Managing Regulatory Compliance in a Non-Compliant World

Dan Han
Virginia Commonwealth University

A little about me

- Worked in IT for close to 15 years, with 12 years focusing on Higher Education and Healthcare, and over 7 years solely focusing in security practice and management
- Like many others, took interest in information security b/c I wanted to learn how to break into things
- Took a heavy interest in cyber law and technology regulations in grad school after studying the ChoicePoint data breach
- Been serving in the current role for the past 3 years.
- Love fancy sports cars, but can't really afford one

Outline

- Define compliance
- Outline major rules and regulations that may affect organizations
- Examine some of the challenges
- Outline programmatic approach to strive for compliance in an organization
- Examples of tools and technologies that can help drive compliance efforts in an organization
- Conclusion and discussion

Disclaimer

I am not a lawyer and am not here to provide you with legal advice on data management laws and regulations. The purpose of this presentation is to introduce you to some of the regulations applicable to data management, and provide some ideas and suggestions on how to navigate the compliance landscape around these regulations from an IT management perspective.

What is Compliance?

1. The action or fact of complying with a wish or command

Or by another definition, perhaps the view of some…

2. unworthy or excessive acquiescence.

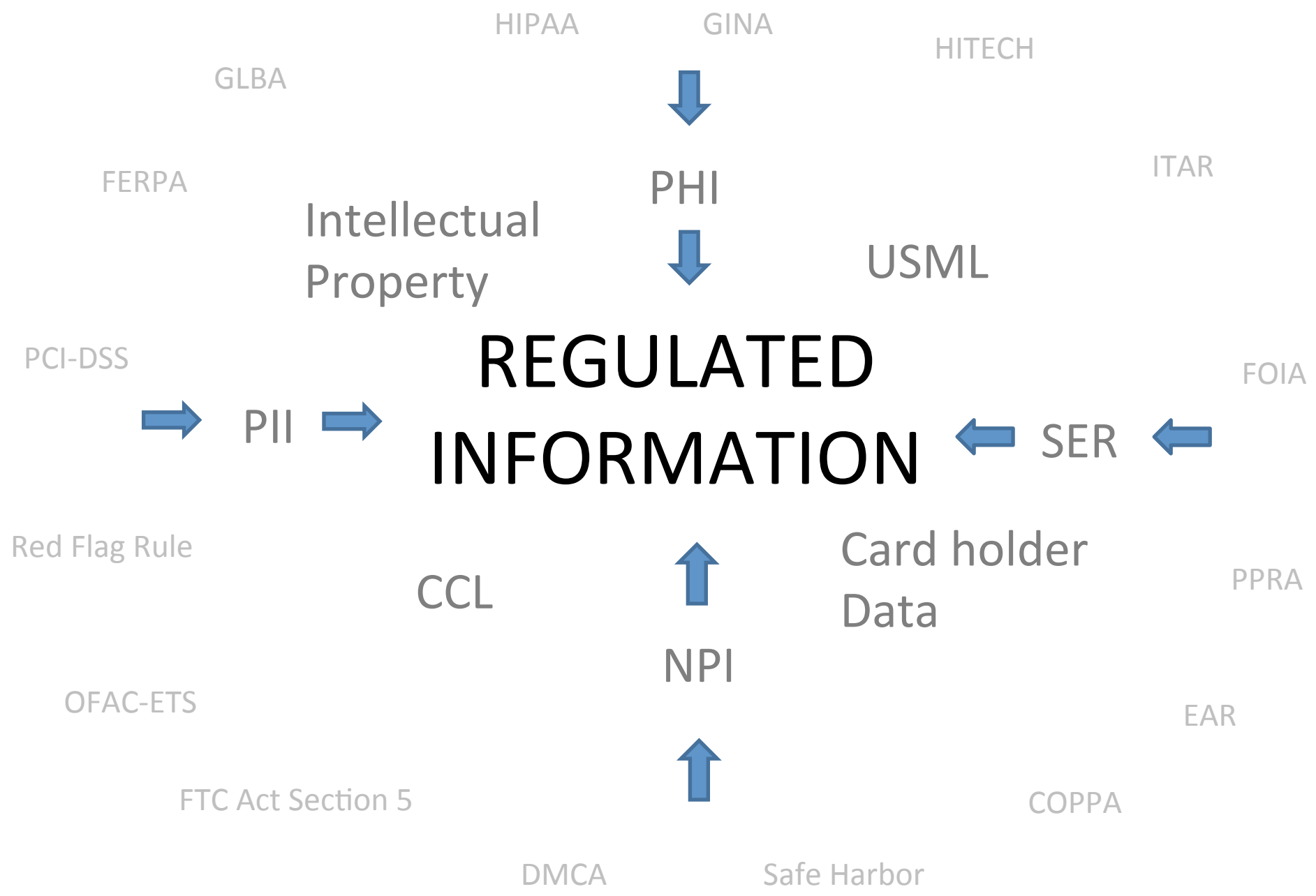
So what about regulatory compliance from the data management perspective?

My definition

The obligations of an organization toward the management of data, which:

1. Fulfills the promises it makes to its customers, and
2. Adheres to the requirements set forth by laws, regulations, and guidelines specific to the data in question

Having worked in a large University for years…


HIPAA
GINA
HITECH
GLBA
FERPA
ITAR
PHI
Intellectual Property
USML
PCI-DSS
REGULATED INFORMATION
FOIA
PII
SER
Red Flag Rule
Card holder Data
CCL
PPRA
NPI
OFAC-ETS
EAR
FTC Act Section 5
COPPA
DMCA
Safe Harbor

Among a long list…

- Code of VA (§ 2.2-3800, § 18.2-186.6, § 32.1-127.1:05)
- HIPAA / HITECH
- PCI-DSS
- FISMA
- Criminal Justice Information Services Security Policy (CJIS)
- Export Control Laws

Code of VA

- § 2.2-3800 Government Data Collection and Dissemination Practices Act
  - Information privacy practice principles and requirements
  - Addresses collection, use, disclosure, and retention of personal information
  - Addresses the rights of individuals providing information to agency
  - Addresses management requirements of systems containing personal information
- Affects almost all state agencies collecting personal information

Code of VA

- § 18.2-186.6, § 32.1-127.1:05
  - Provides notification requirements to State residents for the breach of their PII
    - Based off of the CA SB 1386, 47 States and 4 U.S. Territories have laws applicable to "residents"
    - PII usually include First Name or First initial and Last Name plus SSN, State ID / Driver's License Numbers, Card numbers and other financial information
    - Can also include health care information
- Affect all organizations with data stewardship responsibilities for VA resident data

HIPAA / HITECH

- Health Information Portability and Accountability Act (HIPAA)
  - Title II: regulates the privacy, security, use, and distribution of Protected Health Information
    - Protected Health Information
      - Health Information with 18 HIPAA identifiers from or to a "Covered Entity"
      - Limited Dataset vs. de-identified data
    - Covered Entity
      - Healthcare provider, insurance provider, or clearing house
    - Two sets of rules under Title II
      - Privacy rule: Use and distribution of PHI
      - Security rule: Defines **Required and Addressable security safeguards**

HIPAA / HITECH

- Requirements
  - Must safeguard PHI from unauthorized access, modification, or deletion
  - Required and addressable safeguards
    - Administrative
      - Security policy, training, Business Associates Agreements
    - Physical
      - Secure facility, monitored physical access control PHI
    - Technical
      - Encrypted transmission, partner authentication, data integrity
  - Cannot sell, use, or share PHI without appropriate consent or approval

HIPAA / HITECH

- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Part of ARRA in 2009
  - Final Omnibus rule released early 2013, with compliance date of September, 2013
  - Strengthens HIPAA with stringent Enforcement rule
  - Requires modified and more stringent privacy policies by Covered Entities
  - Places more requirements on "Business Associates"
  - New Breach notification rule that eliminates the "No harm, no foul" loop hole
  - Places personal accountability on individuals in addition to organizations
  - The 500 records / "wall of shame" rule http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

Breach Portal

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	McDermott Will & Emery LLP is the plan sponsor for the McDermott medical plan	IL	Health Plan	880	03/24/2015	Hacking/IT Incident	Network Server
	Freelancers Insurance Company	NY	Health Plan	43068	03/24/2015	Hacking/IT Incident	Network Server
	AT&T Group Health Plan	TX	Health Plan	50000	03/23/2015	Hacking/IT Incident	Network Server
	Life Care Center of Attleboro	MA	Healthcare Provider	2473	03/20/2015	Loss	Paper/Films
	Mount Sinai Medical Center	FL	Healthcare Provider	1406	03/20/2015	Unauthorized Access/Disclosure	Paper/Films
	Florida Hospital	FL	Healthcare Provider	8700	03/20/2015	Unauthorized Access/Disclosure	Other
	Kane Hall Barry Neurology	TX	Healthcare Provider	600	03/19/2015	Theft	Laptop
	Career Education Corporation	IL	Health Plan	2743	03/19/2015	Hacking/IT Incident	Network Server

