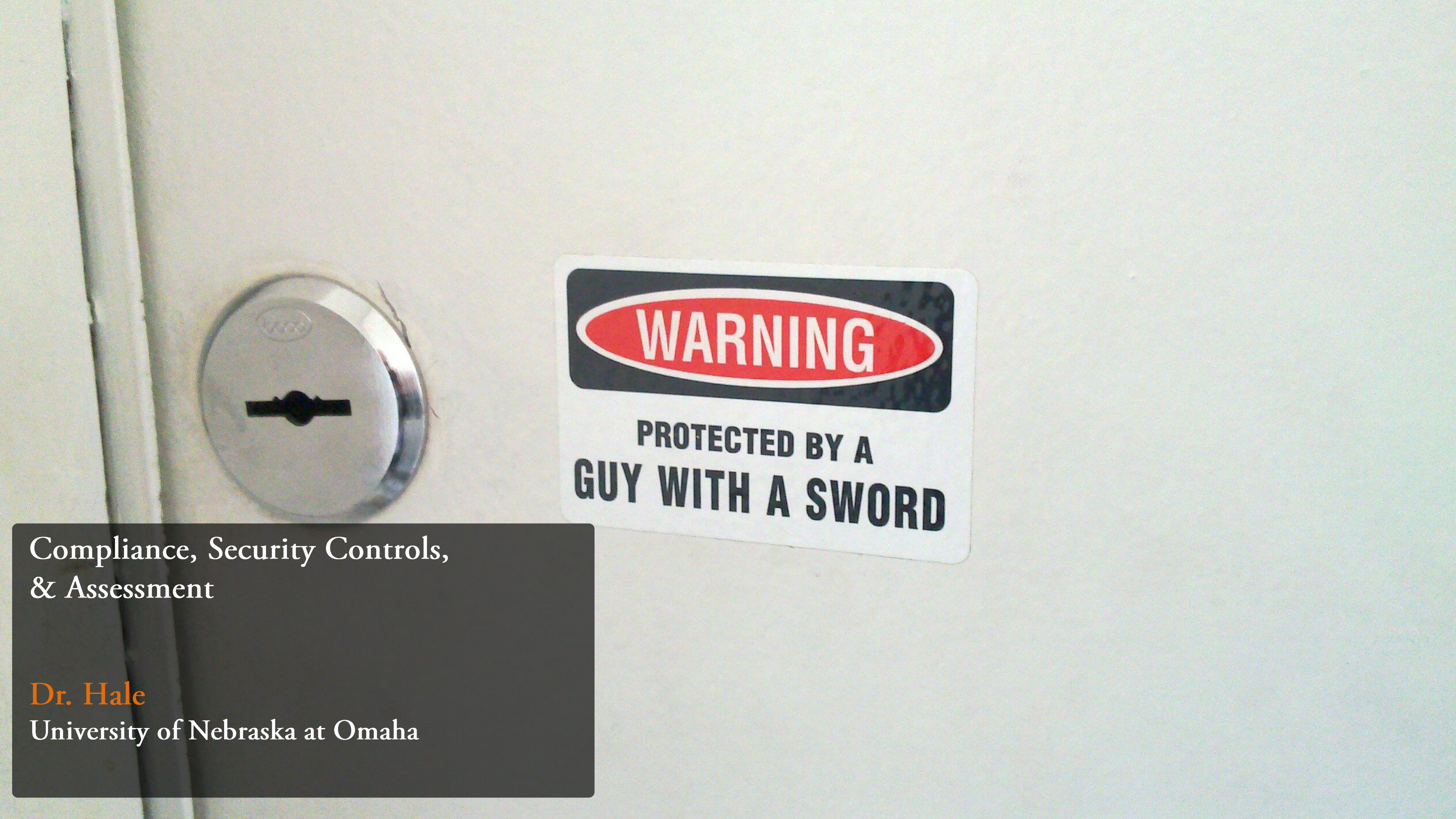


Compliance, Security Controls, & Assessment

Dr. Hale
University of Nebraska at Omaha

Today’s topics:

Review of Policy Documents

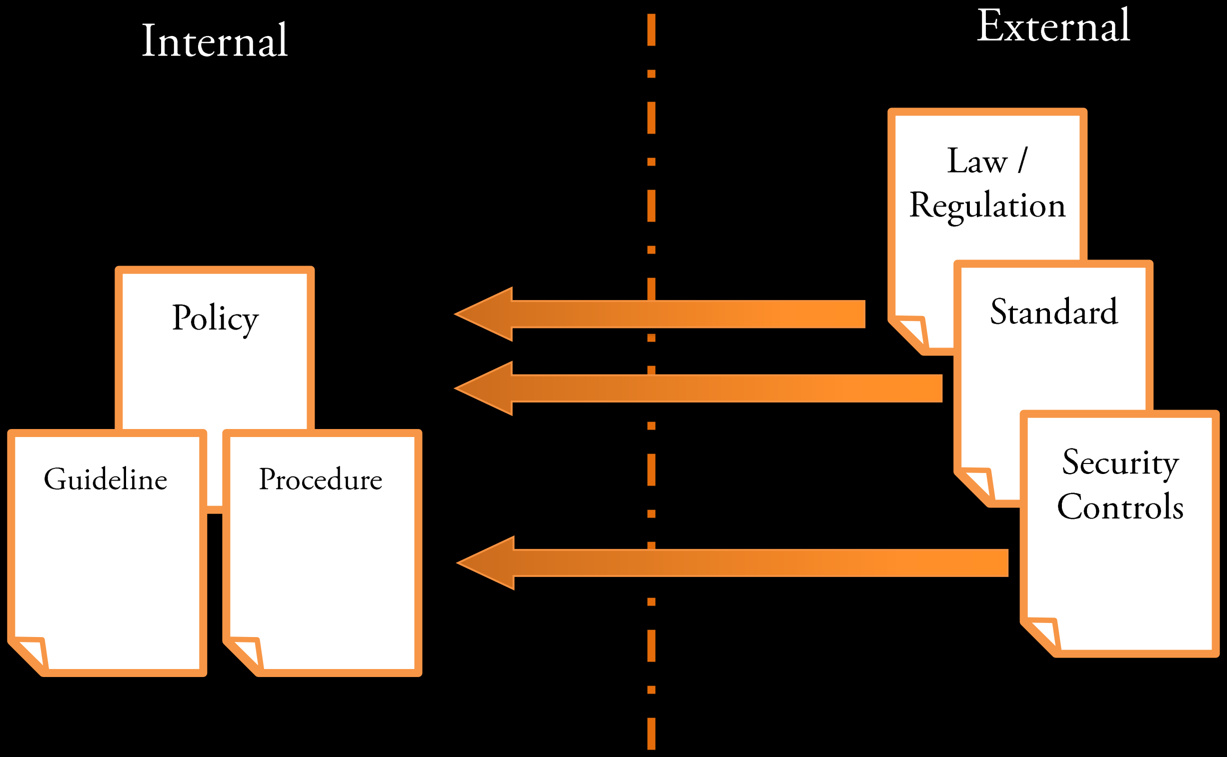
Overview of Laws and Standards

Review of Security Controls

How to use controls and frameworks in development and testing

Resources and Tooling for assessment

Different types of policy documents



Internal

External

Law / Regulation

Standard

Security Controls

Policy

Guideline

Procedure

U.S. Info. Sec. Laws

Law / Regulation	Applies to	Scope of Governance
Health Insurance Portability and Accountability Act (HIPAA)	Heath care providers, health insurance providers	Applies to privacy of any protected health information
Federal Information Security and Management Act (FISMA)	All government agencies, all entities that process federal data	Information security (all domains)
Gramm-Leach-Bliley Act (GLBA)	Banks, Investment companies, financial service providers	Customer data privacy
Sarbanes-Oxley Act (SOX)	Public corporations	Financial accuracy and public disclosure to investors
Family Educational Rights and Privacy Act (FERPA)	Educational organizations (schools)	Privacy of student records
Children's Internet Protection Act (CIPA)	Federally funded Schools and libraries	Access to sexually explicit materials on computers
Attempts (SOPA- PIPA)	Nothing	Thank goodness

(some) U.S. Info. Sec. Industry Standards

Standard	Applies to	Scope of Governance
PCI-DSS	Payment card industry (almost everyone)	Regulates transaction, point of sale system, and network security
Common Criteria ISO/IEC 15408	Organizations that want to certify their systems or products	A system or set of systems in an Org. E.g. windows XP is CC certified
ITIL (Information Technology Infrastructure Library) ISO/IEC 20000	Businesses with IT seeking best practices. Typically large companies	All IT in an organization
ISO/IEC 27000 series Information Technology Security Techniques Code of Practice for Information Security Management	Organizations that want a security certification to show their customers and clients	All information security elements of an organization

Definition:

A *Security Control* is a safeguard or countermeasure that is either preventative, detective, or corrective.

