High Level Policy

Dr. Hale

University of Nebraska at Omaha
Information Security and Policy– Lecture 4

Today’s topics:

Last time recap

High Level Policies

- Definition & Motivation
- Documents Overview
- Development Process and Lifecycle

Writing Policy

- Step by Step Process
- Style guide
- Defining Terms
- Roles and Responsibilities
- Defining Metrics
- Examples

PREVIOUSLY ON

GAME OF TA3600

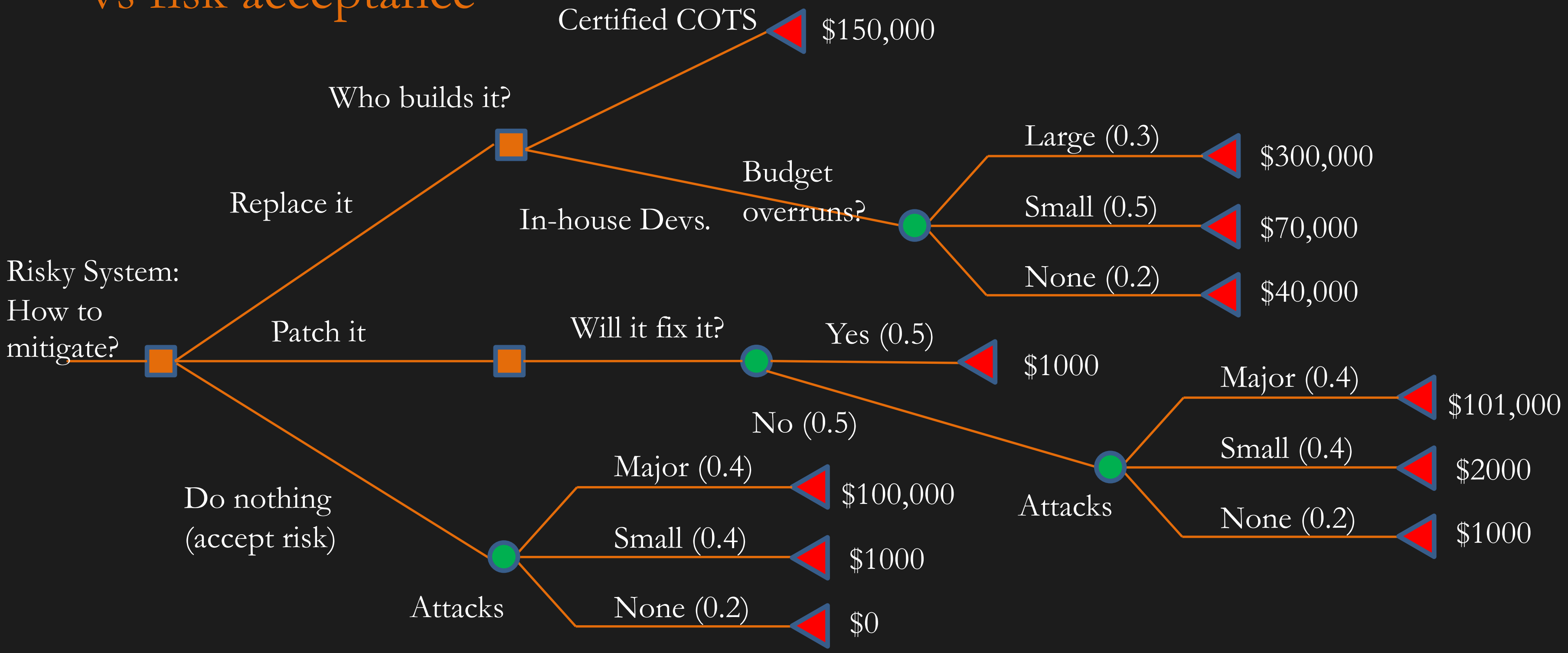
Recap

$$\mathrm{ATLE}_{\mathrm{threat}} = \mathrm{L}_{\mathrm{rate}} \text{ x } ETI_{threat}$$

Recap

=> Decision Trees

Ex. Security spending vs risk acceptance



Recap

=> Strategic Thinking

The goal was to understand what we have, what our options are for protecting what we have, and how we can maximize $ & minimize loss.

Recap

Add some salt and pepper and that is what a policy is.

ok… maybe lots of salt and pepper…

"Those of us in security are very much like heart doctors — cardiologists. Our patients know that lack of exercise, too much dietary fat, and smoking are all bad for them. But they will continue to smoke, and eat fried foods, and practice being couch potatoes until they have their infarction. Then they want a magic pill to make them better all at once, without the effort. And by the way, they claim loudly that their condition really isn't their fault — it was genetics, or the tobacco companies, or McDonalds that was to blame. And they blame us for not taking better care of them.

– Gene Spafford, at the 23rd National Information Systems Security Conference

High Level Policy

Think of an Info. Sec. Policy as a healthy living plan.

High Level Policy

Cardiologist
/ Nutritionist

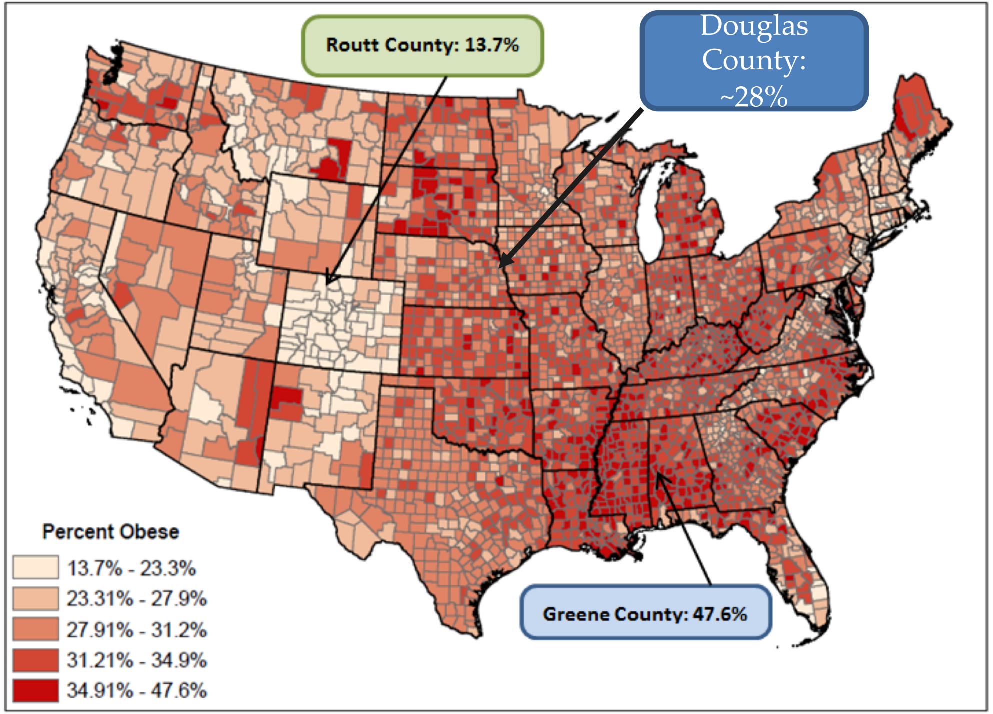
CISO:

HECKING:
Username = marc
Password = passu

STOCKS:
Userna arc
Pa = password

High Level Policy

Obese Population by County 2012



Routt County: 13.7%

Douglas County: ~28%

Greene County: 47.6%

Source: County Health Rankings (2012), Stratasan (2012)

Analogy Fact:

Few people actually listen to cardiologists

High Level Policy

The challenge is obviously to get people to actually follow policy.
(more later)

Definition

Information Security Policies are written rules that define the acceptable and unacceptable states that organizational assets can take on.

Definition: addendum

Organizational assets can range from data, to virtual systems, to physical systems, to personnel…to brooms.

Policies are technology neutral, define goals, responsibilities and *consequences* upon violation.

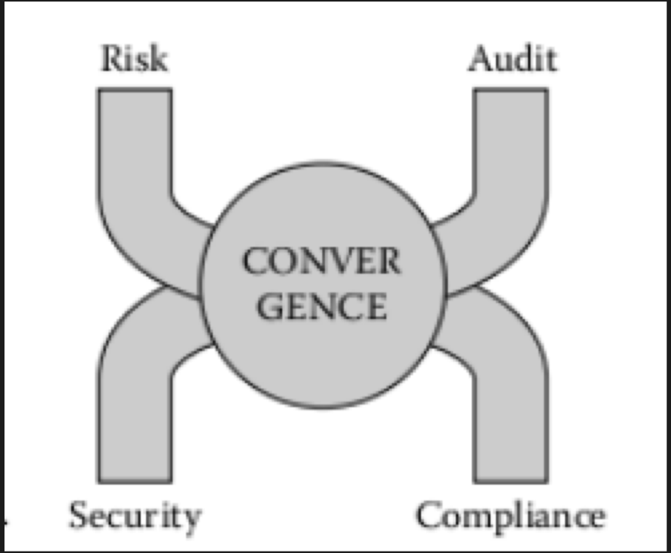
High Level Policy

Why do we need policy?

- Define acceptable use of enterprise assets
- Codify strategic directions and goals
- Ensure consistency in protection efforts across the enterprise
- Requirements point of reference for third parties (e.g., web services)
- Cover your ASSets (C.Y.A.)
    - Legal
    - Ethical
    - Compliance (will be a topic all its own)

High Level Policy

Good policies should be at the center of risk assessment / management, security planning, auditing, and compliance processes.



High Level Policy

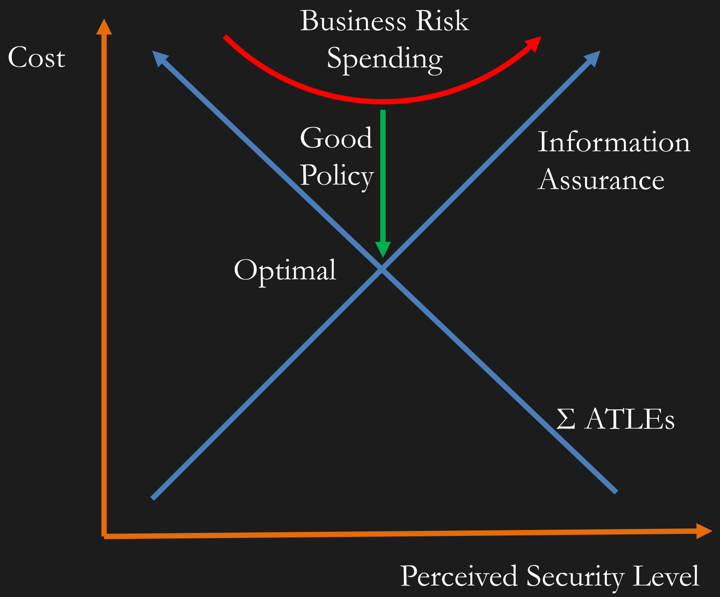
Layered Architecture of Policy

Type of Document	Description
Policy	A high level statement for goals, behaviors, and consequences. Somewhat abstract, but measurable and un-ambiguous
Guidelines	Provide additional directives to ground policy documents. Fill in technology details and/or outline implementations.
Security Control Standards (optional)	External constraints that must govern organizational systems to be certified by the standardizer (e.g. NIST, PCI)
Workflows / Processes / Procedures	Step-by-step instructions designed to meet controls, guidelines and policies.

High Level Policy

Attributes of "good" policies

1. Realistic (Can be implemented).
2. Balances flexibility with rigidity
3. Proper scoping
   - In both terms of coverage and level of detail
4. Provides at or near optimal business strategy



High Level Policy

So how do I form good polices?...