HIPAA / HITECH

- How do I know if I am covered?
  - If you collect health information on behalf of a covered entity
  - If you collect health information from a covered entity
  - If you collect health information on behalf of the covered unit of a hybrid entity
  - The conundrum of a hybrid entity
- Even when HIPAA is not applicable…
  - Code of VA (§ 32.1-127.1:05) will cover health information
- May be applicable to any health information associated with "identifiers"

PCI-DSS

- Payment Card Industry Data Security Standard
  - Protect the confidentiality of Card Holder Data **stored**, **transmitted**, and **processed** by entities involved in payment card processing
    - Prescriptive set of 12 security control groups
    - Recommends network segmentation and scoping
    - Includes minimum standards on administrative, physical, and technical controls, including testing and audits
    - Consist of 4 levels with varying auditing and compliance requirements
    - External and internal assessment may be needed depending on qualifying level
  - Enforced by PCI Counsel and banks
  - Affects physical and web store fronts and any other areas that may intake / process credit cards

PCI-DSS 3.0

- PCI-DSS 3.0 is in effect since 1/1/2014, designed to focus on several new areas:
  - Education and Awareness
  - Passwords and Authentication Methods
  - Third party business partners / Shared hosting
  - Emerging technologies such as e-commerce, mobile processing, and cloud processing
  - Consistent and verifiable security management with heavy focus on documentation

PCI: EMV support

- Support of EMV enabled cards and Liability Shift
  - Curb usage of fraudulent cards, authenticate card against issuer
  - October 1, 2015 deadline before liability shift
  - Merchants without EMV supported terminals will bear full liability of counterfeit and fraudulent charges in U.S.

FISMA

- Federal Information Security Management Act (FISMA)
  - Both a regulation and a framework
  - Follows NIST SP 800-53 security requirements, FIPS 199, FIPS 200, and other NIST SPs.
  - Standard practice for federal government agencies
  - FISMA applies to federal government owned data
  - Uses the Risk Management Framework (RMF)
  - Has a set of baseline controls and tailored controls
  - In some cases requires FISMA certified data processing and storage facilities depending on risk level
- May apply to federally funded projects, and may appear in the form of data management plans.

FISMA

- Components:
  - FIPS 199
    - Requires the categorization of information and systems
    - Three tiers (Low, Moderate, High)
  - FIPS 200
    - Delineates baseline controls (17 categories)
    - Refers to NIST 800-53
  - NIST SP 800-53
    - The System Security Controls catalog
    - Can be extremely prescriptive
    - Select appropriate controls for system based on sensitivity and system type
  - Other NIST SP
    - May apply to specific systems / tasks (such as monitoring / security lifecycle / applications, etc.)

FISMA

- Process of the NIST Risk Management Framework (RMF)
  - Planning
  - Categorization
  - Selection of baseline
  - Threat & risk management
  - Design & implementation
  - Assessment / accreditation (authorization)
  - continuous monitoring

FedRAMP

- Federal Risk and Authorization Management Program
  - Not necessarily a regulation
  - Program used to manage and streamline the approval of cloud services for federal agencies
  - Includes assessment and accreditation
  - Based on FISMA and NIST SP 800-53 with a set of additional controls
- May provide direction on how federal data can be handled in cloud environment.

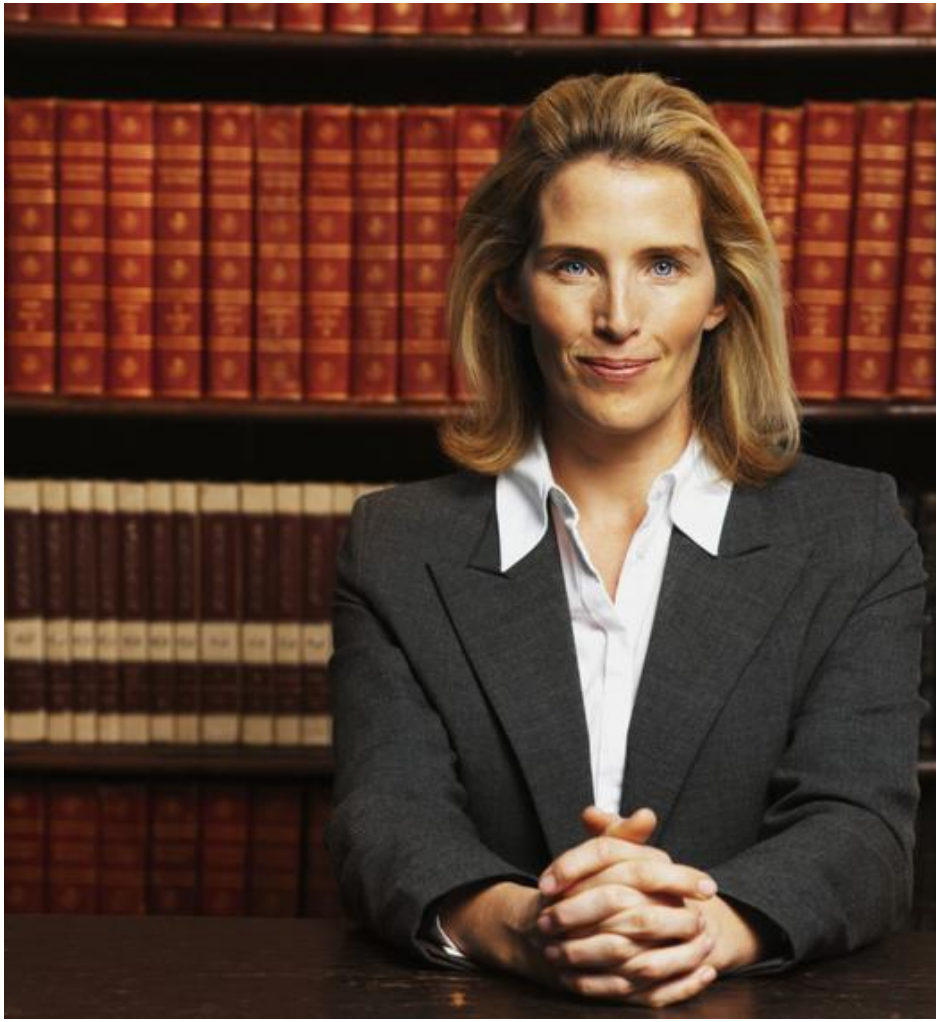
Others that may affect you…

- CJIS Security Policy
  - A set of prescriptive security controls used for the management of criminal justice information
  - Applicable to organizations receiving such information from the FBI - CJIS
- Export Control Laws
  - Used to manage the export / access of material or information regulated by various federal agencies
  - Apply to munitions or items / technology / information that can be used for military purposes
  - Must be accessed by U.S. Person and shipping abroad requires a license from regulating agency

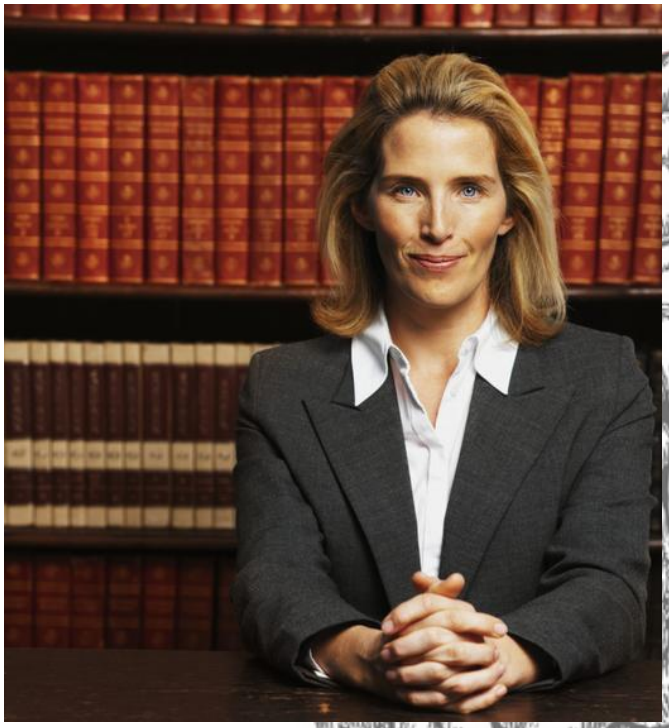
Others?

