High Level Policy meets Compliance

Dr. Hale
University of Nebraska at Omaha
Information Security and Policy– Lecture 5

Today’s topics:

Last time recap

High Level Policy Wrap up

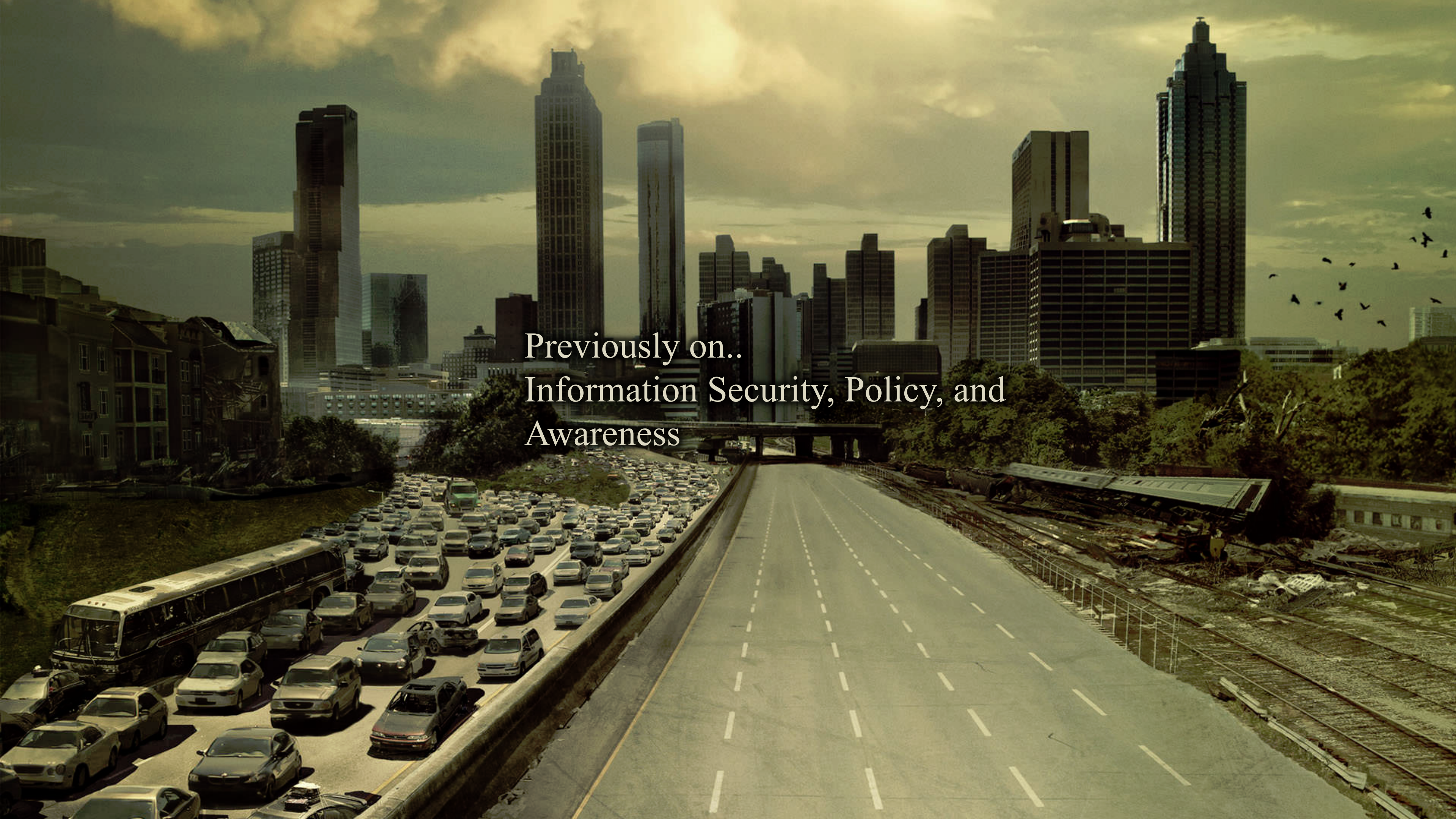
- Types of documents (expanded)
- Categorizing Policy by IT domain

Introduction to Compliance and Security Controls

- U.S. Compliance Laws
- Industry standards (Common Criteria, PCI-DSS, ITIL)
- Aligning Policy with Regulations and industry

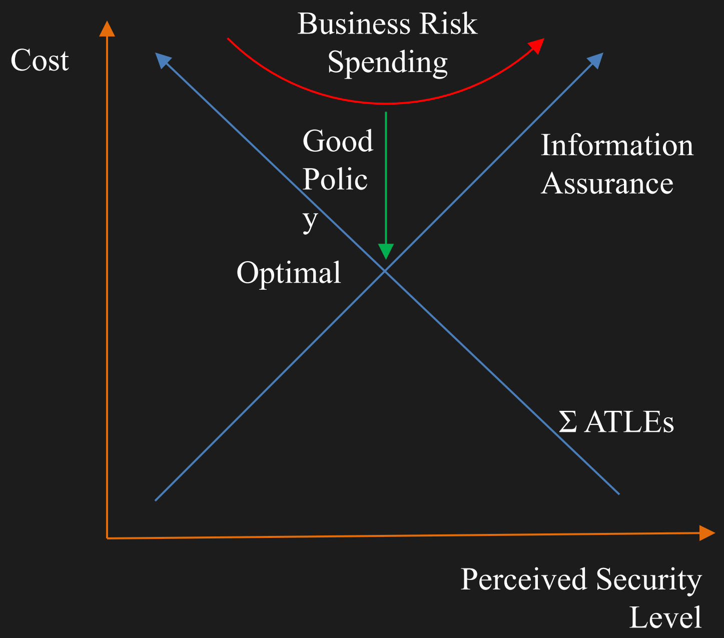
Policy/security control frameworks

- Model and its relation to the organization
- COBIT, ISO/IEC 27000, NIST SP800-53