…Start with “Know thyself” and “thine enemy” (risk analysis) we’ve done that

Next: understand organizational structure

- The names of business leaders and project managers
- Organizational structure chart (if one exists)
- List of Current, Pending, and legacy projects
- Copies of any existing policies or strategic business plans

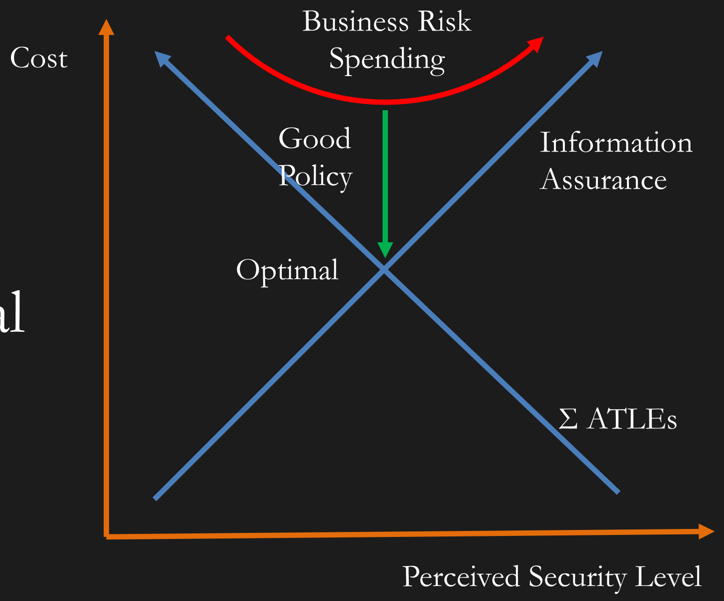
Next Communication:

Open discussion with leaders about amount of $ for policy implementation, staff training, and audit/monitoring

High Level Policy

Communication (con't):

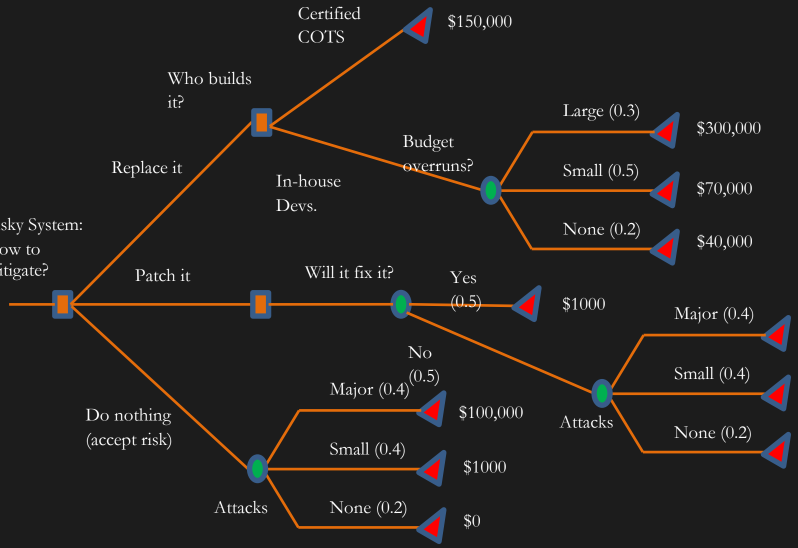
Come prepared with a graph that looks like this. Back it up with actual company data and risk assessment information.



High Level Policy

Communication (con’t):

Present strategic options for leadership decision making. Make sure your model includes as many relevant factors as possible.



Communication Tips

- Know your audience.
  - Don’t speak super technically if your audience isn’t versed in IT/Security/CS
- Identify relevant people in the organization to form alliances with
  - you will need support for good policy since it usually comes at the cost of the status quo
- Don’t be controlling or dictating
- Check your ego at the door and don’t be condescending

Communication Tips

- Be prepared to discuss differences between making new policies vs modifying existing policies (if an organization has them)
    - sometimes new is better, other times modifying existing is good too
    - don’t be too attached to one or the other