Think of controls as mandatory *policy guidelines* that target specific areas

Preventative Control

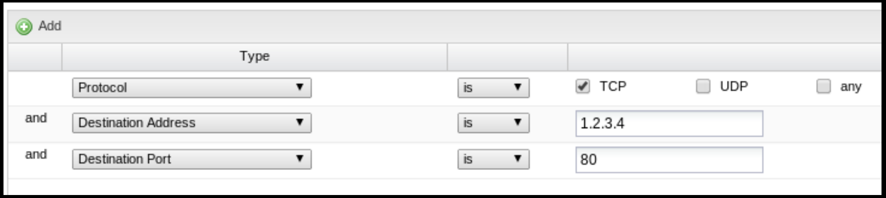
- Mitigates risks/attacks immediately
  - e.g. firewall for port scanning
- or prevents them entirely
  - e.g. strong encryption for MiTM passive observation

Detective Control

- doesn't prevent attacks
- alerts end-user or administrators of attack
- e.g. audit log review

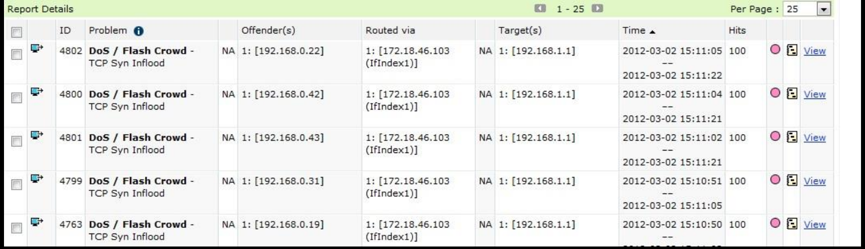
Corrective Control

- doesn't prevent attacks
- limits the impact of attacks by restoring functionality or patching issues
- e.g. backup and recovery