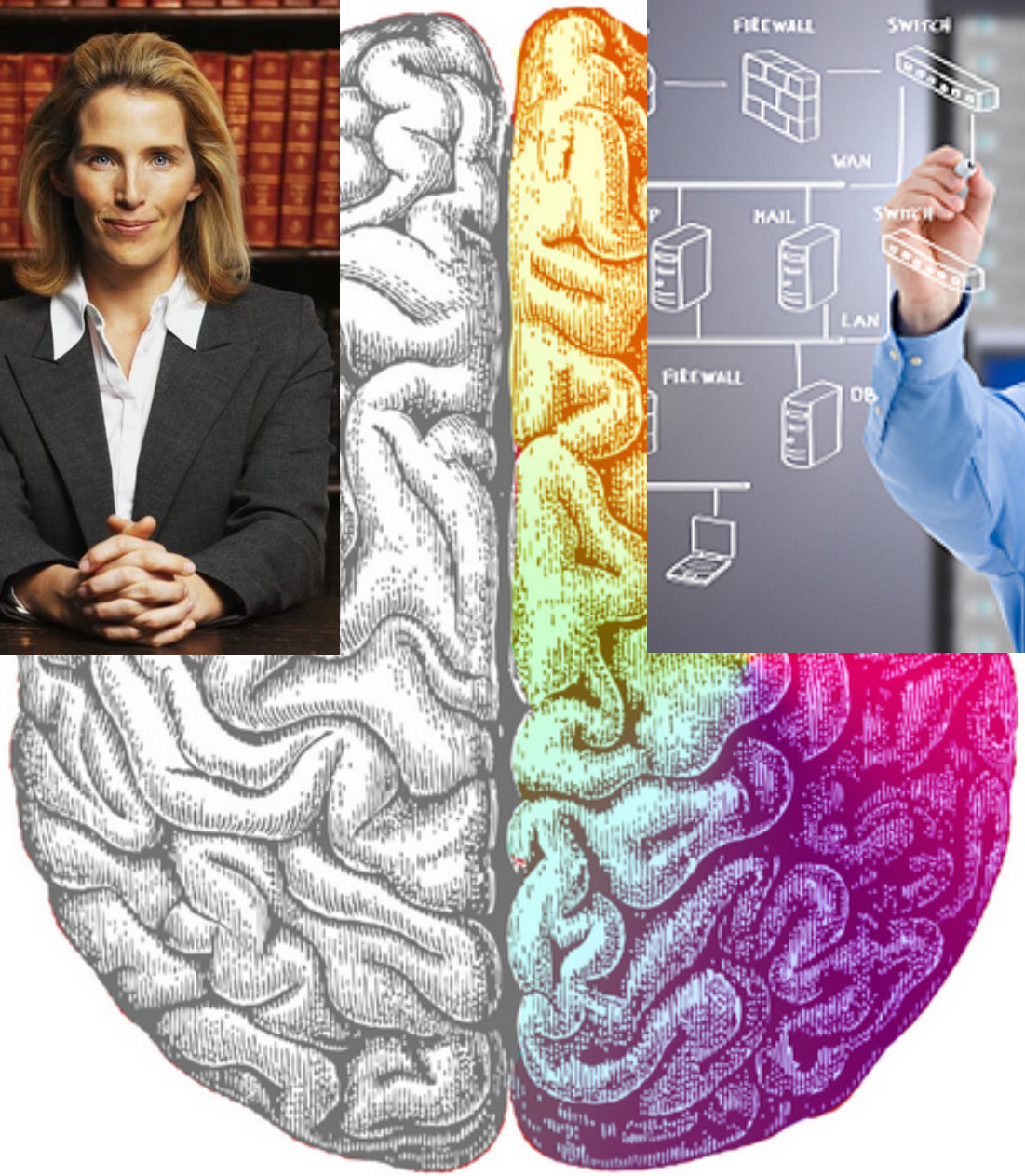
So with all these regulations how do we ensure that we are compliant?

Maybe have a conversation with your legal counsel?



However…





FIREWALL
SWITCH
WAN
MAIL
SWITCH
LAN
FIREWALL
DB

Even more so…

Therefore…

There is an inherent challenge for managing the expectations of our customers while striving to meet the compliance needs from a legal and regulatory perspective

As IT and security professionals…

We are no longer the sole provider to IT services in our organizations

Rather, we are competing with

Google
SkyDrive
join me
eCommerce
accounting
mobility
ERP
CLOUD
COMPUTING
marketing
collaboration
social media
productivity
CRM
amazon
web services™
Dropbox

Deliver the highest value to our customers & constituents at the lowest cost

So my theory / analogy is that

Where the consumer technology is speeding away in the left lane

And the regulations are dragging along the right lane

Organizations are and probably will always be… cruising the middle lane

If we go too fast…

Contrarily, if we go too slow

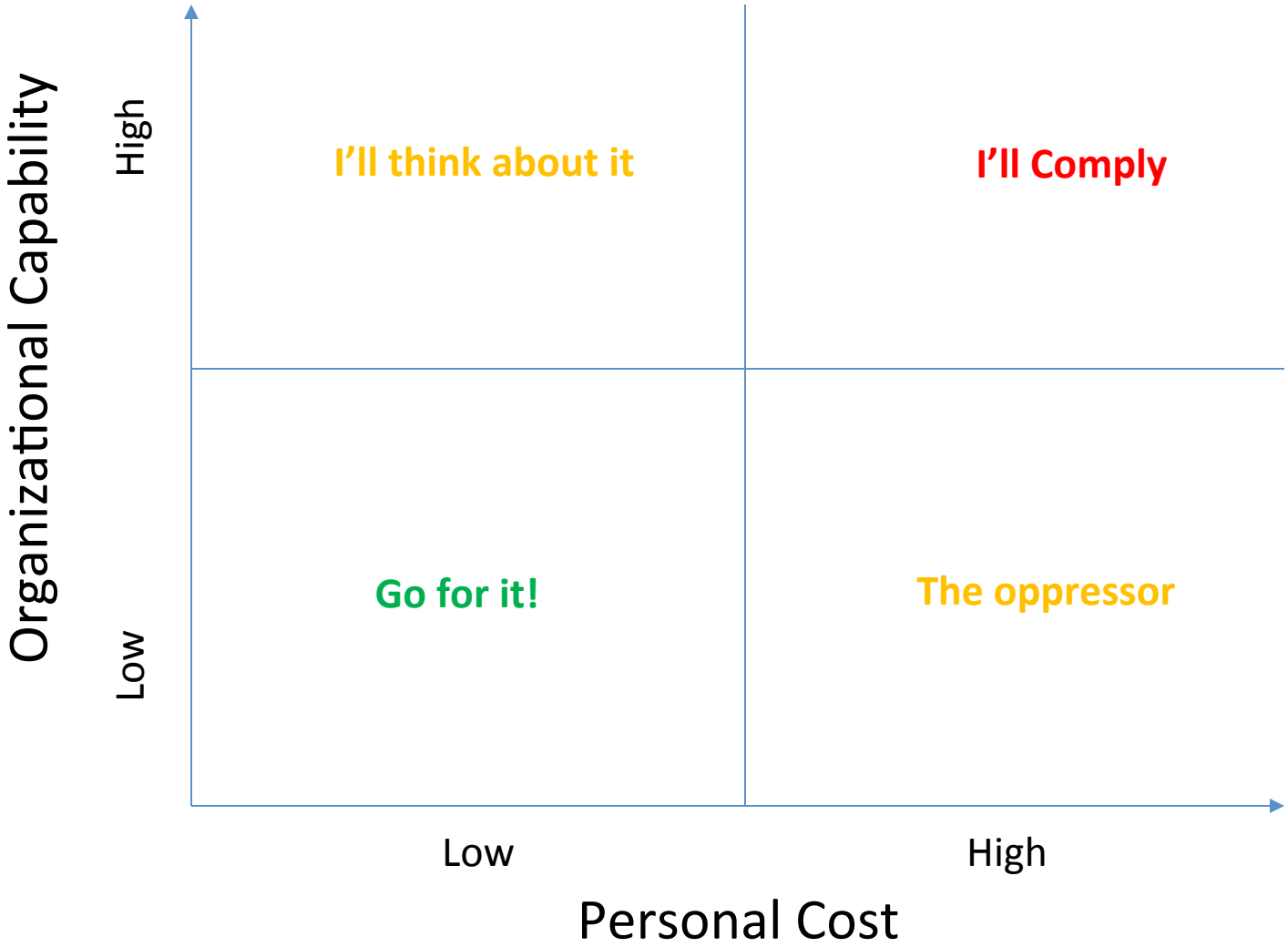
If we go too slow

The goal…

- Adjust our position in the middle lane so we won't:
  - Lose sight and lose competitiveness.
  - Get pulled over by the long arms of the law or crash and burn.