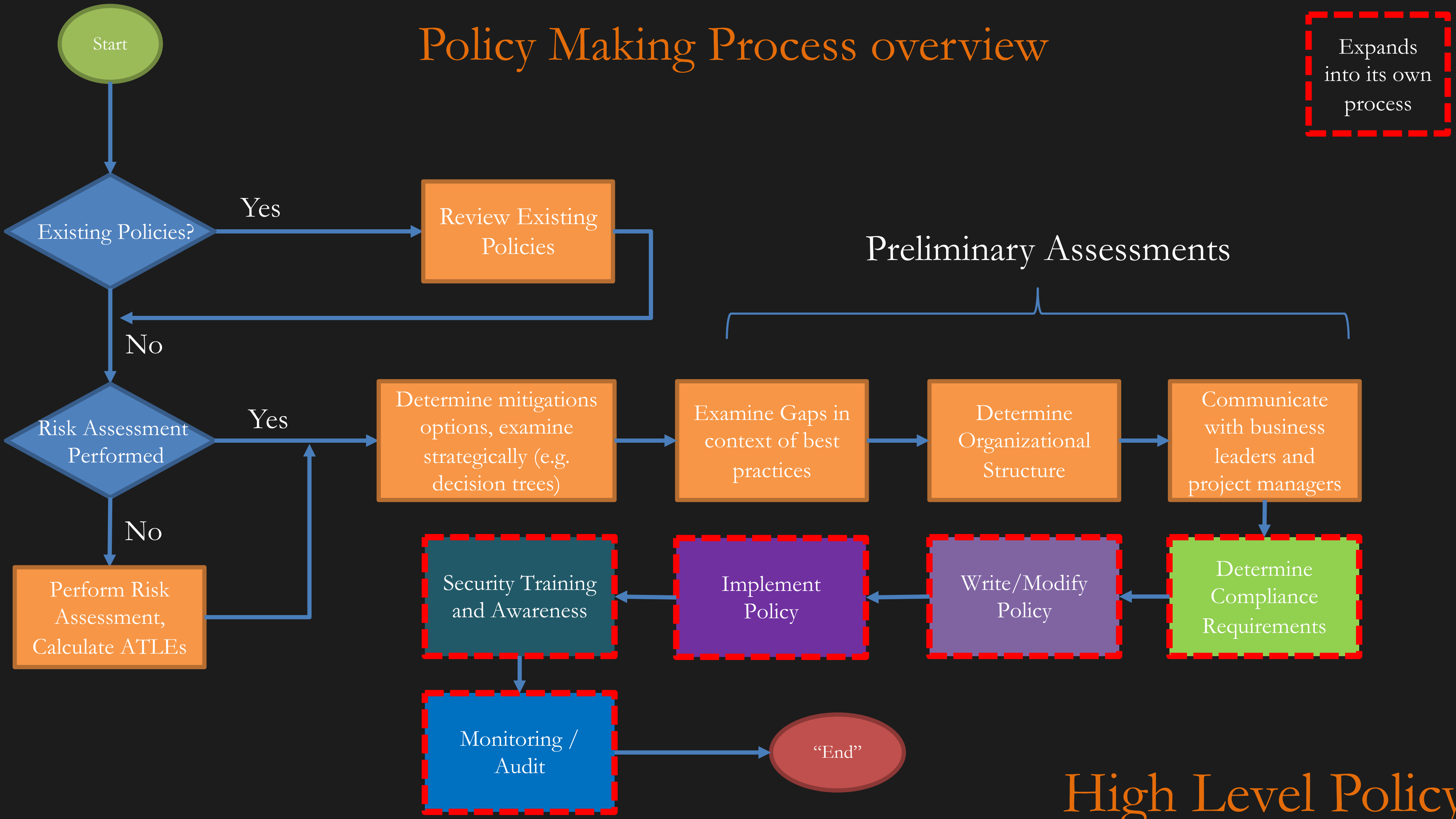
Next Discuss regulatory requirements

All policies you make MUST comply with any external regulatory requirements or they are BAD.

(we will return to this, its several lectures on its own)

High Level Policy

Policy Making Process overview



Start
Existing Policies?
Yes
Review Existing Policies
No
Preliminary Assessments
Risk Assessment Performed
Yes
Determine mitigations options, examine strategically (e.g. decision trees)
Examine Gaps in context of best practices
Determine Organizational Structure
Communicate with business leaders and project managers
No
Perform Risk Assessment, Calculate ATLEs
Security Training and Awareness
Implement Policy
Write/Modify Policy
Determine Compliance Requirements
Monitoring / Audit
"End"
Expands into its own process

High Level Policy

Will return in later lectures

Determine Compliance Requirements

Implement Policy

Security Training and Awareness

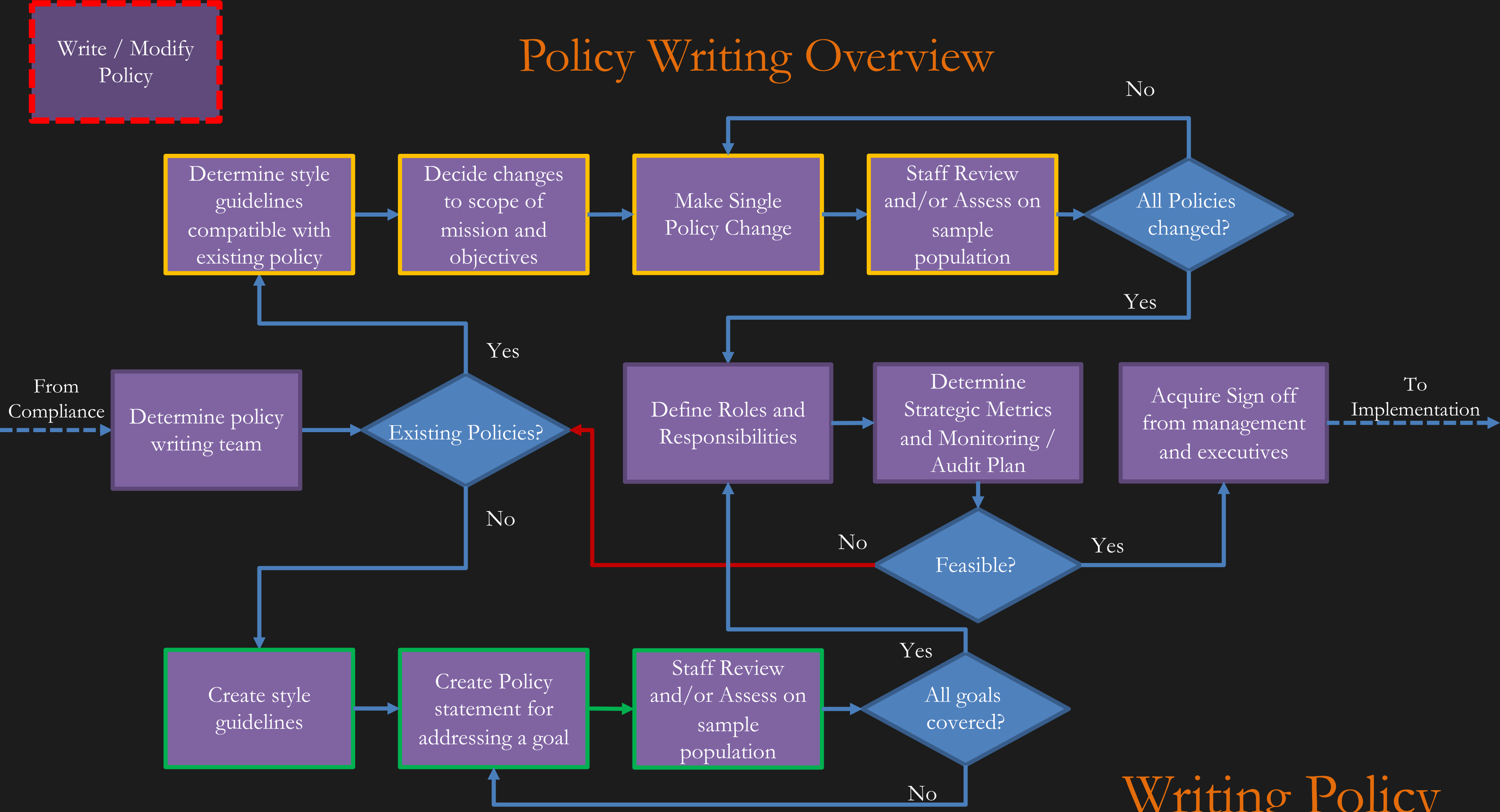
Monitoring / Audit

High Level Policy

Todays focus

Write/Modify Policy

Policy Writing Overview


Write / Modify Policy
From Compliance
Determine policy writing team
Existing Policies?
Yes
No
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
Define Roles and Responsibilities
Determine Strategic Metrics and Monitoring / Audit Plan
Acquire Sign off from management and executives
To Implementation
Feasible?
No
Yes
Create style guidelines
Create Policy statement for addressing a goal
Staff Review and/or Assess on sample population
All goals covered?
Yes
No

Writing Policy

Step 1: Form a team

Policies aren’t written by 1 person.

