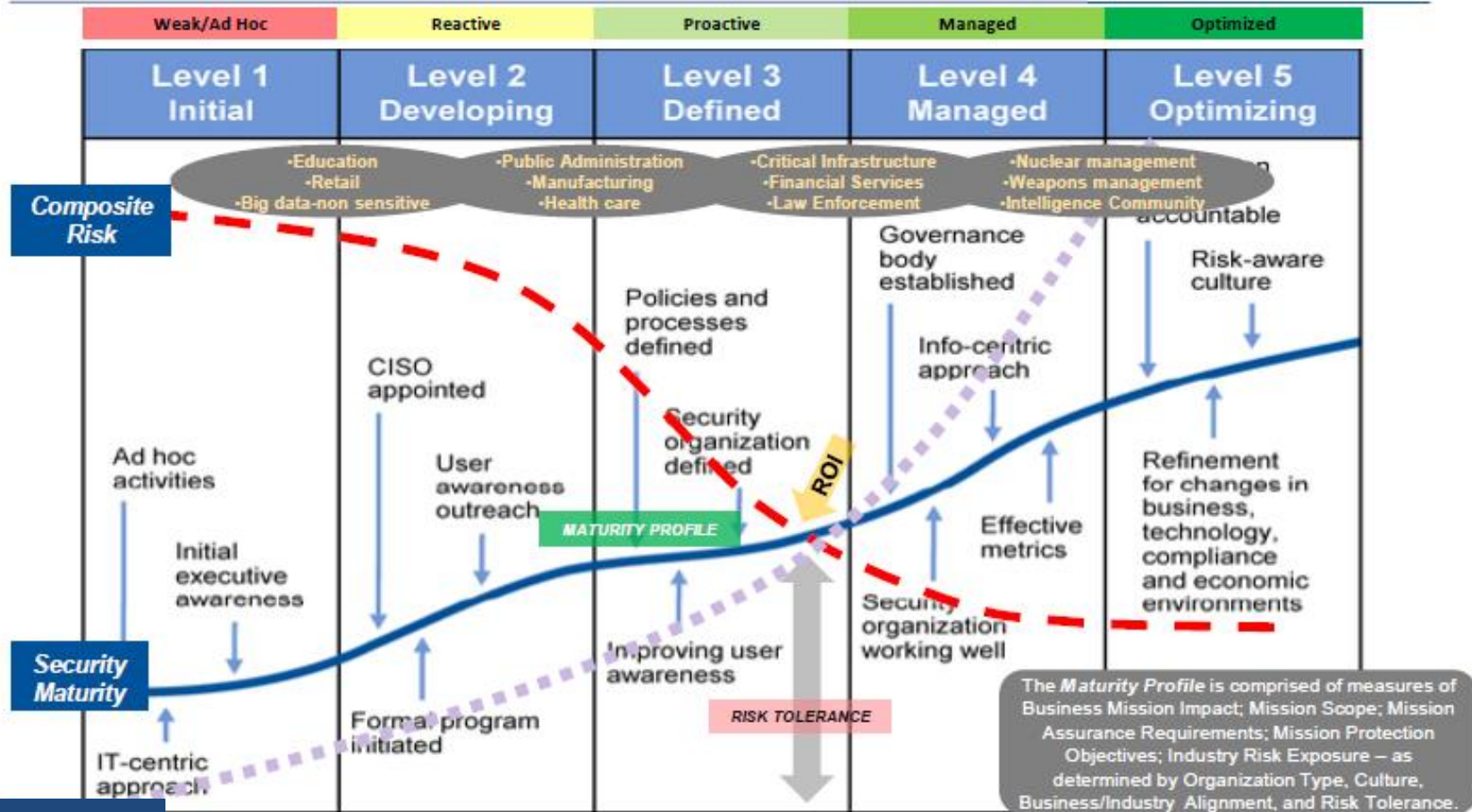


Why do I need to worry about data security?

Results Introduction

Gartner A Primer for Security Maturity

Gartner Research indicates that it typically requires 3 – 4+ years for a government organization to incrementally change maturity levels within their environments (e.g., level 2 to level 3)



Why do I need to worry about data security?

Educational institutions are specifically being targeted because of the current state of ad-hoc security coupled with the educational environment being a rich trove of emails, information and research.



Why do I need to worry about data security?