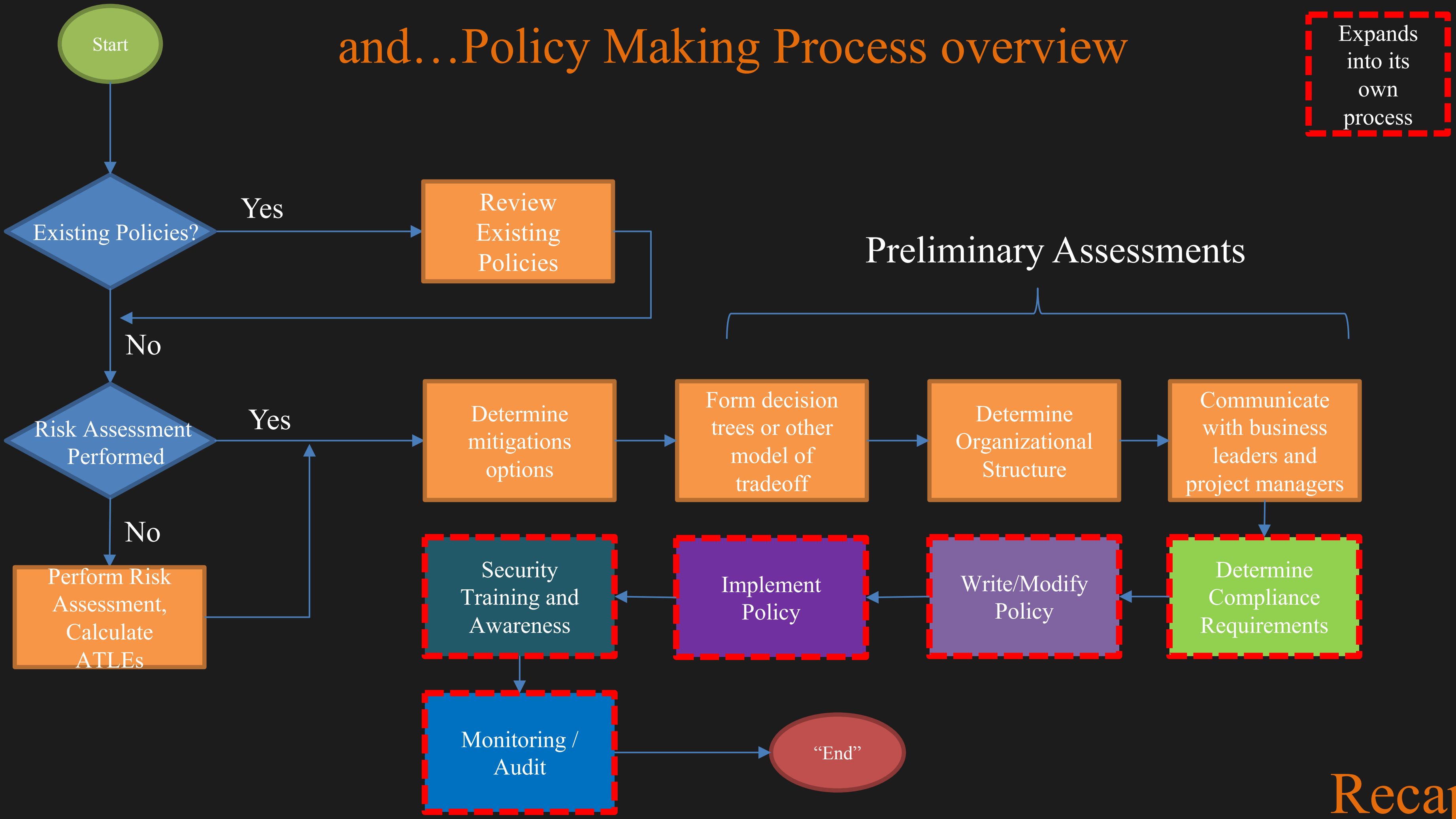
Previously on..
Information Security, Policy, and Awareness

good policies



Recap

and…Policy Making Process overview

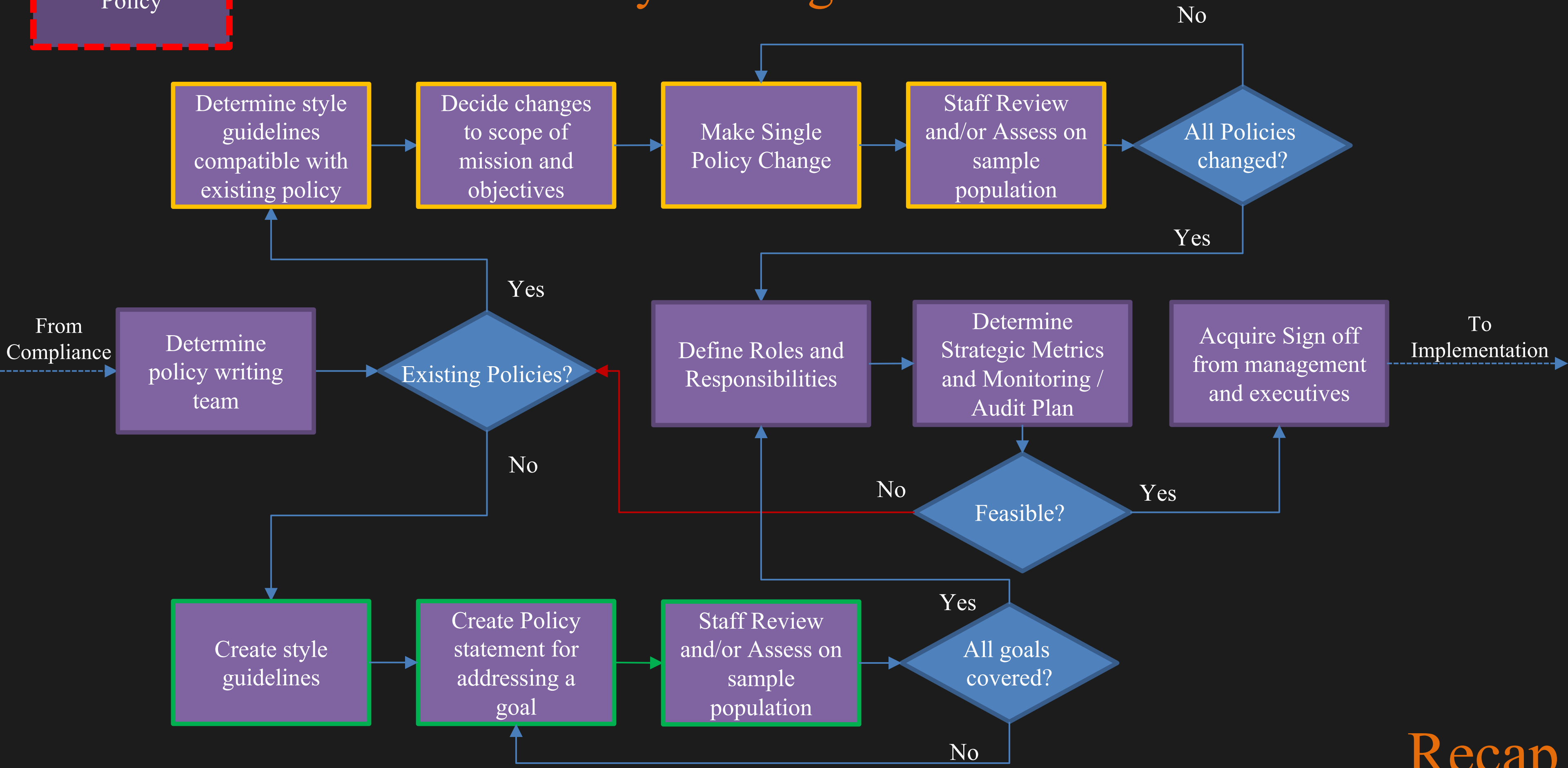


Start
Existing Policies?
Yes
Review Existing Policies
No
Risk Assessment Performed
Yes
No
Perform Risk Assessment, Calculate ATLEs
Preliminary Assessments
Determine mitigations options
Form decision trees or other model of tradeoff
Determine Organizational Structure
Communicate with business leaders and project managers
Determine Compliance Requirements
Write/Modify Policy
Implement Policy
Security Training and Awareness
Monitoring / Audit
"End"
Expands into its own process

Recap

Write / Modify Policy

Policy Writing Overview



From Compliance

Determine policy writing team

Existing Policies?

Yes

Determine style guidelines compatible with existing policy

Decide changes to scope of mission and objectives

Make Single Policy Change

Staff Review and/or Assess on sample population

All Policies changed?

No

Yes

No

Create style guidelines

Create Policy statement for addressing a goal

Staff Review and/or Assess on sample population

All goals covered?