As an optimist, I like to believe

- Most of our constituents want to do the right thing
- The “pain” compliant technologies bring into question is factored into the cost for our constituents
- Our constituents will explore competitors’ offerings when our compliant solution provided do not meet their expectations
- Many times, our constituents’ expectations are set by their personal experiences from others or consumer technology
- The cost induced by the regulatory pains are then factored into the <u>personal</u> risk of non-compliance.
- Based on their knowledge and understanding of applicable regulations and risk tolerence, a decision is then made by our constituents on how the data in their possession is handled


Organizational Capability
High
Low
I'll think about it
I'll Comply
Go for it!
The oppressor
Low
High
Personal Cost

Objectives

- From the compliance perspective
  - Understand the applicable regulations
    - Compliance managers
    - Administration / data stewards
    - Data custodians
  - Bridge regulatory requirements and technical capabilities to
    - Meet our regulatory obligations
    - Deliver value to our constituents
    - Effectively compete with other solution providers
  - Assess our capabilities and identify regulatory gaps
    - Establish and follow through with sanction processes and procedures for non-compliance

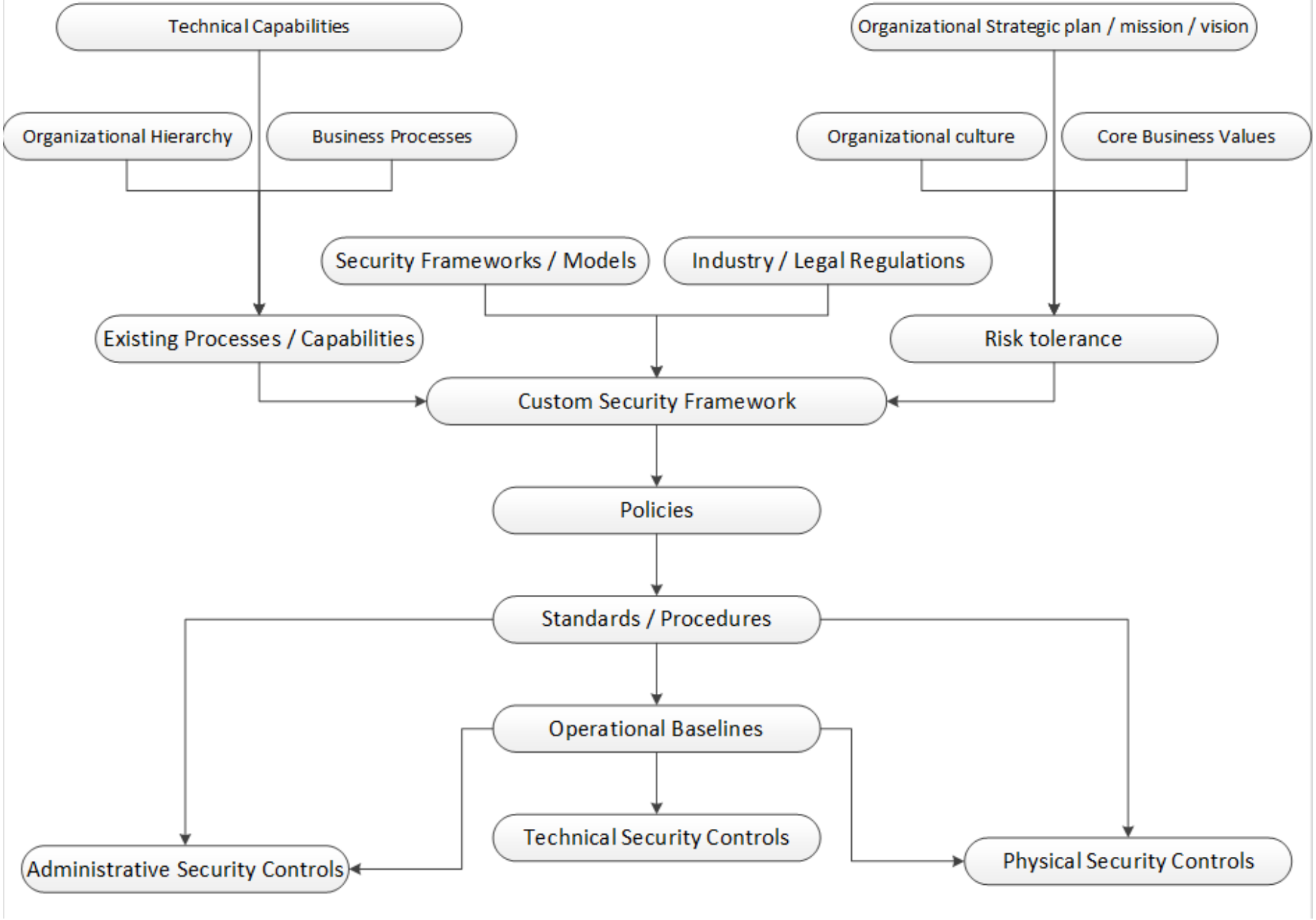
Objectives

- From the constituents perspective
  - Provide constituents with <u>relevant, concise and easy to understand</u> information on
    - Applicable regulations
    - How to comply
  - Build compliance into processes and culture
  - Evaluate and provide data handling methods and processes that are both complaint and offers comparable experiences as the competitors

Over the past year and half

- Formalize a security management architecture
- Construction of customized controls framework for consistent security / compliance management
- Construction and distribution of a data classification tool
- Develop a method to relay relevant information to our constituents

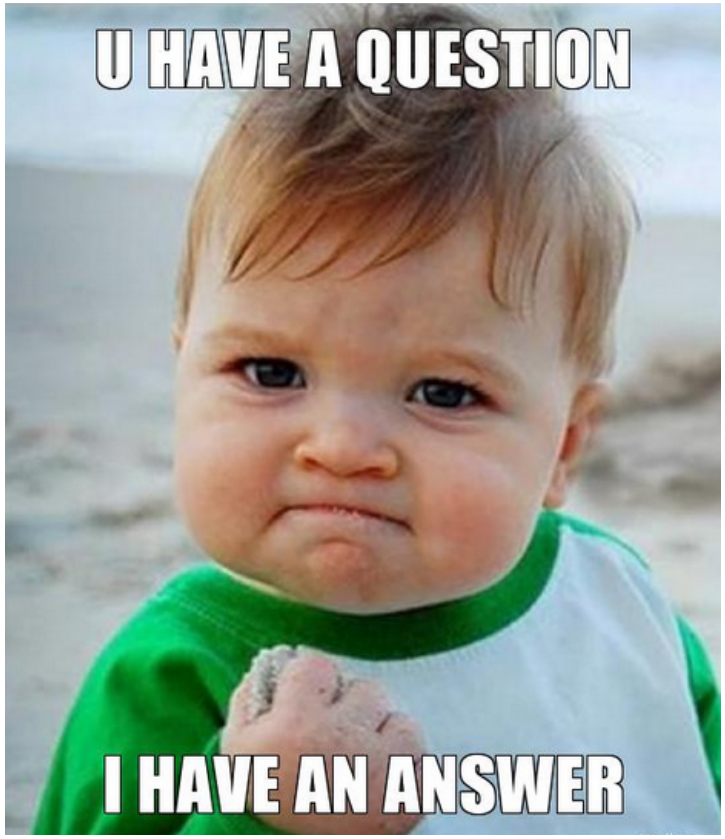
Security Management Architecture



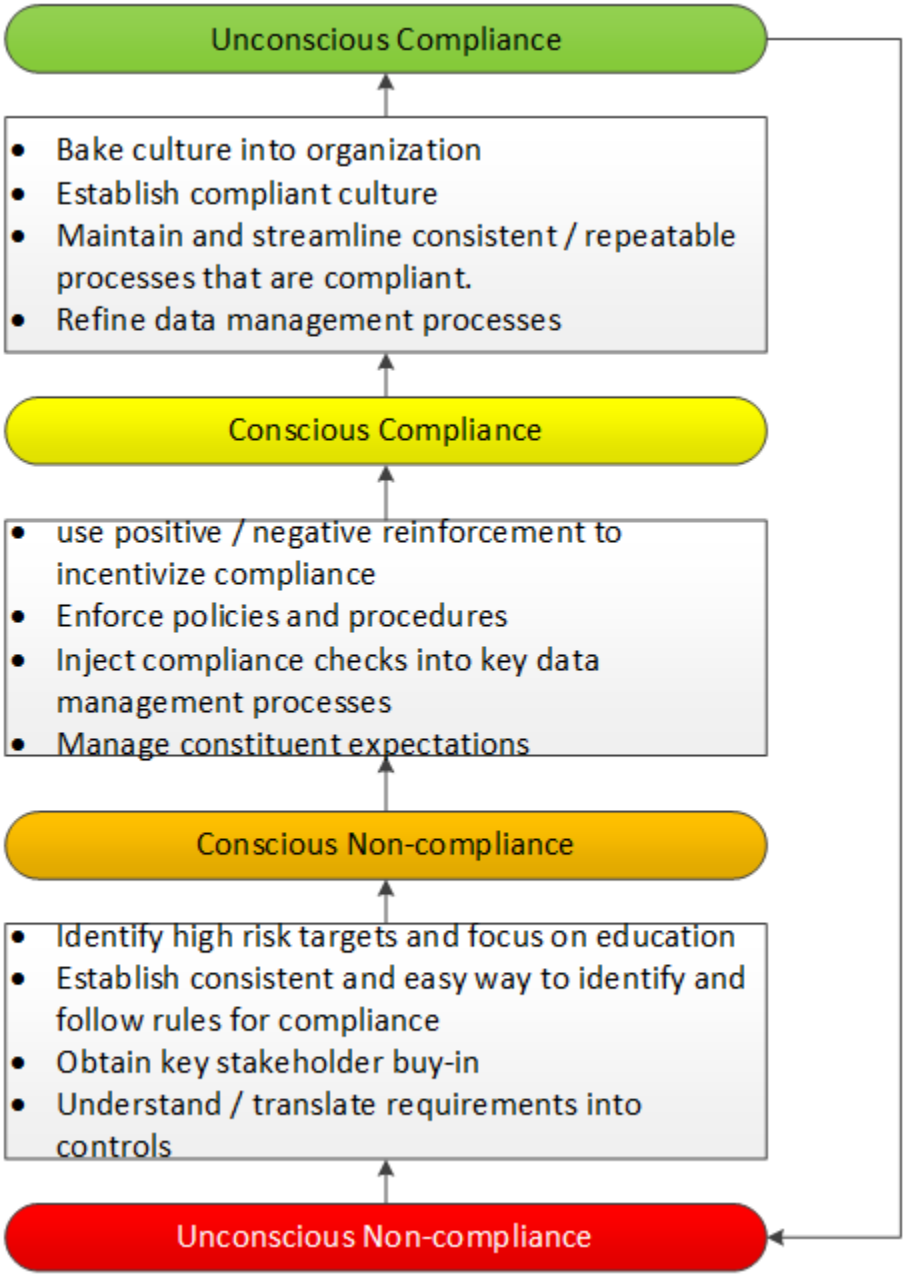
With this in mind, the next question is…