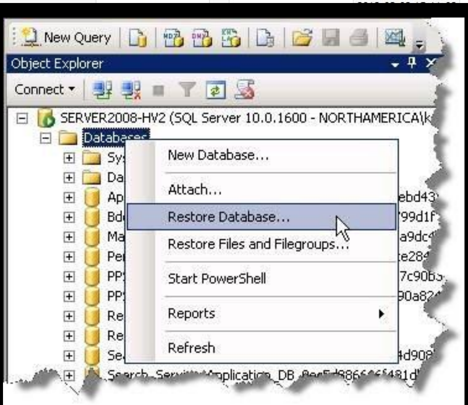
Add

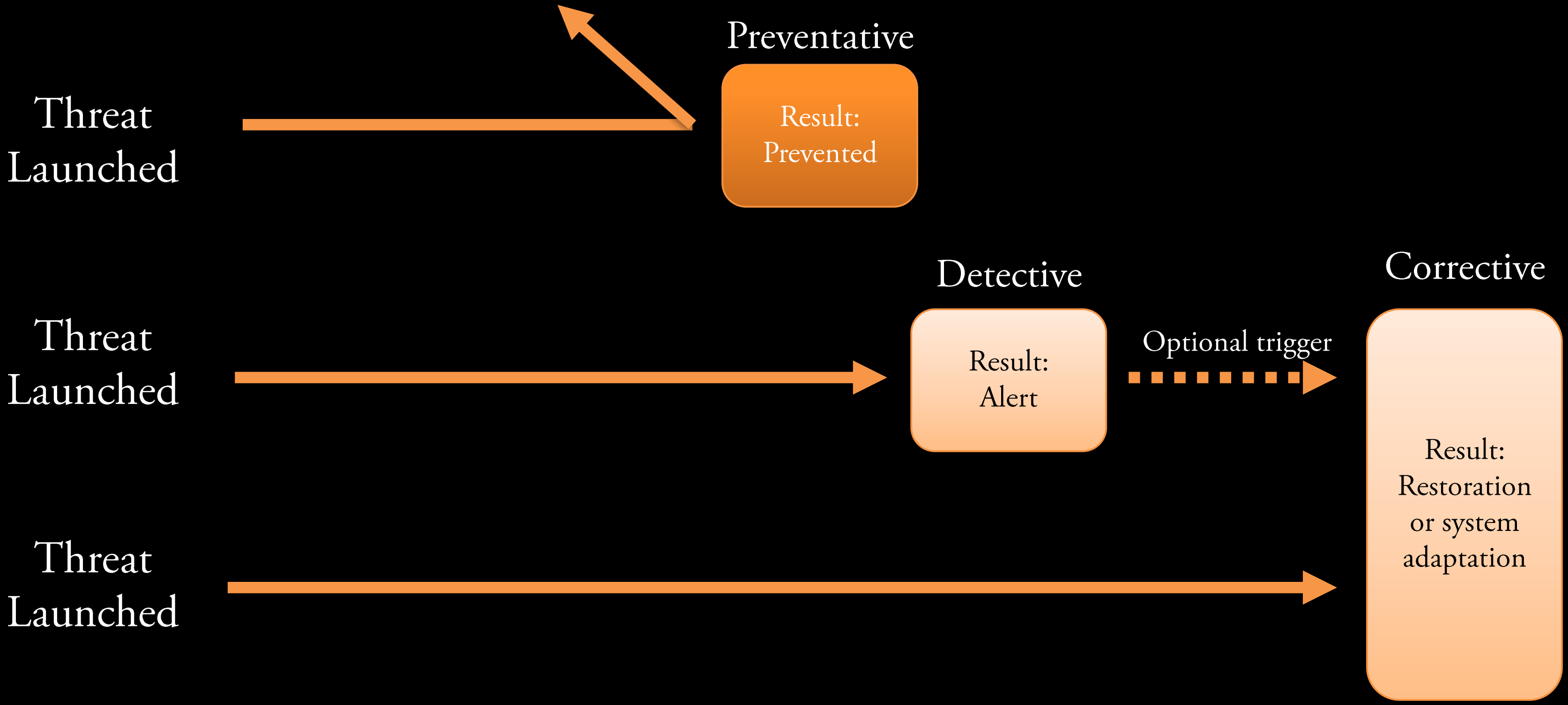
	Type		
	Protocol	is	☑ TCP ☐ UDP ☐ any
and	Destination Address	is	1.2.3.4
and	Destination Port	is	80



Report Details — 1 - 25 — Per Page : 25

☐		ID	Problem		Offender(s)	Routed via		Target(s)	Time ▲	Hits			
☐		4802	**DoS / Flash Crowd -** TCP Syn Infload	NA	1: [192.168.0.22]	1: [172.18.46.103 (IfIndex1)]	NA	1: [192.168.1.1]	2012-03-02 15:11:05 -- 2012-03-02 15:11:22	100	●		View
☐		4800	**DoS / Flash Crowd -** TCP Syn Infload	NA	1: [192.168.0.42]	1: [172.18.46.103 (IfIndex1)]	NA	1: [192.168.1.1]	2012-03-02 15:11:04 -- 2012-03-02 15:11:21	100	●		View
☐		4801	**DoS / Flash Crowd -** TCP Syn Infload	NA	1: [192.168.0.43]	1: [172.18.46.103 (IfIndex1)]	NA	1: [192.168.1.1]	2012-03-02 15:11:02 -- 2012-03-02 15:11:21	100	●		View
☐		4799	**DoS / Flash Crowd -** TCP Syn Infload	NA	1: [192.168.0.31]	1: [172.18.46.103 (IfIndex1)]	NA	1: [192.168.1.1]	2012-03-02 15:10:51 -- 2012-03-02 15:11:05	100	●		View
☐		4763	**DoS / Flash Crowd -** TCP Syn Infload	NA	1: [192.168.0.19]	1: [172.18.46.103 (IfIndex1)]	NA	1: [192.168.1.1]	2012-03-02 15:10:50 --	100	●		View





Threat Launched

Preventative

Result: Prevented

Threat Launched

Detective

Result: Alert

Optional trigger

Corrective

Threat Launched

Result: Restoration or system adaptation

Intro to compliance

Controls can be:

- technical (apply to systems, apps, networks, etc)
- operational/managerial (apply to people, organizations, etc)
- physical (apply to buildings, doors, etc)

Note: Sometimes managerial controls are split entirely into their own category (e.g. NIST)

Technical Controls

Involve applying protections to systems, software components, networks, and/or data.