No

Yes

Define Roles and Responsibilities

Determine Strategic Metrics and Monitoring / Audit Plan

Feasible?

No

Yes

Acquire Sign off from management and executives

To Implementation

Recap

Said we would return in later lectures

Determine Compliance Requirements

Implement Policy

Security Training and Awareness

Monitoring / Audit

Recap

This is a later lecture

Determine Compliance Requirements

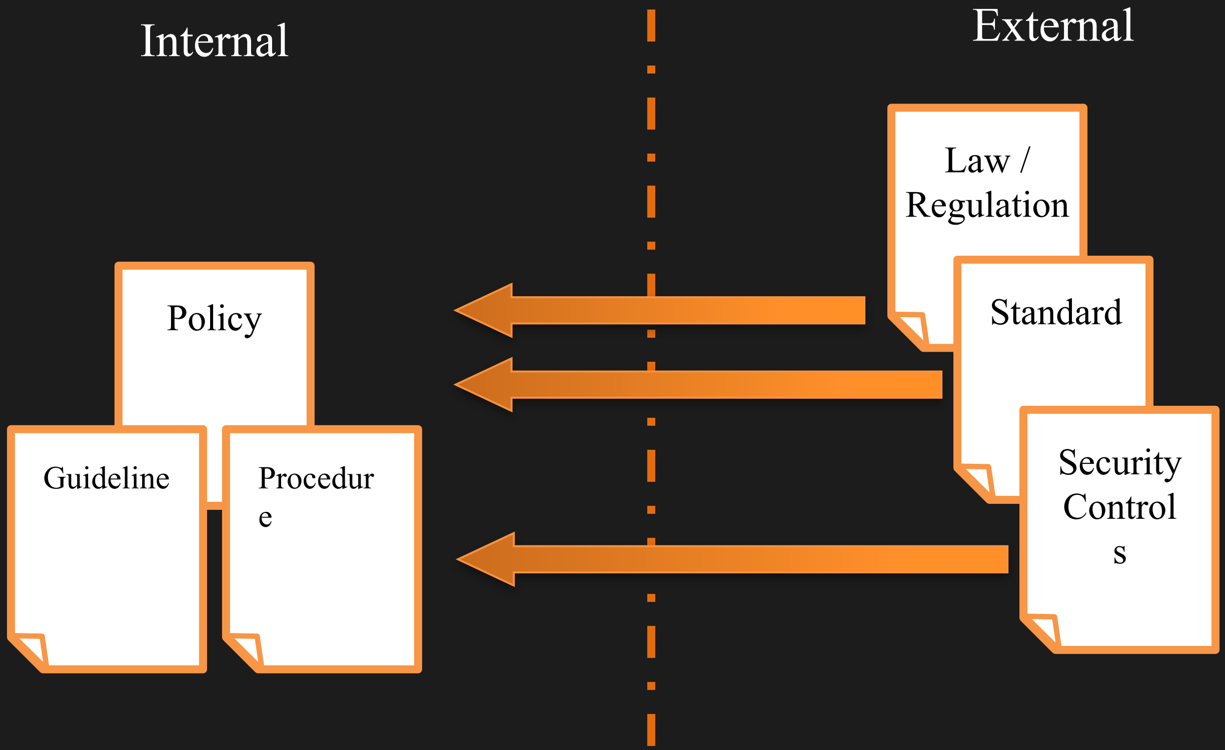
Then…

Implement Policy

But first…

High Level Policy Wrap up

Different types of policy documents



Internal

External

Law /
Regulation

Standard

Security
Control
s