How can we translate this architecture into something that is relevant and understandable to our constituents?

From a conversation with a colleague a couple of years ago…



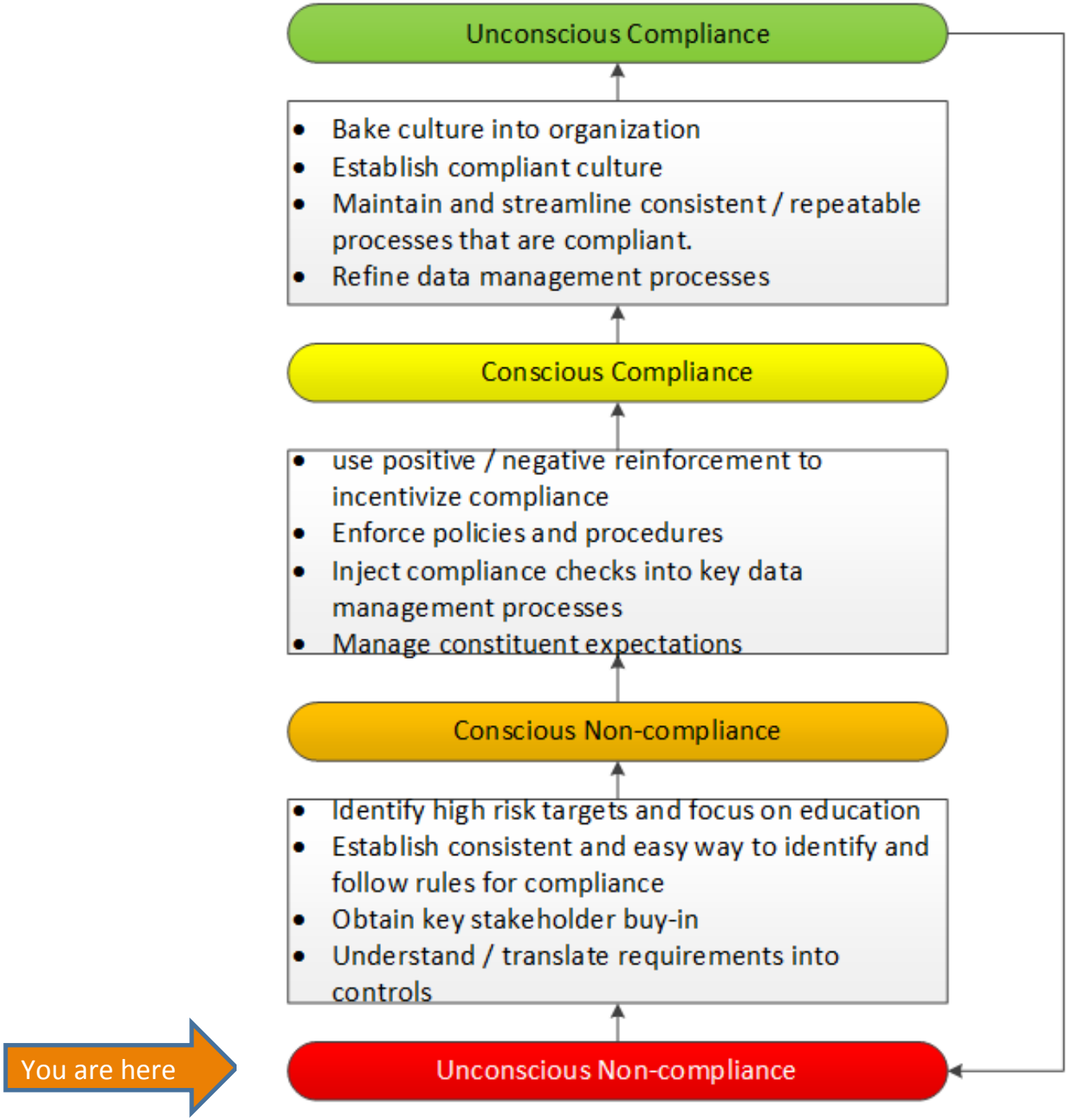
Roadmap to Compliance / Awareness Maturity



Where were we?

- Findings from data governance group*:
  - Varying degrees of understanding
    - Some stewards and even line managers understood the responsibilities and requirements around the handling of the respective data
    - Some didn't know they are data stewards
  - Inconsistent process in the authorization and handling of data, no centralized effort to drive data management compliance
  - Compliance related knowledge from data stewards did not typically permeate past line managers
  - Typically good understanding on privacy regulations, but lacking technical knowledge and translation for more technical and security related regulations

* Information based on observed conversations with identified data stewards, selected business area managers, and appointed staff members.


Unconscious Compliance
Bake culture into organization
Establish compliant culture
Maintain and streamline consistent / repeatable processes that are compliant.
Refine data management processes
Conscious Compliance
use positive / negative reinforcement to incentivize compliance
Enforce policies and procedures
Inject compliance checks into key data management processes
Manage constituent expectations
Conscious Non-compliance
Identify high risk targets and focus on education
Establish consistent and easy way to identify and follow rules for compliance
Obtain key stakeholder buy-in
Understand / translate requirements into controls
Unconscious Non-compliance
You are here

Step one

- Assuming we are starting from unconscious non-compliance:
  - Educate ourselves first (Formulate the framework)
    - Examined existing data classification standards
    - Re-mapped the data classification back to applicable regulations
    - Examined all identified regulations, frameworks & best practices
    - Documented common requirements and variances
    - Examined currently available technology and implementation at VCU

Referenced Regulations / Frameworks

Children's Online Privacy Protection Act (COPPA) -- TITLE XIII
Cloud Security Alliance Cloud Controls Matrix (CCM) v3.0
Code of Virginia §2.2.3800
Code of Virginia §18.2-186.6
Code of Virginia §32.1-127.1
Digital Millennium Copyright Act (DMCA)
Database of Genotypes and Phenotypes (dbGaP) Security Best Practices
Gramm-Leach Bliley Act (GLBA) Safeguards rule
Gramm-Leach Bliley Act (GLBA) Privacy rule
Genetic Information Nondiscrimination Act of 2008 (GINA)
Family Education Rights and Privacy Act (FERPA)
FBI Criminal Justice Information Services (CJIS) Security Standard
Federal Trade Commision Act (FTCA) Section 5 (unfair and deceptive business practices)
Health Insurance Portability and Accountability Act (HIPAA) Security Rule
Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule
HITRUST v6.1
Individuals with Disablibilities Education Act (IDEA)
International Standards Organization ISO / IEC 27001-2013
International Standards Organization ISO / IEC 27002-2013
NIST 800-53 v4 Control Baselines (FISMA, low, mod, high)
PCI-DSS v3
Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies (GWAS)
Protection of Pupil Rights Amendment (PPRA)
The Cancer Genome Registry Data Use Agreement
U.S. - E.U. Safe Harbor Privacy Principles