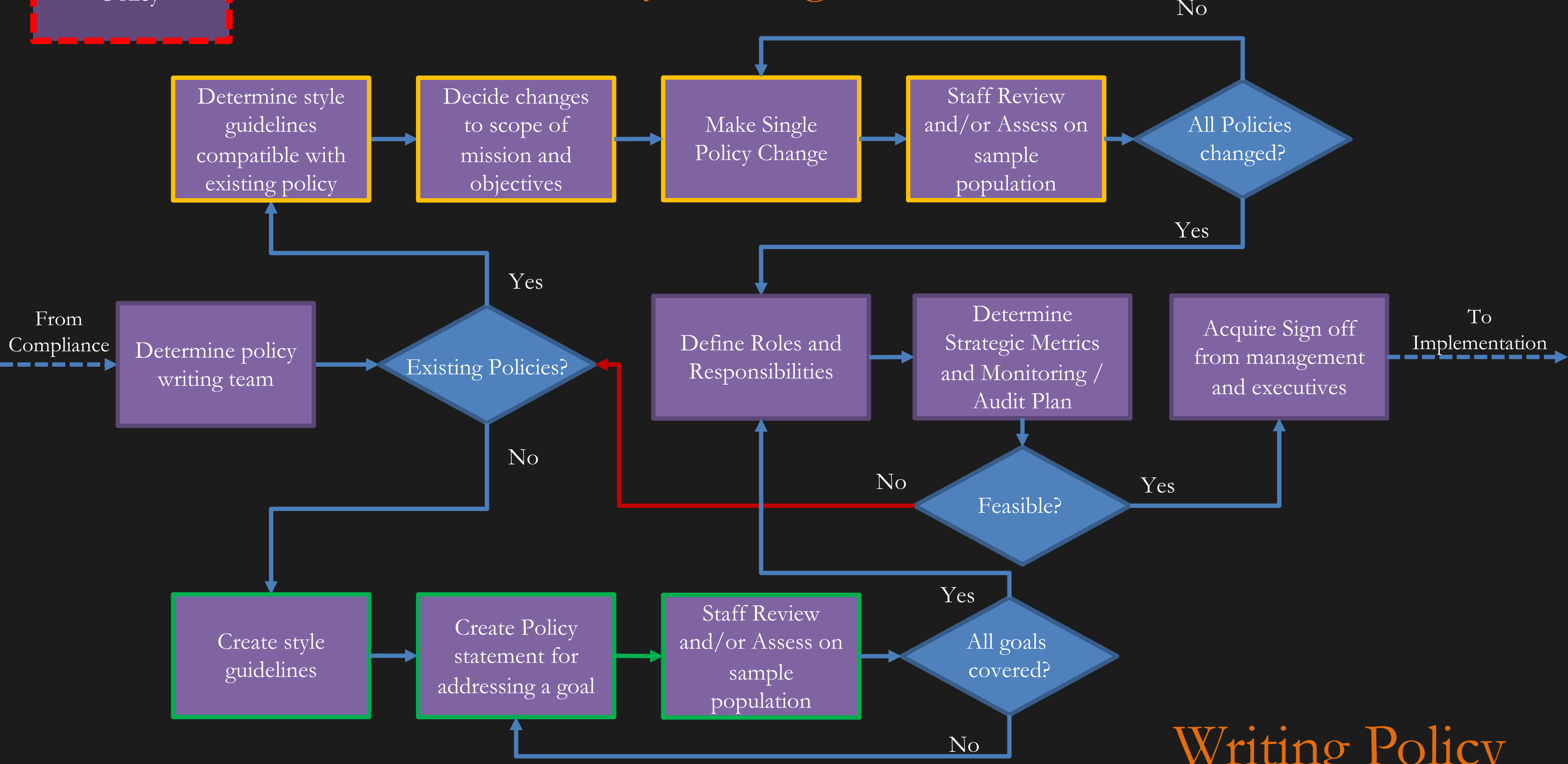
Multiple stakeholders at different levels of the organization need to be involved.

Step 1: Form a team (a good start)

- Senior Network Administrator
- Management representative
  - bonus if they will be involved in enforcement
- Legal representative (lawyer)
- Internal audit team member
- Project manager(s)
- Workforce representative (internal senate, union rep, or just employees)
- Writer (preferably a technical writer)

Policy Writing Overview

Write / Modify Policy



No
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?
Yes
Yes
From Compliance
Determine policy writing team
Existing Policies?
Define Roles and Responsibilities
Determine Strategic Metrics and Monitoring / Audit Plan
Acquire Sign off from management and executives
To Implementation
No
No
Feasible?
Yes
Yes
Create style guidelines
Create Policy statement for addressing a goal
Staff Review and/or Assess on sample population
All goals covered?
No