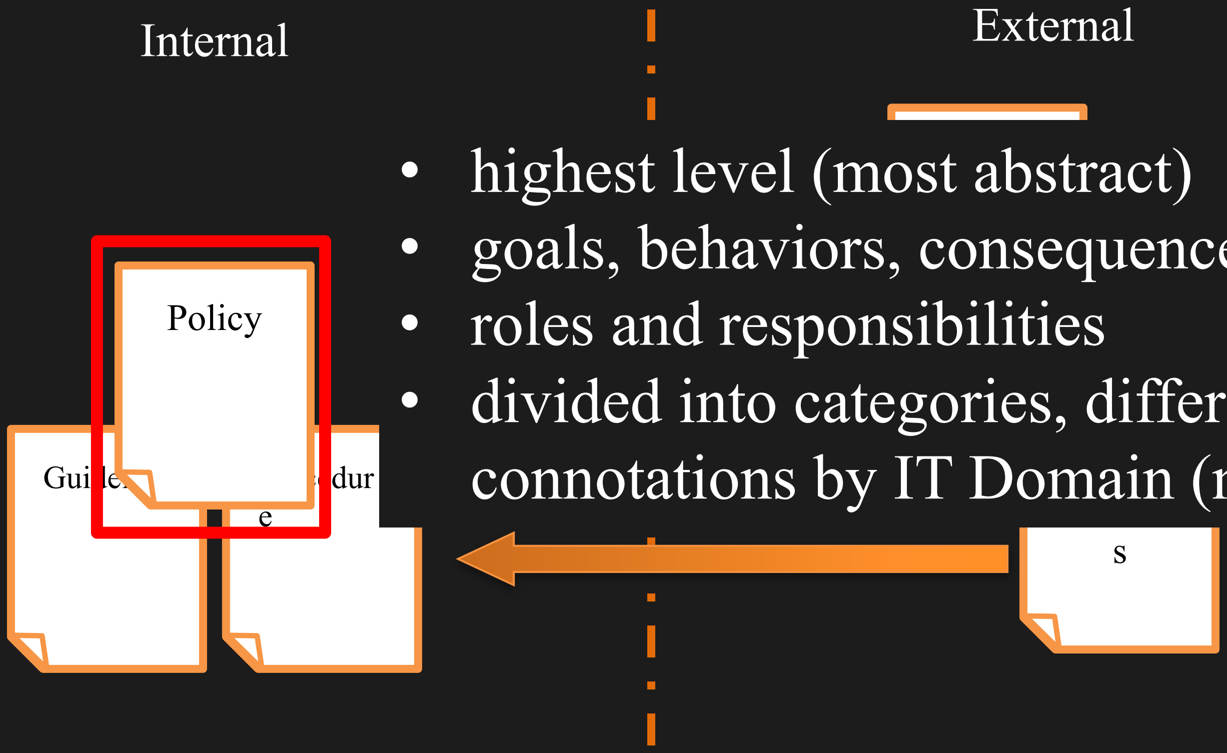
Policy

Guideline

Procedur
e

High Level Policy Wrap up

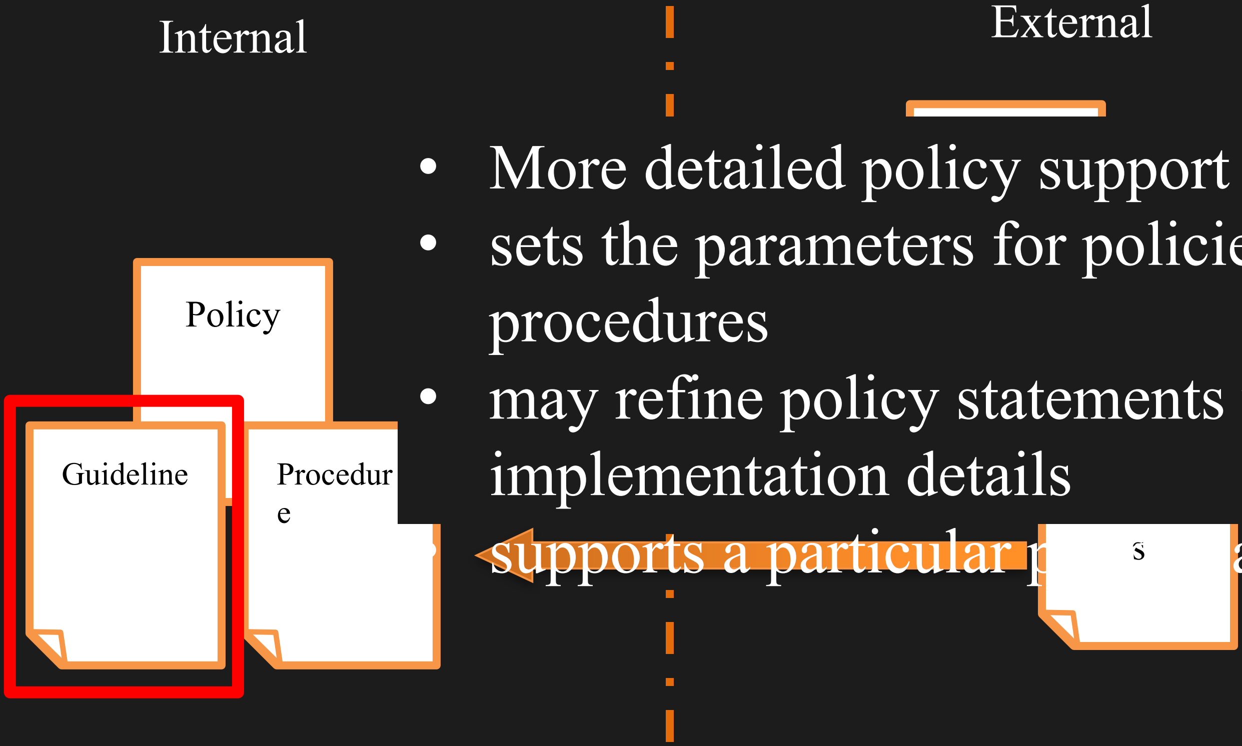
Different types of policy documents



- highest level (most abstract)
- goals, behaviors, consequences
- roles and responsibilities
- divided into categories, different connotations by IT Domain (next)

High Level Policy Wrap up

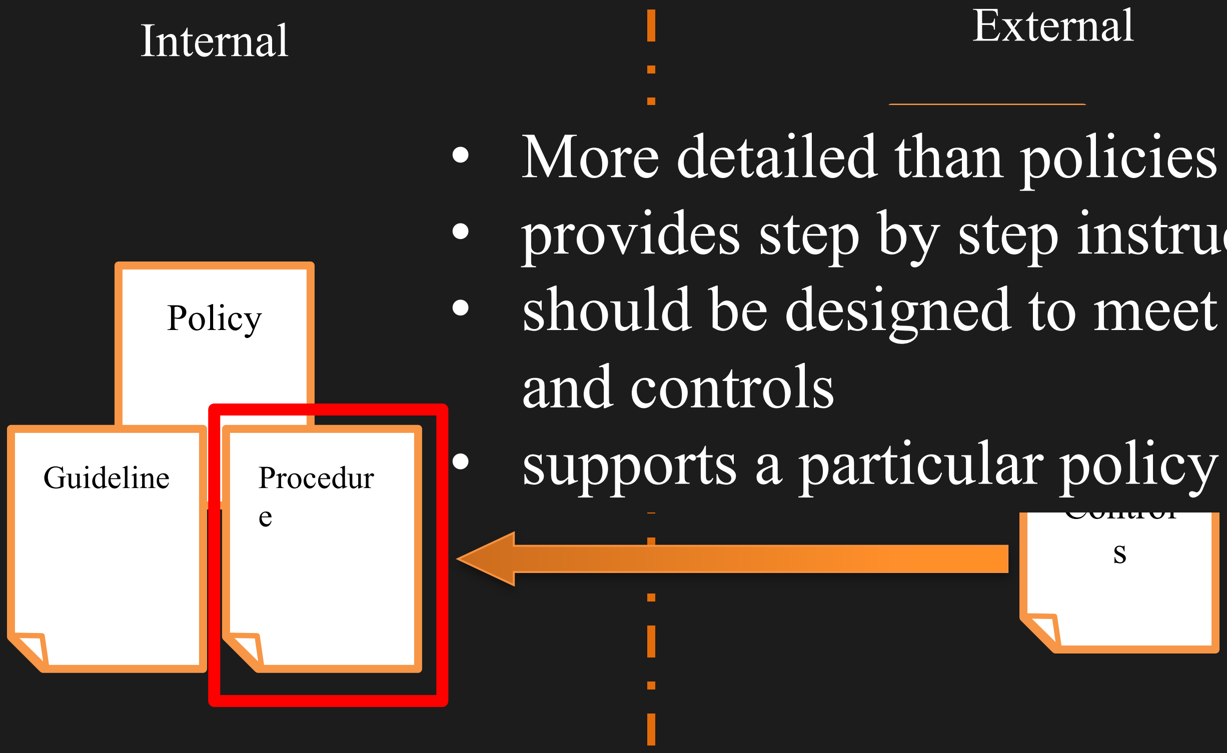
Different types of policy documents



- More detailed policy support document
- sets the parameters for policies or procedures
- may refine policy statements with implementation details
- supports a particular p ategory