Operational Controls

Dictate human behavior, requires training
May require employees, external staff, or managers to behave in certain ways
E.g. Not respond to phishing email

[small subset of] Operational Controls - Managerial

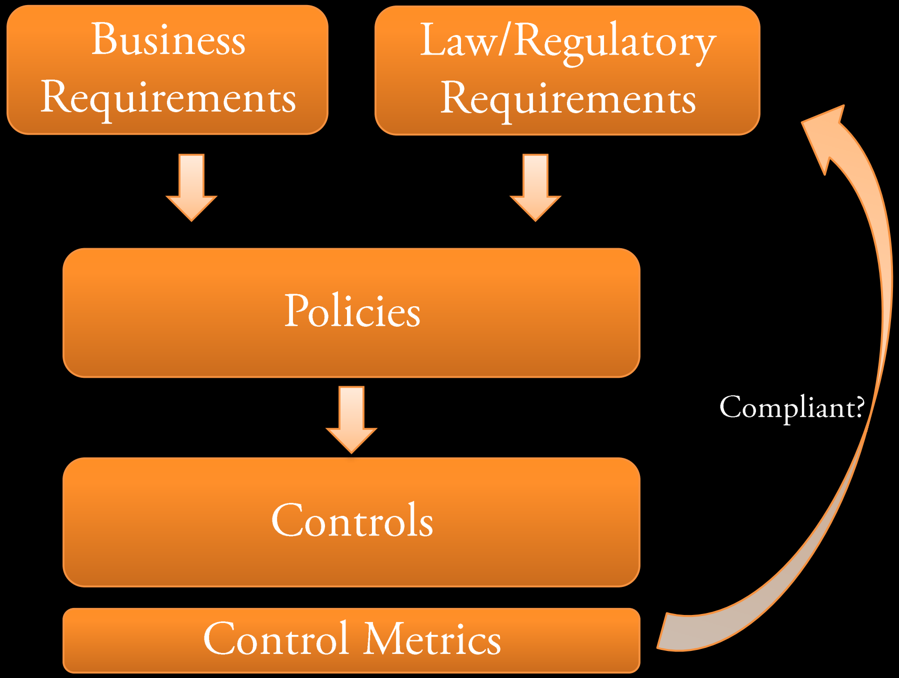
May also dictate organizational behavior or structure
(e.g. annual reviews, planning requirements, designated officials, etc)

Physical Controls

Dictates parameters that structure the real world
e.g. require hardware to be in a locked server closet,
have a guard posted at a door, or
use cameras for surveillance

Linking controls to requirements

- Laws / regulatory selections and business requirements set policy
- Policies should support business requirements and satisfy regulatory demands
- Controls implement Policies
- Metrics measure control satisfaction
- Satisfying metrics means being compliant with regulatory requirements



So how do I actually work with controls?

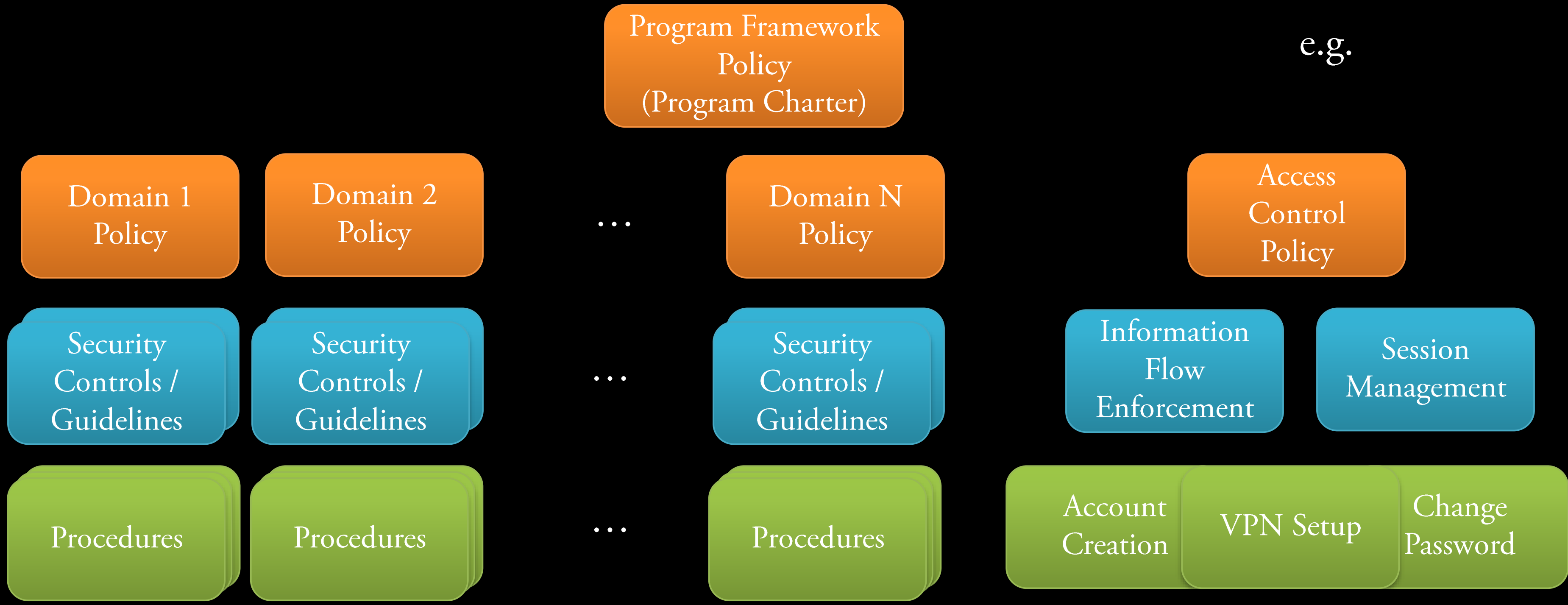
Typically you will use a *control framework*.