Writing Policy

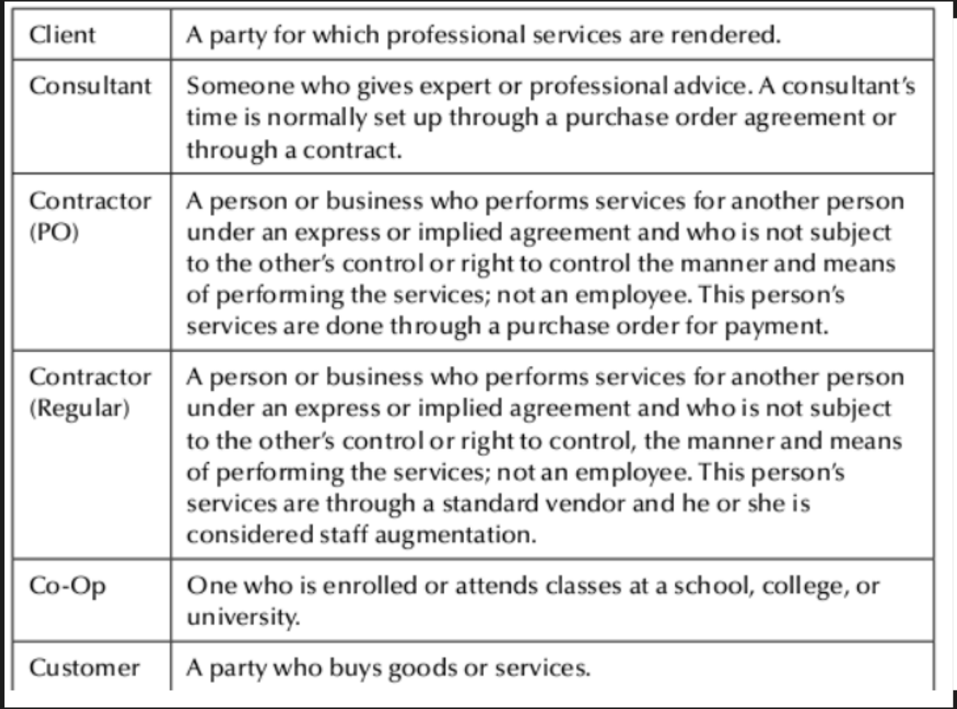
Step 2a and 2b: Setup style guidelines

1. Determine how you will encode the policy
   - Could be an HTML document
   - Could be a plaintext doc or pdf (usually)
   - Could be an XML document
2. Specify a singular vernacular to work from, define standard terms
   - i.e. define legalese (what is the meaning of "is")
3. If you are modifying existing policy, check to ensure compatibility. The end result should be a single cohesive policy style, not piecemeal.

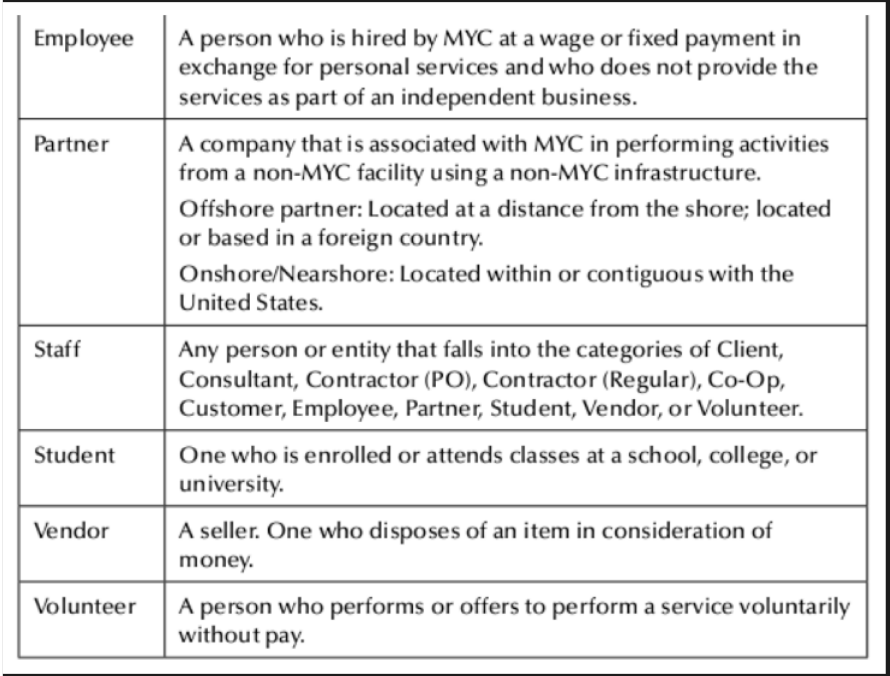
Example: Style Guide

- Font and tone
- Signature sheet style
  - for doc approval
  - for staff acknowledgement
- Header footer information
  - title / document ID
  - dates
  - review
  - revision
- Change tracking and revision history
  - date format
  - change messages
  - storage method
- Purpose scope
  - glossary of standard terms
  - acronyms
  - supporting details
  - references to other documents
  - responsibilities

Example: Defining Terms



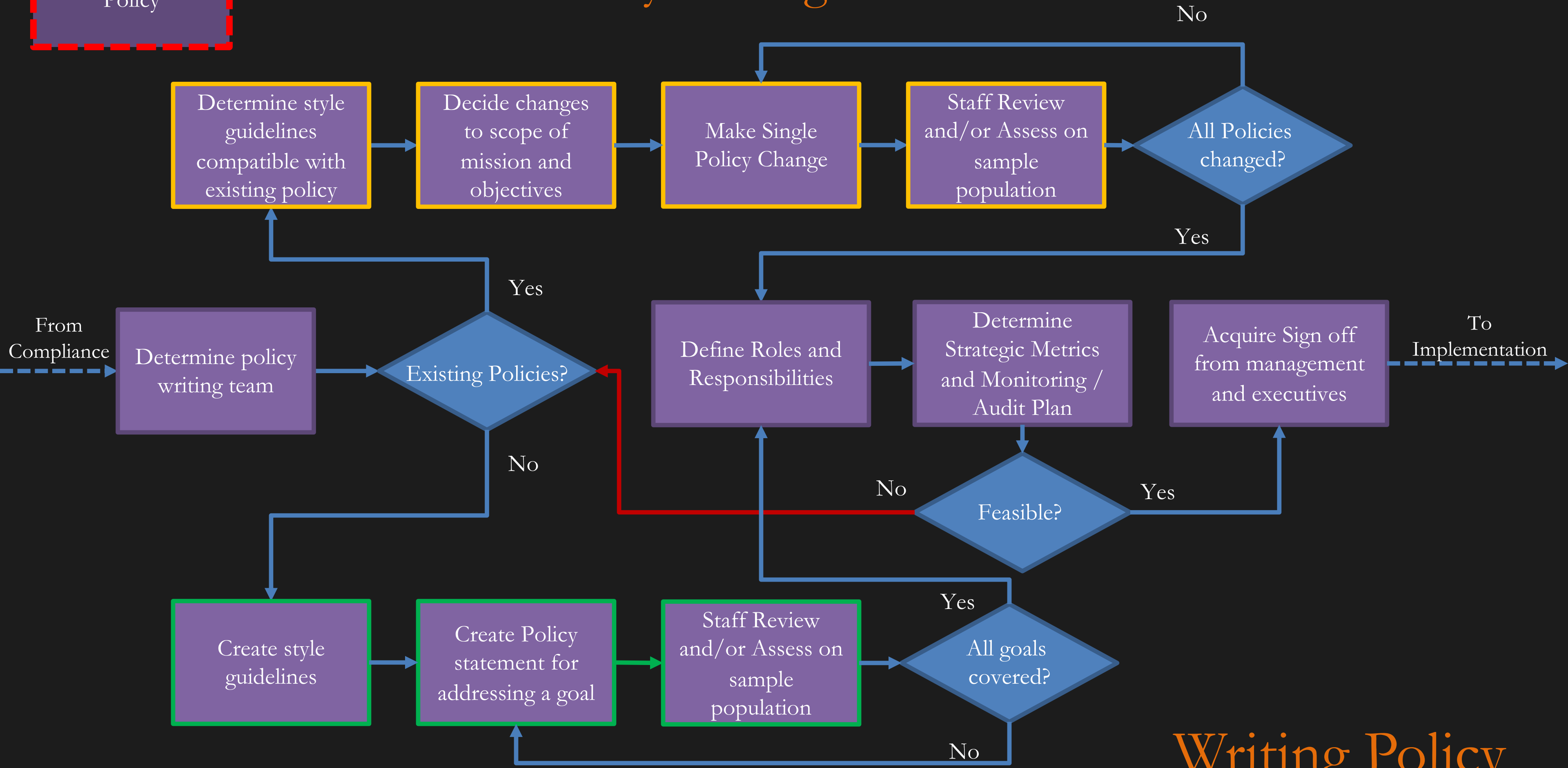
Client	A party for which professional services are rendered.
Consultant	Someone who gives expert or professional advice. A consultant's time is normally set up through a purchase order agreement or through a contract.
Contractor (PO)	A person or business who performs services for another person under an express or implied agreement and who is not subject to the other's control or right to control the manner and means of performing the services; not an employee. This person's services are done through a purchase order for payment.
Contractor (Regular)	A person or business who performs services for another person under an express or implied agreement and who is not subject to the other's control or right to control, the manner and means of performing the services; not an employee. This person's services are through a standard vendor and he or she is considered staff augmentation.
Co-Op	One who is enrolled or attends classes at a school, college, or university.
Customer	A party who buys goods or services.