High Level Policy Wrap up

Different types of policy documents

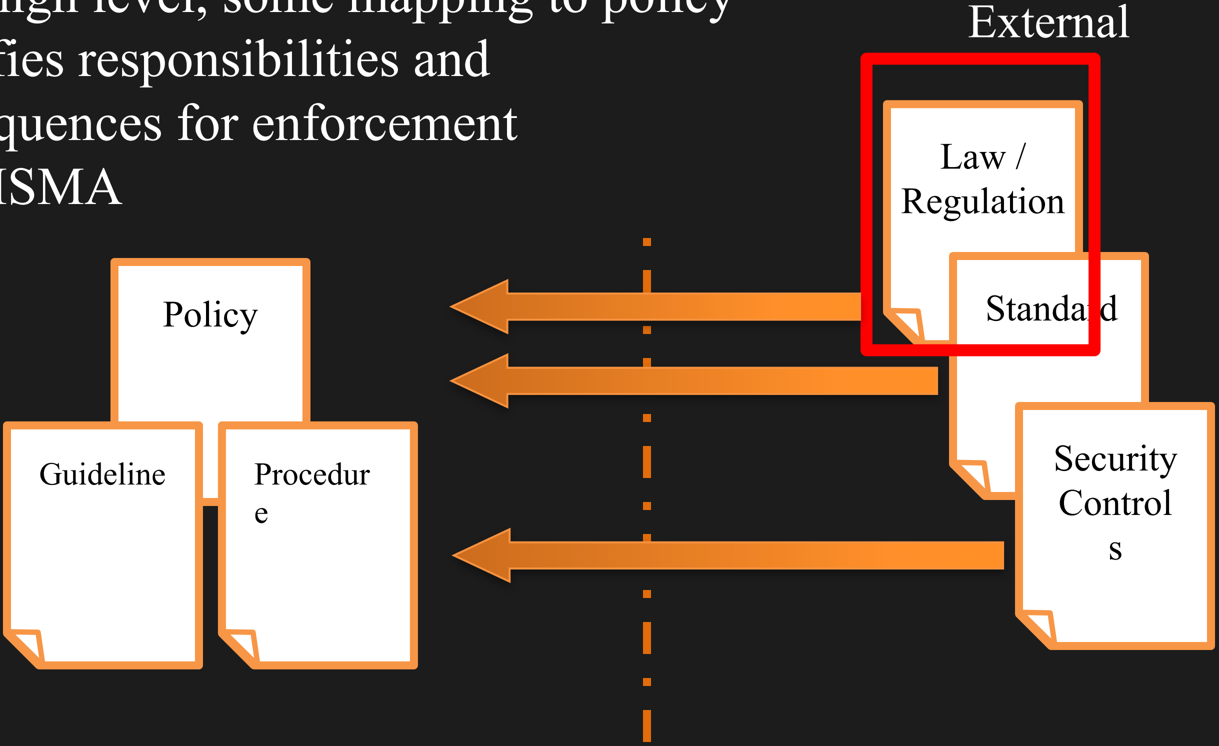


- More detailed than policies
- provides step by step instructions
- should be designed to meet guidelines and controls
- supports a particular policy category

High Level Policy Wrap up

Different types of policy documents

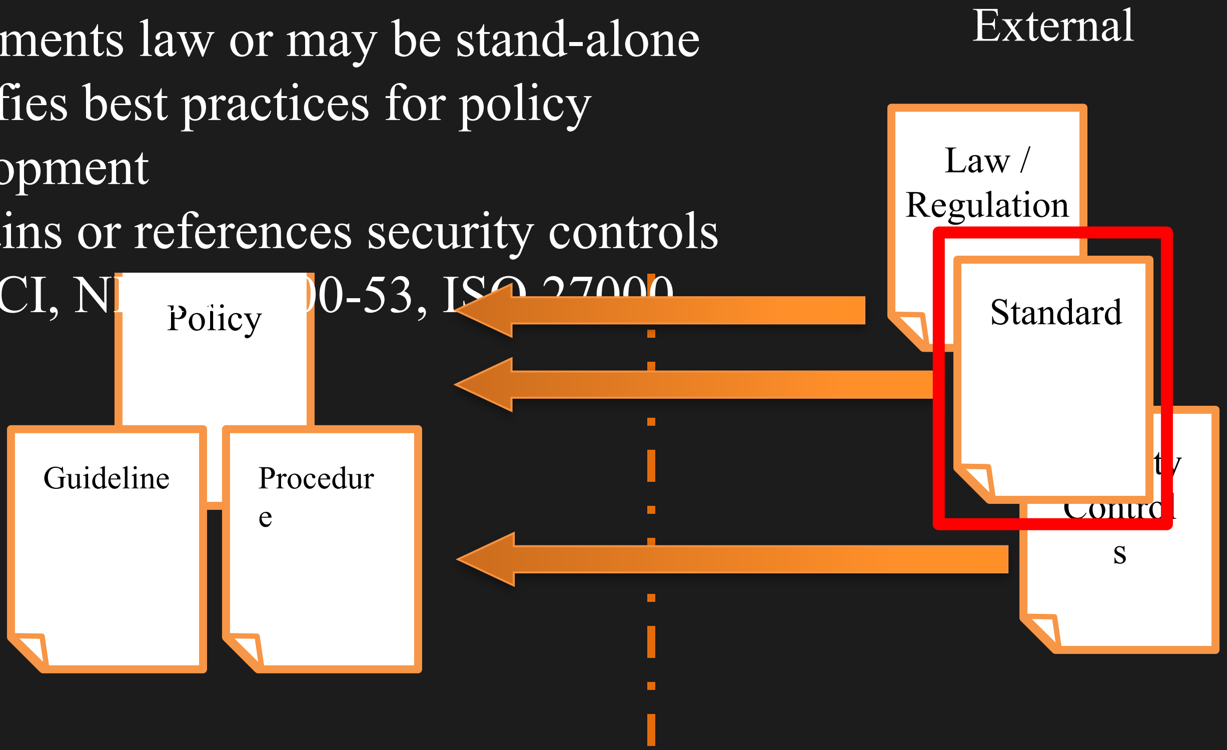
- Very high level, some mapping to policy
- Specifies responsibilities and consequences for enforcement
- e.g. FISMA



High Level Policy Wrap up

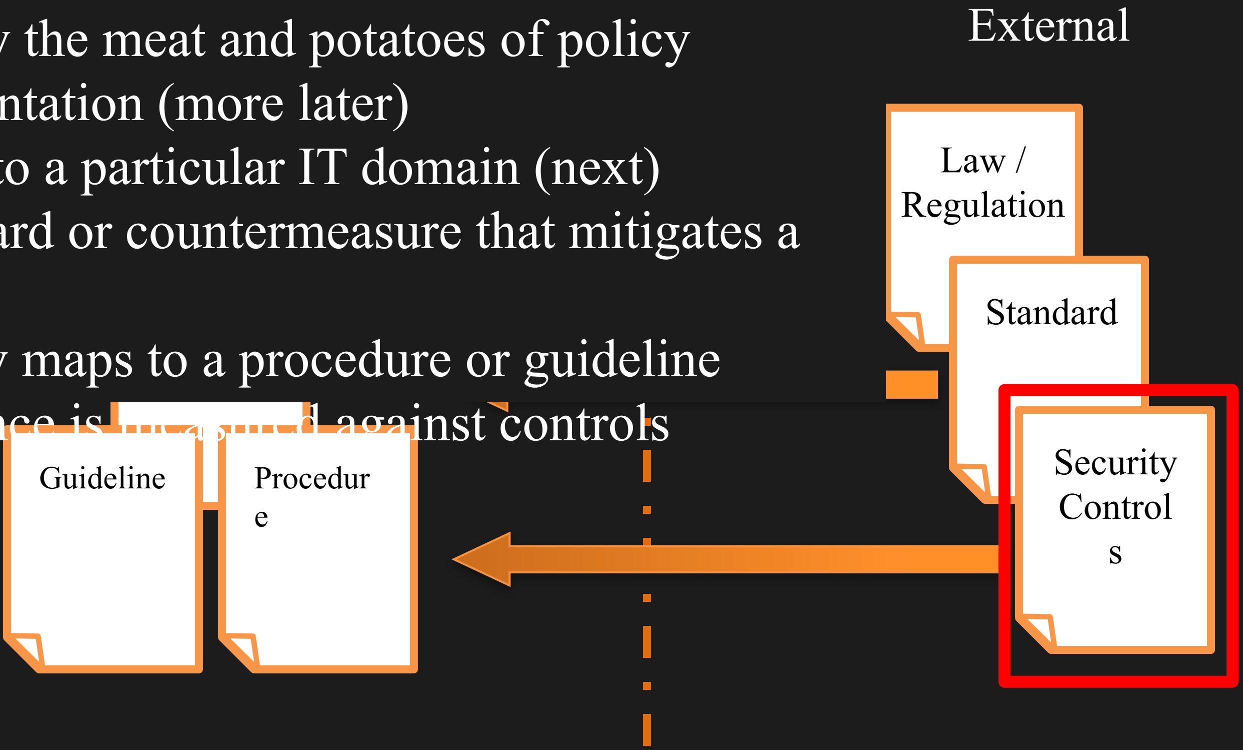
Different types of policy documents

- Implements law or may be stand-alone
- Specifies best practices for policy development
- Contains or references security controls
- e.g. PCI, NI 00-53, ISO 27000