Data Classification

- Three-tiers
  - Social Security Number
  - First Name / First Initial and Last Name
  - Student Educational Records (Schedule, Academic Standing, Evaluation, Grades, Demographics, etc.)
  - Student Directory Information (Click here for details on VCU student directory information)
  - Employee / Personnel Records (Pay Information, Disciplinary Records, Awards / Credentials, Attendance Records, etc.)
  - Driver's License or State / Federal ID Numbers
  - Credit Card / Debit Card Numbers
  - Other Financial Records
  - Medical or Mental History
  - Medical Treatment or Diagnoses information
  - Health Insurance Policy Numbers
  - Other Protected Health Information (Electronic or Paper)
  - Contract / Grants Information
  - Non-Public Research and Intellectual Information
  - Human Subject Research Information
  - Investigative / Court Information
  - Internal memos / Documentation / Reports / Code or any other non-public business documents
  - Export Controlled Information (ITAR / EAR / DFAR / OFAC etc.)
  - Criminal Justice Information (Arrest records, criminal offense records, etc.)
  - Sensitive or confidential information of business partners or third party individuals / organizations
  - Other Regulated / Private / Protected / Confidential Information
- Combination of elements will be classified as CAT II or I

Step two

- The mapping process
  - Map compliance requirements to capabilities
    - Examine current University technology capabilities in accordance with the compliance requirements
    - Examine and map documentation, processes to regulatory requirements
    - Consulted other security frameworks (HITRUST, ISO27000)
    - List individual and common requirements for each regulation and map them back to data types
    - Construction of a custom data security and compliance framework.
      - Regulatory obligations
      - Existing processes / capabilities
      - Security Frameworks
      - Risk Tolerance

Step three

- So what's next?
  - Must educate and obtain individual buy-in
    - Collaborated with the University Data and Information Management group (Governance Group) and defined the individual roles for data management
      - Data Trustee (VP or above)
      - Data Stewards (Directors of authoritative functions for data)
      - Data Custodians (Individuals / Consumers of data)
        - » IT Administrators

Step three continued

- Mapped out the data stewardship in relation to data types:
  - **FERPA:** Registrar / Enrollment
  - **PCI-DSS:** University Treasury
  - **Research medley:** Office of Research
  - **HIPAA / HITECH:** VCU ACE / Research / VCUHS
  - **FISMA:** Office of Research
  - **Export Control:** Office of Research
  - **CJIS:** VCUPD
  - **GLBA:** Financial Aid / Enrollment
  - **Employment data:** HR
  - **PII (Code of VA):** HR / All parties
  - **Donor information:** Office of Development and Alumni Relations

Step three continued…

- So what's next?
  - Must educate and obtain individual buy-in
    - Met with each data steward separately and examined the framework to obtain their expert opinion and their buy-in
      - Each steward is contacted with an early draft of the framework and asked to review and provide comments.
      - A 1.5 hours meeting is setup with each steward for the review of the relevant portions of the framework
      - Modified the framework according to feedback from the stewards
      - Additional data types and regulations were examined as a result
      - Added sections on how to meet requirements

Step three continued…

- So what's next?
  - Must educate and obtain individual buy-in
    - Collaborated with VCU Health System and both organizations agreed to follow the same set of framework.
      - Ensure employees serving both organizations will follow the same consistent set of requirements
      - Ensure data security / privacy controls addressed are consistent across both organizations

The framework

- Columns contain data types
  - 30 specific data types
  - SSN, Driver's License Numbers, Intellectual info, etc.
- Rows contain guidelines / requirements
  - Separated into different sections

Framework overview

- Sections: Broken down into several smaller sections
  - University specific
    - Data storage tools
    - Data networks
    - Data transmission tools
    - Other Media
    - Related policies and procedural documentation

		IT Admin	Data Trustee	Data Steward	Data Custodian	SSN	First name, init / Last name	Student Educational Records (Non-directory Information)	Stu inf
A.	Data Storage Tools								
A1.	VCU Google Drive	X	X	X	X	Yes, must be properly used	Yes	Yes, must be properly used	Yes
A2.	University Central File Servers	X	X	X	X	Yes	Yes	Yes	Yes
A3.	VCU Managed Encrypted Local Computer	X	X	X	X	Yes	Yes	Yes	Yes
A4.	VCU Managed Unencrypted Local Computer	X	X	X	X	No	Yes	No	Yes
A5.	Personal or un-managed computer	X	X	X	X	No	Yes	No	Ass nee
A6.	Public use computer	X	X	X	X	No	Yes	No	No
A7.	DropBox	X	X	X	X	No	Assessment / Approval Needed	No	Ass nee
A8.	Other Personal Cloud Storage Provider	X	X	X	X	No	Assessment / Approval Needed	No	Ass nee
A9.	Other Enterprise Cloud Storage Provider	X	X	X	X	Assessment / Approval needed	Yes	Assessment / Approval needed	Ass nee
A10.	VCU FileDrop*** (Evaluation pending)	X	X	X	X	Yes, encrypted	Yes	Yes, encrypted	Yes
A11.	Unencrypted flash drive / Ext HD / Tape	X	X	X	X	No	Yes	No	Ass nee
A12.	Encrypted flash drive / Ext HD / Tape	X	X	X	X	Yes	Yes	Yes	Yes
A13.	VCU QuestionPro survey software	X	X	X	X	No	Yes	No	Yes

B.	Data Networks*							
B1.	VCU faculty and staff network (SecNet)	X		X		Yes	Yes	Yes
B2.	VCU Research Network (ResearchNet)	X		X		Yes, encrypted	Yes	Yes
B3.	VCU Academic Network (AcademicNet)	X		X		Yes, encrypted	Yes	Yes
B4.	VCU SafeNet wireless network	X		X		Yes, encrypted	Yes	Yes
B5.	VCU Guest network	X		X		Assessment / Approval Needed	Yes	Ass
B6.	VCU Dorm Wired network	X		X		Assessment / Approval Needed	Yes	Ass
B7.	VCU MCV Campus MedNet	X		X		Yes	Yes	Yes
B8.	VCU PCI network (PCINet)	X		X		No	Yes	No
B9.	VCU DMZ (ServDMZ)	X		X		Yes, encrypted	Yes	Yes
B10.	VCU Internal non-public facing server network (ServNet)	X		X		Yes	Yes	Yes

Framework overview

- Sections: Broken down into several smaller sections
  - Common requirements:
    - Administrative requirements
    - Data security requirements
    - Device security requirements
    - Application security requirements
    - Network security requirements
    - Infrastructure security requirements
    - Physical security requirements
    - Personnel security requirements
    - Administrative documentation / procedures needed
    - Third party hosting / contracting

		IT Admin	Data Trustee	Data Steward	Data Custodian	SSN	First name, init / Last name
F.	Administrative requirements						
F1.	Definition and documentation of roles and responsibilities	I	A, C, I	R, C, I	C, I	Required	Required
F2.	Periodic evaluation / audit of processes for handling data	R, I	A, I	R, C, I	I	Recommended	Not required
F3.	Periodic review and removal of unneeded data	R, C, I	A, I	R, C, I	R, C, I	Recommended	Not required
F4.	Must complete project risk assessment (incl. Business Impact Analysis)	C	A, I	R, C, I	I	Required	Not required
F5.	Must complete system and data security plan review	R, C, I	A, I	R, C, I	I	Required	Recommended
F6.	Must complete periodic penetration testing and remediation at least annually	R, C, I	A, I	R, C, I	I	Recommended	Not required
F7.	Identify / Document critical business processes supported by system and data	C	A, C, I	R, C, I	C	Recommended	Not required
F8.	Formal employee sanction process for non-compliance	C, I	A, I	R, C, I	C, I	Recommended	Not required
F9.	Communication of applicable policies and procedures to individuals handling the data	I	A, I	R, C, I	I	Recommended	Not required
F10.	Must complete security review before external party is given access to data	R, I	A, I	R, C, I	I	Required	Not required
F11	Asset and media inventory must be kept for assets accessing / containing data	R, I	A, I	R, C, I	I	Recommended	Not required

		Credit / Debit Card Info	University Financial Records	Financial A
G.	Data security requirements			
G1.	Authentication for data access	Required	Required	Required
G2.	Account user name must be longer than 6 characters	Recommended	Not Required	Not Requir
G3.	Password / passphrase used must meet VCU password policy	Required	Required	Required
G4.	Password / passphrase used must meet dbGaP regulatory requirements	Not Required	Not Required	Not Requir
G5.	Change password / passphrase at least every 90 days	Required	Not Required	Not Requir
G6.	Change password / passphrase at least every 365 days	Not Applicable	Required	Required
G7.	Multi-factor authentication for data access	Recommended	Not Required	Recommen
G8.	Data stored in shared systems must be logically separated from other, less sensitive data	Required	Not Required	Recommen
G9.	Default deny access control must be implemented for data	Required	Recommended	Required
G10.	Secure data backup (w/ documented procedures)	Required	Required	Required
G11.	Create a secure backup copy of data before movement of equipment	Recommended	Not Required	Recommen
G12.	Secure disposal of data when no longer needed	Required	Recommended	Required
G13.	VCU / VCUHS centrally managed backup	Recommended	Recommended	Recommen
G14.	Logging and auditing of account / data creation, access, modification, and deletion	Required	Recommended	Recommen