Employee	A person who is hired by MYC at a wage or fixed payment in exchange for personal services and who does not provide the services as part of an independent business.
Partner	A company that is associated with MYC in performing activities from a non-MYC facility using a non-MYC infrastructure. Offshore partner: Located at a distance from the shore; located or based in a foreign country. Onshore/Nearshore: Located within or contiguous with the United States.
Staff	Any person or entity that falls into the categories of Client, Consultant, Contractor (PO), Contractor (Regular), Co-Op, Customer, Employee, Partner, Student, Vendor, or Volunteer.
Student	One who is enrolled or attends classes at a school, college, or university.
Vendor	A seller. One who disposes of an item in consideration of money.
Volunteer	A person who performs or offers to perform a service voluntarily without pay.

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

Writing Policy

Step 3a: Create policy statements

- Policy statements should have a definitive focus without being *too* specific. Be careful to scope accordingly.

Org A Password policy:

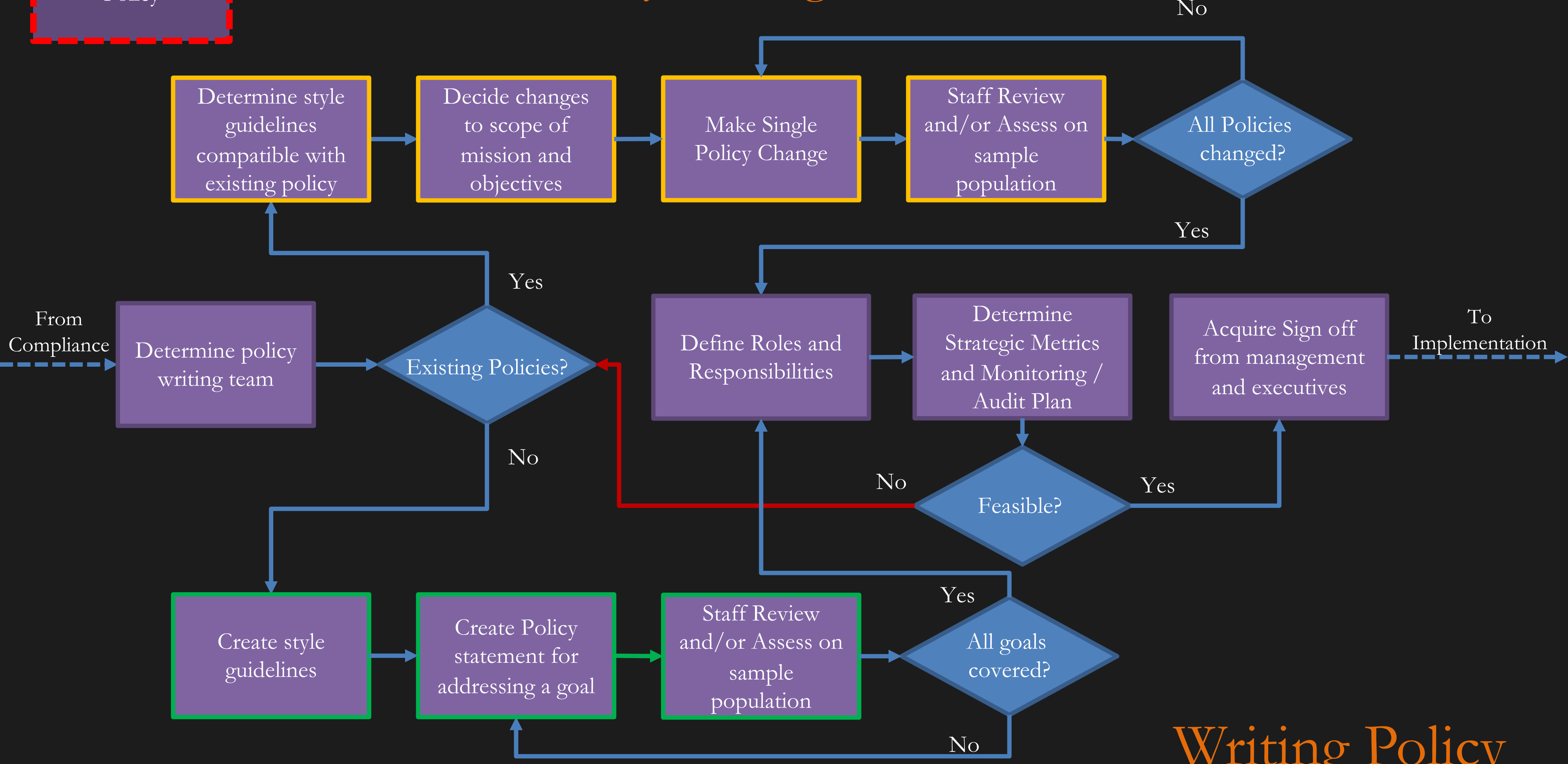
- 7-16 chars
- Must have but not start with a number
- must have two upper case letters
- must have two non consecutive numbers
- must not have more than 4 consecutive letters
- expires every 90 days
- cannot be similar to previous 12 passwords
- must contain 2 special characters