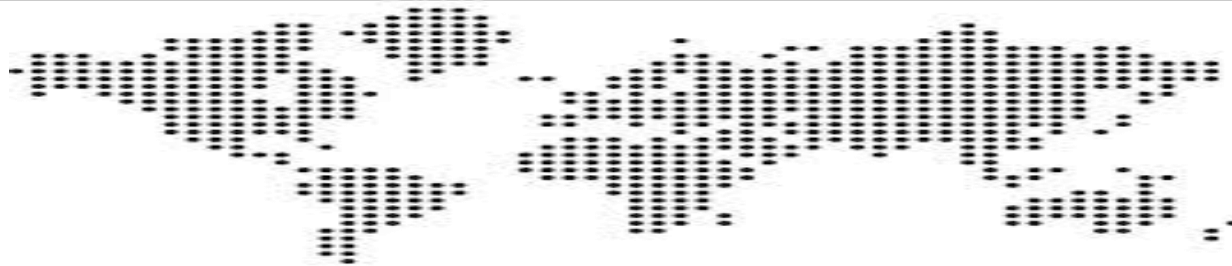
Starting in FY18, GLBA information security safeguards will be audited to ensure administrative capability. Draft audit language:

Audit Objectives – Determine whether the IHE designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.

Suggested Audit Procedures

- a. Verify that the IHE has designated an individual to coordinate the information security program.
- b. Obtain the IHE risk assessment and verify that it addresses the three required areas noted in 16 CFR 314.4 (b).
- c. Obtain the documentation created by the IHE that aligns each safeguard with each risk identified from step b above, verifying that the IHE has identified a safeguard for each risk.

What are the data security requirements?



- Title IV schools are financial institutions per Gramm-Leach-Bliley Act (GLBA, 2002)
- Per FSA PPA & SAIG agreements, these schools must have GLBA safeguards in place. Schools without GLBA safeguards may be found administratively incapable (unable to properly administer Title IV funds).
- GLBA Safeguards are:
 - Develop, implement, & maintain documented data security (info-sec) program
 - Designate an employee(s) to coordinate the program

What are the data security requirements? cont'd

- Identify reasonably foreseeable internal and external risks to data security via formal, documented risk assessments of:
 - 1) Employee training and management
 - 2) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal
 - 3) Detecting, preventing and responding to attacks, intrusions, or other systems failures
- Control the risks identified, by designing and implement information safeguards and regularly test /monitor their effectiveness.



What are the data security requirements? cont'd

- Oversee service providers, by:
 - 1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the FSA, student, & school (customer) information at issue
 - 2) Requiring your service providers by contract to implement and maintain such safeguards.
- Evaluate & adjust school's info-sec program in light of:
 - the results of the required testing /monitoring
 - any material changes to your operations or business arrangements;
 - any other circumstances that you know may have a material impact on your information security program.



What are the data security requirements? cont'd

- Title IV schools are subject to the requirements of the FTC **Identity Theft Red Flags Rule** (72 Fed. Reg. 63718) issued on November 9, 2007
- The “Red Flags Rule” requires an institution to develop and implement a written Identify Theft Prevention Program to:
 - Detect
 - Prevent
 - Respond to patterns, practices, or specific activities that may indicate *identity theft*



What is a breach?

- Per GLBA, a breach is *any unauthorized disclosure, misuse, alteration, destruction or other compromise of information.*
- Administrative, technical, and physical safeguards:
 - 1) ensure the security & confidentiality of customer information
 - 2) protect against any anticipated threats or hazards to the security or integrity of such records
 - 3) protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.



Important items to note:

- No minimum size or # of records
- Employee access is not exempt if wrong
- Not strictly digital or technology-based – **paper counts!**
- Covers data in storage, in transit or being processed

When do I report a breach?

- The Student Aid Internet Gateway (SAIG) Agreement requires that as a condition of continued participation in the federal student aid programs Title IV schools report suspected/actual data breaches
- Title IV schools must report **on the day of detection** when a data breach is even suspected
- The Department has the authority to fine institutions that do not comply with the requirement to self-report data breaches; up to **\$54,789 per violation** per 34 C.F.R. § 36.2
- The Department has reminded all institutions of this requirement through Dear Colleague Letters ([GEN 15-18](#), [GEN 16-12](#)), electronic announcements, and the annual FSA Handbook.



How do I report a data breach? (Yes, you!)

1. Email cpssaig@ed.gov & copy your data breach team, executives, per your policy

Data to include in the e-mail:

- Date of breach (suspected or known)
- Impact of breach (# of records, etc.)
- Method of breach (hack, accidental disclosure, etc.)
- Information Security Program Point of Contact
 - Email and phone details will be necessary
- Remediation Status (complete, in process – with detail)
- Next steps (as needed)

2. Call Education Security Operations Center (ED SOC) at 202-245-6550 with above data. ED-SOC operates 7x24.

3. Call or Email Tiina Rodrigue – tiina.rodrigue@ed.gov or 202-377-3887 – if both previous methods fail.



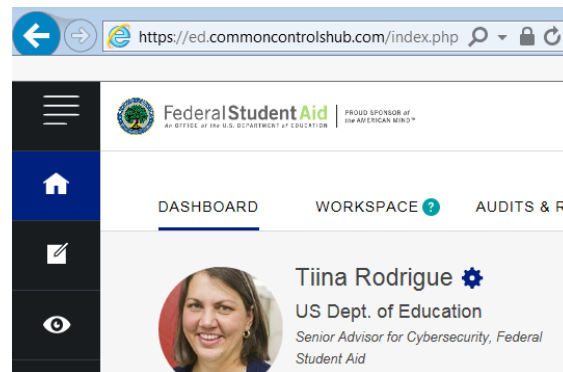
How can you help me with data security?