Policy Frameworks

Definition:

A *Control Framework* is a structured collection of security controls that implements policy to create business value and minimize enterprise risks.

Control Framework



Program Framework Policy (Program Charter)

e.g.

Domain 1 Policy

Domain 2 Policy

…

Domain N Policy

Access Control Policy

Security Controls / Guidelines

Security Controls / Guidelines

…

Security Controls / Guidelines

Information Flow Enforcement

Session Management

Procedures

Procedures

…

Procedures

Account Creation

VPN Setup

Change Password

Policy Frameworks

You can build this yourself.
But why re-invent the (very well designed) wheel(s)

Policy Frameworks

CSA cloud security alliance℠

DoD Issuances

The Official Department of Defense Website for DoD Issuances

(open) security control document players

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

Common Criteria

Security Control Frameworks

Framework	Type of Organizations	Implements?
NIST SP 800-53 Recommended Security Controls for Federal Information Systems	Federal, Federal Contractors, some Industry	FISMA, Other federal risk management processes (SP 800-37), FIPS 199/200
NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	Any, particularly Federal or Hospitals	HIPAA
Control Objectives for Information and related Technology (COBIT)	Industry	ITIL (compatible with 27000 series as well)
ISO/IEC 27000 series Information Technology Security Techniques Code of Practice for Information Security Management	Industry	Itself (it's a standard and a framework)
Common Criteria ISO/IEC 15408	Organizations that want to certify their systems or products	Itself (it's a standard and a framework)
DoDi 8500.01: Defense Department Cybersecurity Instruction	All DoD	Itself and a bunch of other related documents
Cloud Security Alliance CCM (Cloud Control Matrix)	Cloud vendors	COBIT, PCI, NIST, ISO 27000 series for cloud services

(Discussion of software assessment strategies)

https://www.nist.gov/cyberframework (Multi-doc Organizational overview for security risk mgmt.)
https://samate.nist.gov/Main_Page.html (Nice central portal for software assurance NIST docs)
https://samate.nist.gov/BF/ (Good Starting point for understanding bugs)
https://samate.nist.gov/index.php/Source_Code_Security_Analyzers.html (List of Tools for different purposes)
https://samate.nist.gov/SARD/ (Awesome project that catalogs test cases for different apps and systems)
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf
(has nice TL;DR Summaries for testing procedures)

Software Assessment

(Discussion of software assessment tooling)

https://www.owasp.org/index.php/Source_Code_Analysis_Tools (Collection of static analysis tools)
https://www.owasp.org/index.php/OWASP_Cheat_Sheet_Series (succinct curated info by topic)
https://www.owasp.org/index.php/OWASP_Testing_Project (full scale web app testing guide)
http://www.softwaretestinghelp.com/penetration-testing-tools/ (Nice curated list of pen testing tools)

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

faculty.ist.unomaha.edu/mhale/
mlhale@unomaha.edu

Twitter: @mlhale_