Different types of policy documents

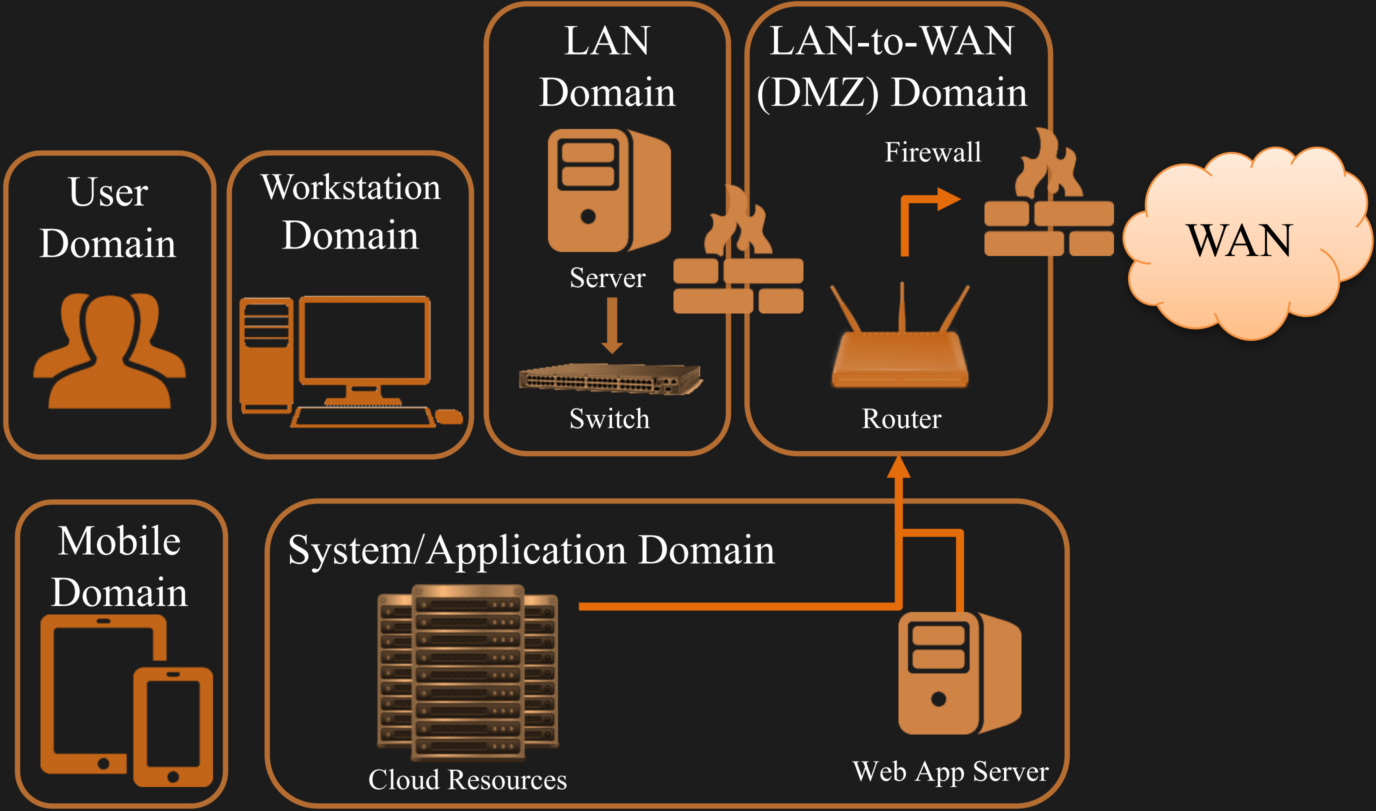
- Typically the meat and potatoes of policy implementation (more later)
- Applies to a particular IT domain (next)
- a safeguard or countermeasure that mitigates a risk
- generally maps to a procedure or guideline
- compliance is measured against controls



High Level Policy Wrap up

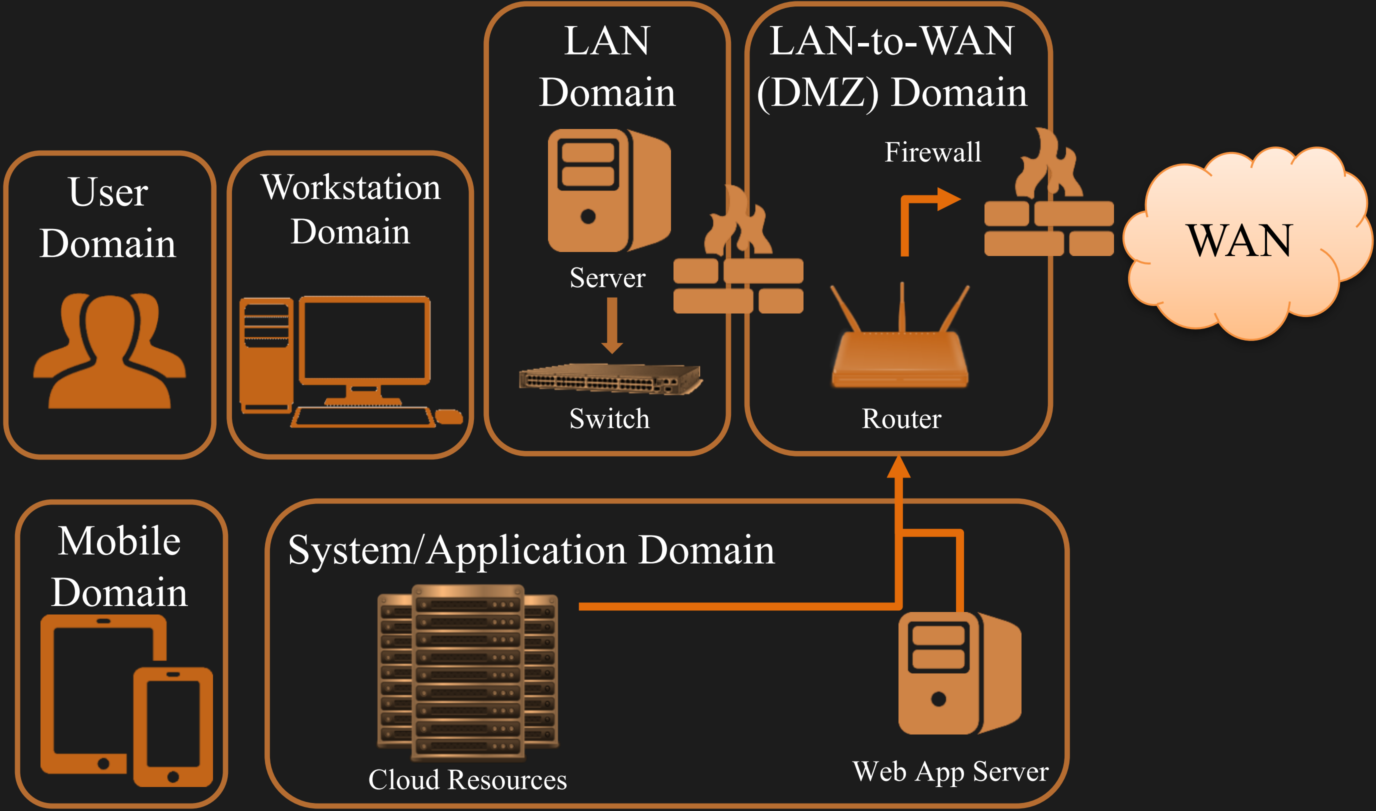
IT Domains

- IT covers a range of assets
- controls and policies typically apply categorically to different domains