Framework overview

- Sections: Broken down into several smaller sections
  - Data retention section
  - Other requirements section
  - Privacy requirements

		Credit / Debit Card info	University Financial Records	Financial Aid informat
Q.	Other requirements			
Q1.	Store the data outside of U.S	No	Assessment / Approval needed	Assessment / Approva needed
Q2.	MOU required with internal department before providing access	Required	Not required	Recommended
Q3.	Must be U.S. Person to handle data	Not required	Not required	Not required
Q4.	Cannot use shared or group accounts to access data	Required	Not Required	Recommended
Q5.	Voice network must meet local legal requirement for emergency communications	Not required	Not required	Not required
Q7.	Annual request must be sent to data provider for renewal or termination of data access	Not Applicable	Not Applicable	Not Required
Q8.	Data cannot be shared with any other party not explicitly approved by data provider	Not Applicable	Not Applicable	Not required
R.	Privacy requirements			
R1.	Seek individual consent before disclosing data to employers	Not Applicable	Not Applicable	Required
R2.	Seek consent / disclosure agreement with individual if data maybe shared with others	Not Applicable	Recommended	Required
R3.	Ensure that minimum amount of data is shared (based on need-to-know)	Required	Recommended	Recommended
R4.	Must maintain records for disclosures or requests of disclosures for individual record	Not Applicable	Not Required	Required
R5.	Must provide individuals and / or guardian (if minor) with access to their own data	Not Required	Not Applicable	Required
R6.	Must allow individuals and / or gurdian (if minor) to amend data	Not Required	Not Applicable	Required
R7.	Must provide individuals and / or guardian (if minor) with means to report privacy violations	Recommended	Recommended	Required
R8.	Must establish process and procedures to investigate reported privacy / security violations	Required	Recommended	Required
R9.	Periodically review / revise security / privacy incident response procedures	Required	Not Required	Recommended
R10.	Must not retaliate against individuals for reporting inappropriate behavior or violations	Recommended	Recommended	Required
R11.	Must provide acceptable collection / use / privacy notice to individuals / or guardian (if minor) providing data	Not Required	Not Applicable	Required
R12.	Seek verifiable consent from parent before collecting information	Not required	Not required	Not required
R13.	Seek written parental consent before collection or dissemination	Not required	Not required	Assessment / Approva Needed
R14.	Allow parents / guardians to inspect instructional materials	Not Applicable	Not Applicable	Not Applicable

So following this work…

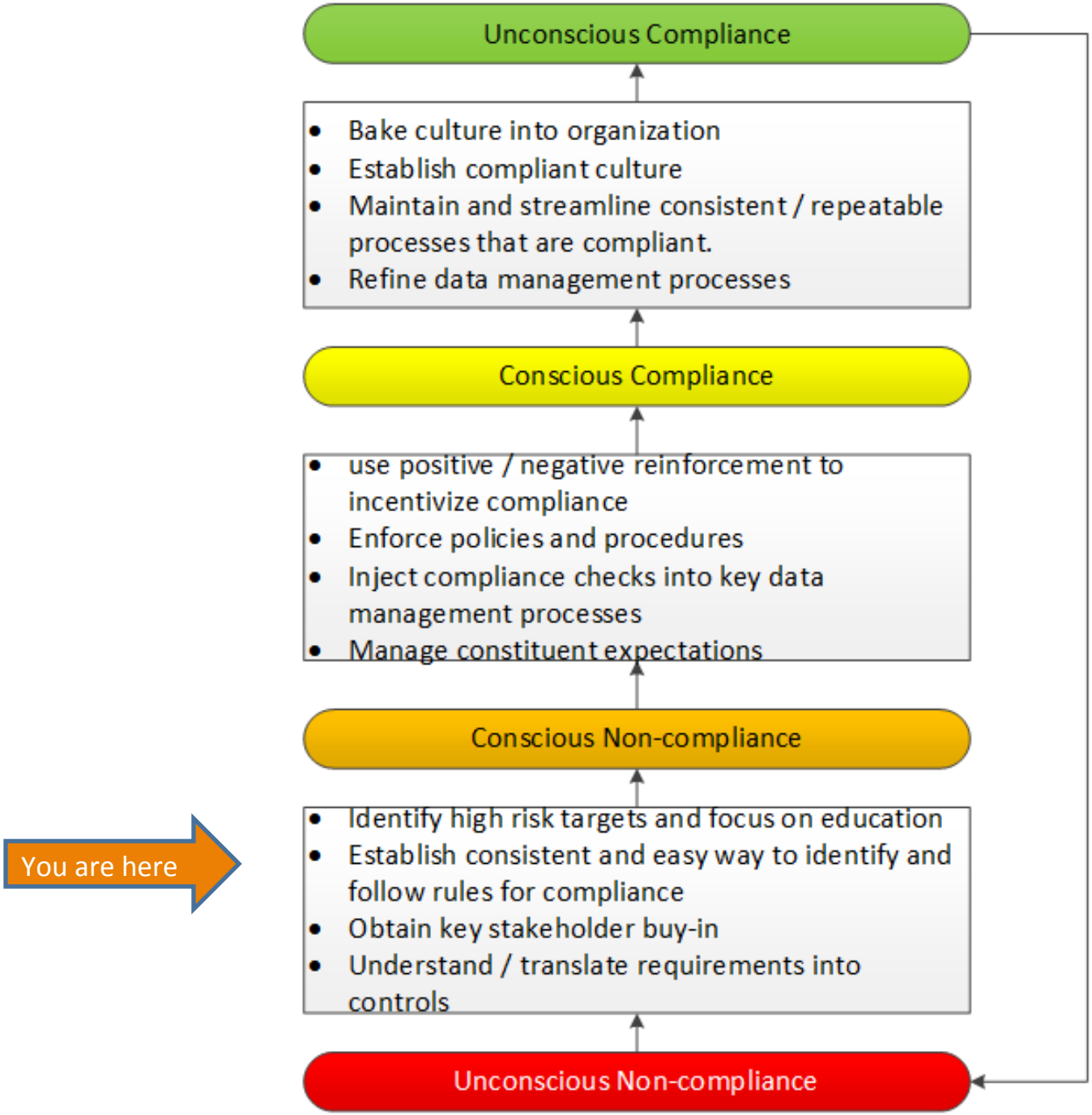
We have developed a data classification formula and a framework

- Complex formula that classifies combinations of data elements
- Spreadsheet
  - close to 400 rows
  - Over 30 columns
  - A RACI chart

Bridging document between regulatory requirements and data management practices

Are we done?

It is unrealistic to expect a constituent to sift through all of this information


Unconscious Compliance
Bake culture into organization
Establish compliant culture
Maintain and streamline consistent / repeatable processes that are compliant.
Refine data management processes
Conscious Compliance
use positive / negative reinforcement to incentivize compliance
Enforce policies and procedures
Inject compliance checks into key data management processes
Manage constituent expectations
Conscious Non-compliance
Identify high risk targets and focus on education
Establish consistent and easy way to identify and follow rules for compliance
Obtain key stakeholder buy-in
Understand / translate requirements into controls
Unconscious Non-compliance
You are here

Data Classification Tool

- Web based tool that can classify data based on selection of data elements
- Provides basic information about the data category and who to contact
- Distributed to Data Stewards and injected into application / system provisioning processes

VCU Data Classification Tool

This tool is designed for you to determine the sensitivity of your data. Please check all applicable data elements to see the classification of your combined data set.

The Data Classification Tool allows you to determine the classification of the data combination as specified below. To use this tool, simply check the desired data elements below to see the combined categorization information.

This tool applies to data generated, collected, or otherwise handled by the University for its academic, research, and administrative functions, and any third party data used by University personnel for university related business.