- [Cybersecurity Assessment Tool \(CAT\)](#) - optional self-assessment electronic tool that helps establish school's current risk profile and cybersecurity maturity for executive review & prioritization:
 - Built by [Federal Financial Institution Examiners' Council](#) (FFIEC) to help financial institutions review current state
 - Education has automated it to better enable schools of all levels to review current state of risk and maturity
 - Targets specific areas to address to close the gaps from a best practice perspective while preventing waste or over-engineering
 - Covers 5 Domains in depth, with diverse areas including culture, acquisitions, 3rd-party management which aligns with GLBA requirements
 - Pertains to policy, people and process issues, too

How can you help me with data security?

- [Institutions of Higher Education \(IHE\) Compliance Framework](https://ed.commoncontrolshub.com/index.php)
 - Public-Private Partnership to reduce the burden of compliance for security **and** privacy controls for Title IV schools
 - Register for a free account to access the optional tool & data
 - Driven by the regulation on a federal and state level
 - Includes the international regulations for foreign schools
 - Consolidates all relevant laws into one compliance framework
 - Prevents duplicate effort, saving the schools money and effort



How can you help me with data security?

NIST has provided non-FISMA guidelines ([800-171](https://www.nist.gov/800-171)) that are recommended by FSA & Education [in GEN 16-12](#) which gives specific technical standards to prove [GLBA](#) compliance:

- Access Control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment Requirements
- Security Assessment Requirements
- System and Communications Protection
- System and Information Integrity

How can you help me with data security?

As an option, you can contact Senior Advisor – Cybersecurity to:

- Ask hypothetical questions – is this an area of concern?
- Get a consultative review – policy or process (it's free!)
- Use the tools or get additional information (also free)
- Collaborate on best practices or bring ideas forward
- Review new [Cybersecurity Compliance](#) page – send input

Contact information:

- Tiina Rodrigue – tiina.rodrigue@ed.gov
- 202-377-3887

What are my next steps?

1. Find your information security policy and program for your school - If you don't have one, develop one
2. Verify your school's information security policy and program has an individual with his/her contact information - Make sure to keep that person up to date in the policy and is actively managing the program
3. Verify that your school has information risk assessment/testing schedule in place - if you don't have one, develop one
4. Verify that your school has documented the tests and results based on that schedule - if haven't tested, have team start to follow the schedule and DOCUMENT it
5. Add your information security policy/program/schedule/contact information to your consumer information and compliance website so that you can easily find/maintain it
6. Communicate to your entire executive team so that if a breach happens, everyone is prepared to respond immediately & appropriately

Post-Secondary Institution Data-Security Overview and Requirements

Tiina K.O. Rodrigue, EdDc, CISSP, CISM, PMP, CSM,
CEA, ITIL, ISC2 Compliance Mapper, A+
Senior Advisor – Cybersecurity - 2017

The [GLBA Safeguards Rule](#) defines the following:

- An **information security program** is defined as the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
- **Customer information** is defined as any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the financial institution or its affiliates.
- A **service provider** is defined as any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to the Safeguards Rule.

Federal Student Aid

An OFFICE of the U.S. DEPARTMENT of EDUCATION

PROUD SPONSOR of
the AMERICAN MIND™

Consolidated Cloud Global Footprint Map



SOURCES: MS O365 - <https://www.microsoft.com/online/legal/v2/?docid=25> | Amazon - <https://aws.amazon.com/about-aws/global-infrastructure/> | Google - <https://www.google.com/about/datacenters/inside/locations/index.html>
Salesforce - <https://help.salesforce.com/servlet/servlet.FileDownload?file=015300000038PzoAAE>, <http://www.cloudsuccess.com/blog/where-are-salesforce-com-data-centres/>, <http://www.datacenterknowledge.com/archives/2014/11/04/salesforce-com-data-center-opens-in-the-uk>
MS Azure - <http://www.itclouds.org/20141114/maps-of-data-center-localization/> | Map - http://play.ramjam.co.uk/travelsupermarket/img/TS_Map_Blue2.png | Oracle - <http://4.bp.blogspot.com/-pqFYOnLVJM8/VUQus8THB8I/AAAAAAAAIx8/IXNT4ocse>