High Level Policy Wrap up

IT Domains



Policies, procedures, guidelines, and controls should be applied appropriately by domain

High Level Policy Wrap up

Policy Challenges with each domain

User Domain

Challenge	Mitigation
Ensuring Employees know about policy	Training
Getting employees to comply with policy	enforcement, rewards
Not impeding work / productivity	Good policy design

High Level Policy Wrap up

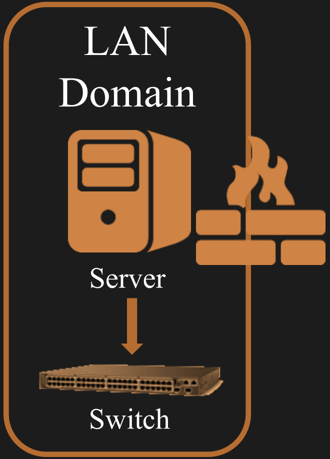
Policy Challenges with each domain

Workstation Domain

Challenge	Mitigation
Preventing security breaches	Technical security controls
Not being draconian	Not being draconian
Maintaining privacy while ensuring correct use of resources	Use of windows policies, limit access, secure logging

High Level Policy Wrap up

Policy Challenges with each domain



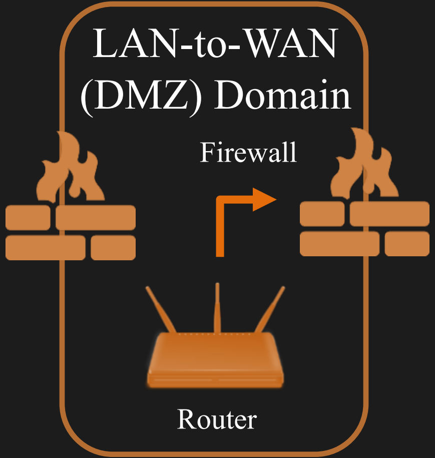
LAN Domain

Server

Switch

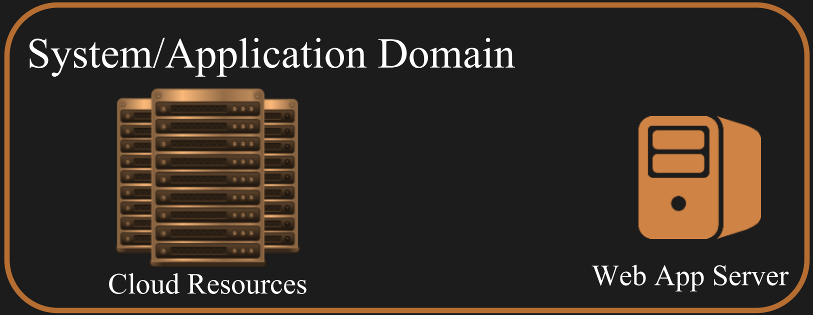
Challenge	Mitigation
Availability of the network	Acceptable use policy
Integrity and confidentiality of data	Technical security controls, use of segmented network

Policy Challenges with each domain



Challenge	Mitigation
Securing the DMZ	Technical security controls, configuration testing, monitoring and audit
Adapting to threats	Monitoring and audit, incident response

Policy Challenges with each domain



Challenge	Mitigation
Preventing data breaches	Data loss protection security controls - perimeter monitoring of data in motion, inventory of data at rest, encryption of data outside of secure space
Reducing or limiting vulnerabilities	Baking security into the SDLC, failsafes, incident response, risk management

High Level Policy Wrap up

Policy Challenges with each domain

Mobile Domain

Challenge	Mitigation
Securing data	Personally owned device policy, data management protocols
Secure remote access	VPN usage, authentication, access control

High Level Policy Wrap up

Policy Challenges with each domain

WAN

Challenge	Mitigation
Reliability	Service level agreement with ISP
Speed	Service level agreement with ISP
Third party web/cloud application/data security	Service level agreements with web/cloud service provider

Time for compliance!

Intro to compliance

Time for compliance!

Definition:

Compliance is *adhering to* [stuff].

Time for compliance!

Definition:

[stuff] => Laws | Regulations | Standards | Internal Policy

Time for compliance!

Standards offers preferential treatment or added value to compliant organizations.

Time for compliance!

Laws and regulations mandate compliance and levy external penalties (usually money) for non-compliance.

Time for compliance!

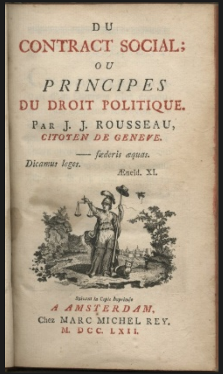
Internal policy offers yourself the things you've decided are best. Not following them is cognitive dissonance.

US Compliance Laws

Despite what you think of congress, laws *ideally* codify the good

Motivations for Law

- Three main drivers
  - Consumer Protection, Civil Rights
  - Economic Stability
  - Social Contract (order)
- Drivers usually linked
- Tend to focus more on economics than others



DU

CONTRACT SOCIAL;

OU

PRINCIPES

DU DROIT POLITIQUE.

PAR J. J. ROUSSEAU,

CITOYEN DE GENEVE.

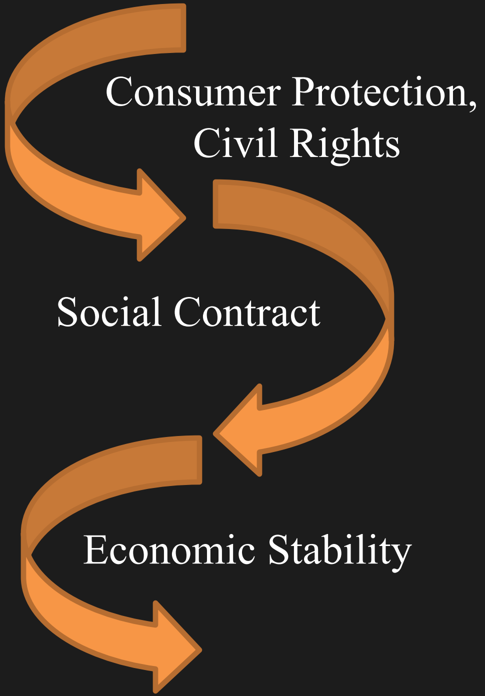
— fœderis æquas
Dicamus leges.
Æneid. XI.

Suivant la Copie imprimée

A AMSTERDAM,

Chez MARC MICHEL REY.