* must provide value

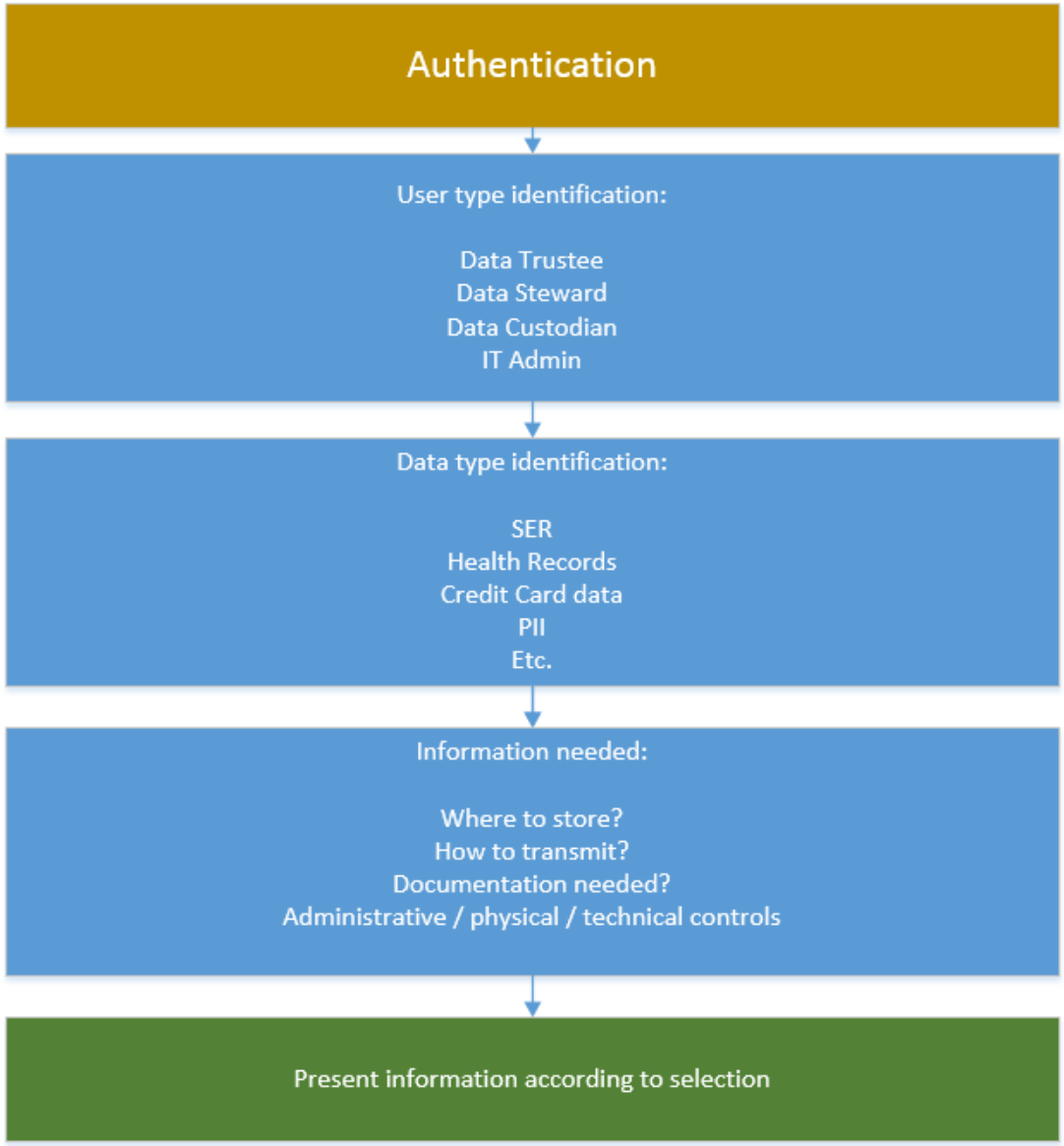
Select all data types that will be stored, processed or transmitted by the IT system:

- [ ] Social Security Number
- [ ] First Name / First Initial and Last Name
- [ ] Student Educational Records (Schedule, Academic Standing, Evaluation, Grades, Demographics, etc.)
- [ ] Student Directory Information (Click here for details on VCU student directory information)
- [ ] Employee / Personnel Records (Pay Information, Disciplinary Records, Awards / Credentials, Attendance Records, etc.)
- [ ] Driver's License or State / Federal ID Numbers
- [ ] Credit Card / Debit Card Numbers
- [ ] Other Financial Records
- [ ] Medical or Mental History
- [ ] Medical Treatment or Diagnoses information
- [ ] Health Insurance Policy Numbers
- [ ] Other Protected Health Information (Electronic or Paper)
- [ ] Contract / Grants Information
- [ ] Non-Public Research and Intellectual Information
- [ ] Human Subject Research Information
- [ ] Investigative / Court Information
- [ ] Internal memos / Documentation / Reports / Code or any other non-public business documents
- [ ] Export Controlled Information (ITAR / EAR / DFAR / OFAC etc.)
- [ ] Criminal Justice Information (Arrest records, criminal offense records, etc.)
- [ ] Sensitive or confidential information of business partners or third party individuals / organizations
- [ ] Other Regulated / Private / Protected / Confidential Information

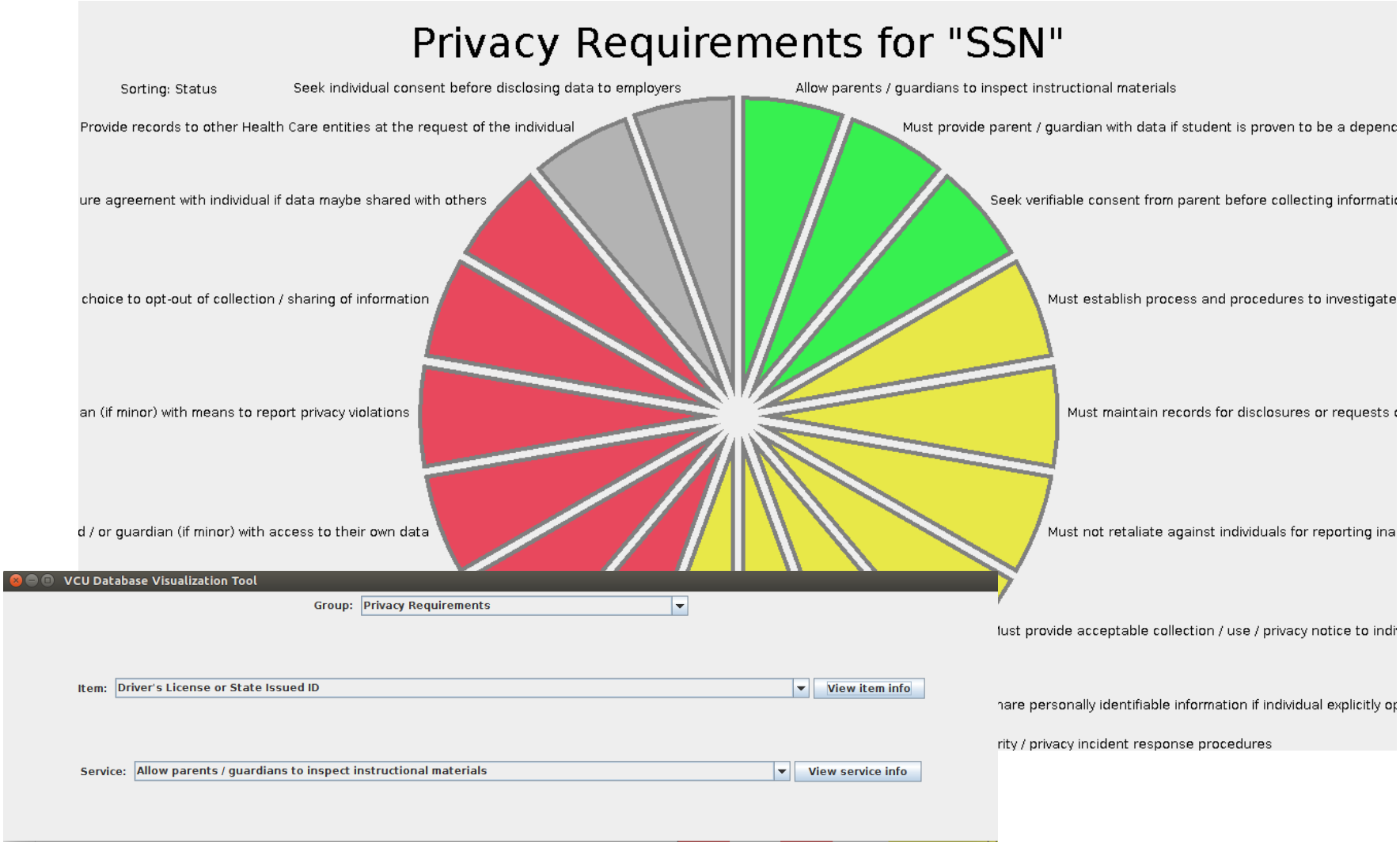
The next steps

- Establish a consistent and user-friendly way for folks to understand the requirements
  - The daunting spreadsheet problem
  - Application development
  - Injecting the application into key data management processes.

Application concept



Thanks to our friends at VT



Recommendations & Conclusion

- Understand the applicable regulatory requirements
- Classify your data
- Maintain data governance structure and properly assign responsibilities and accountability for data management
- Choose a data management framework and modify it to fit your organizational needs
- Obtain buy-in from data managers / stewards
- Identify and catalog the existing tools and processes used for data management, fill the gaps, streamline and simplify where possible
- Create easy to use tools for constituents to understand organizational expectations for data management
- Identify key data flow processes from data managers & Inject data management tools and processes into these processes
- Educate constituents who use and manage data

Thank you, questions?