M. DCC. LXII.



Consumer Protection,
Civil Rights

Social Contract

Economic Stability

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

US Info. Sec. Laws

(or if you are following along later)

http://lmgtfy.com/?q=fisma+filetype%3Apdf

http://lmgtfy.com/?q=hipaa+filetype%3Apdf

http://lmgtfy.com/?q=gramm+leach+bliley+filetype%3Apdf

Intro to compliance

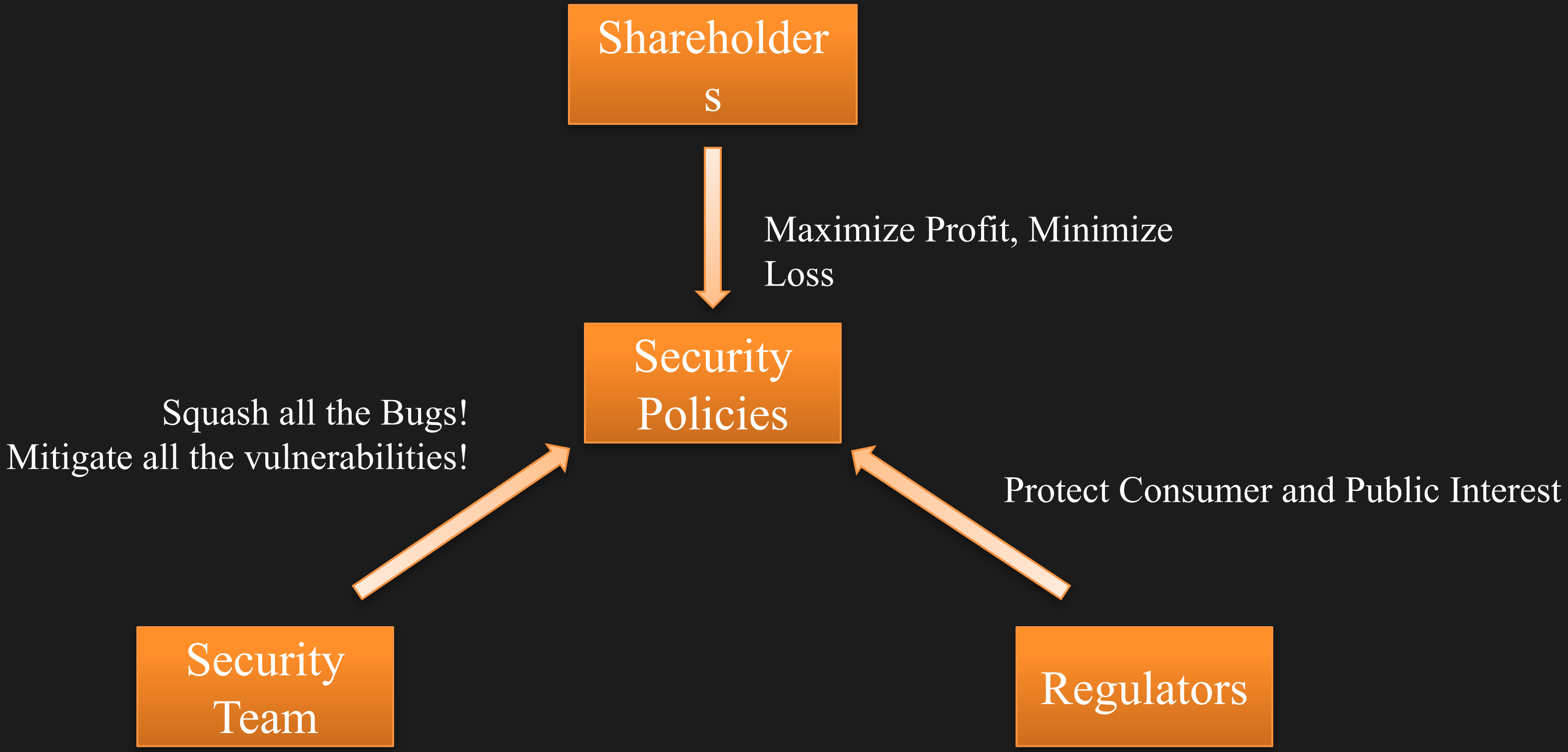
(some) U.S. Info. Sec. Industry Standards

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

US Info. Sec. Laws

…you get the idea
(hint: go look them up)

Context: Competing Goals


Shareholder
s
Maximize Profit, Minimize
Loss
Security
Policies
Squash all the Bugs!
Mitigate all the vulnerabilities!
Protect Consumer and Public Interest
Security
Team
Regulators

Good when goals align..

I promised..

Determine Compliance Requirements

Determine Compliance Requirements

First identify laws that you need to comply with.

Determine Compliance Requirements

Next identify industry regulations you want to comply with.

Determine Compliance Requirements

Both of these identifications should be integrated into an organizational risk assessment.

Determine Compliance Requirements

Now examine and integrate security controls suggested/required by the selected laws/standards.*

Determine Compliance Requirements

*This is a big task

…so big we should probably stop here

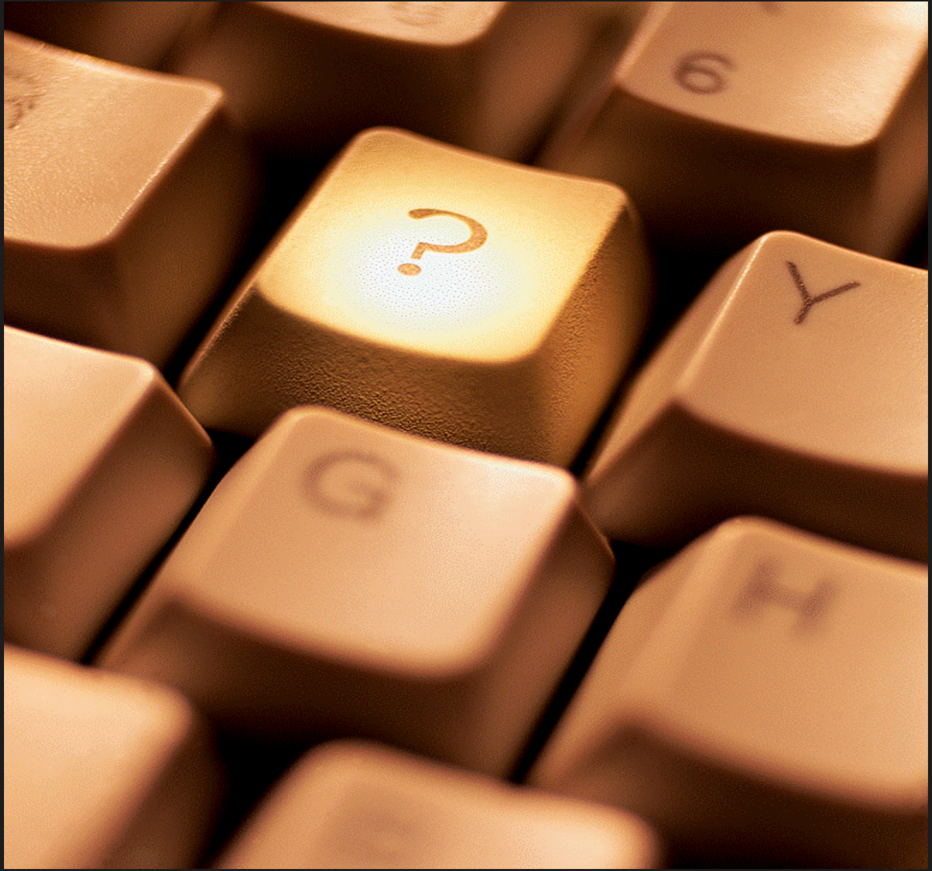
Reading

Brotby 3 and 7

Next Time

Continue this lecture

Questions?



Matt Hale, PhD

University of Nebraska at Omaha

Assistant Professor of Cybersecurity

mlhale@unomaha.edu

Twitter: @mlhale_