Org b Password policy:

- minimum 8 characters
- must have at least one upper case letter
- must have at least one number
- expires every 12 months
- cannot exactly reuse any of the previous 6 passwords

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

Define Roles and Responsibilities

Determine Strategic Metrics and Monitoring / Audit Plan

Feasible?

No

Yes

Acquire Sign off from management and executives

To Implementation

No

Create style guidelines

Create Policy statement for addressing a goal

Staff Review and/or Assess on sample population

All goals covered?

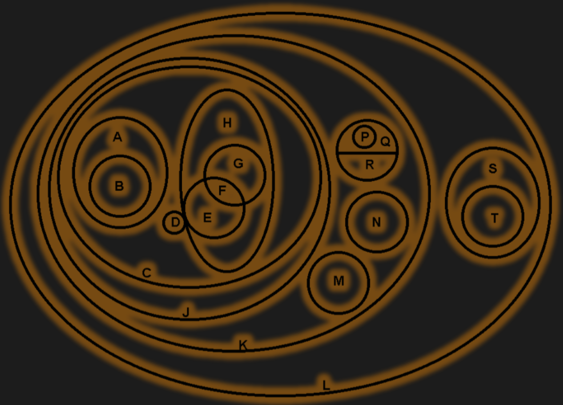
Yes

No

Writing Policy

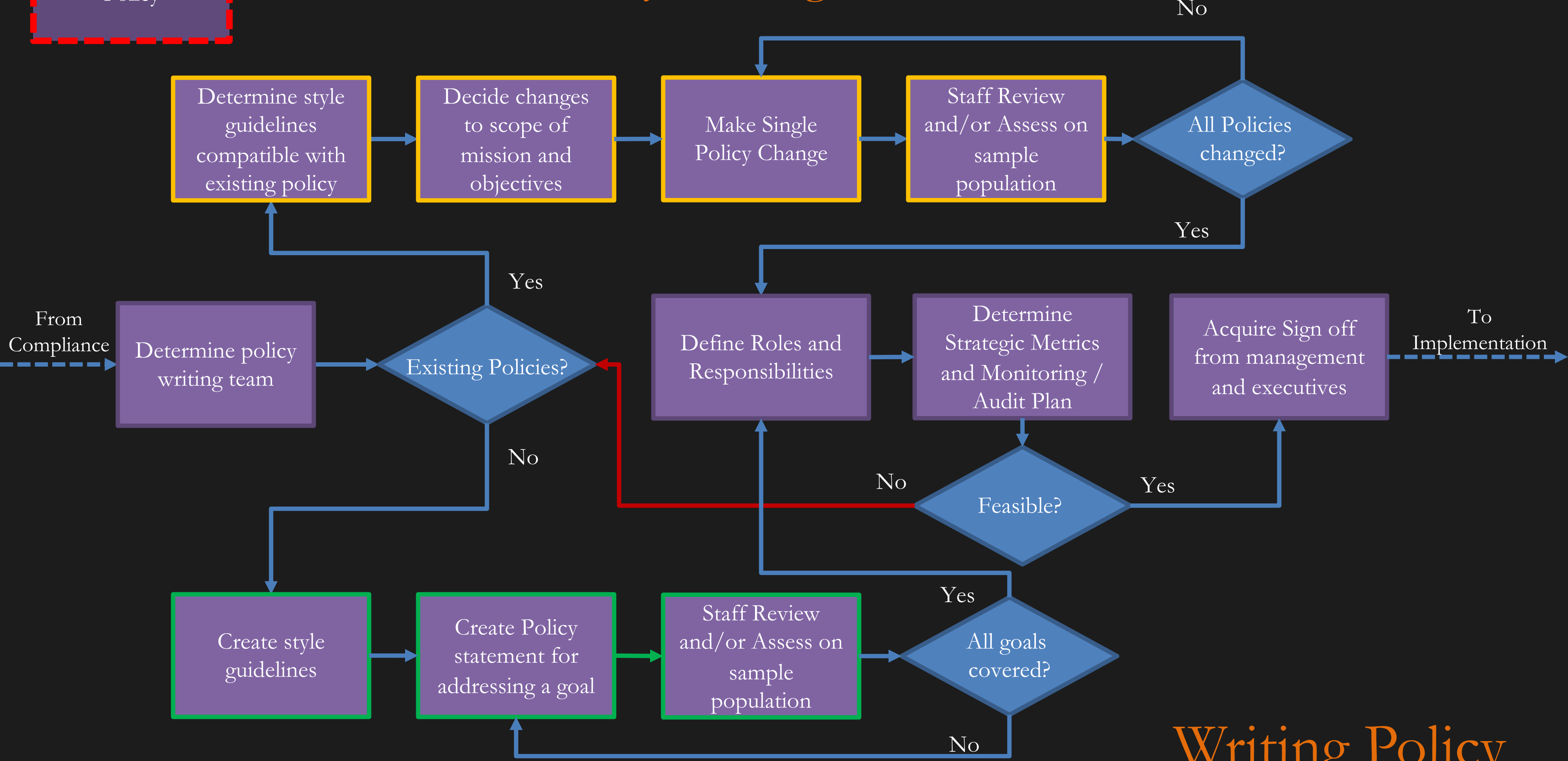
Steps 3b and 4b: Decide changes to scope of mission and objectives and make a policy change

- If you are modifying existing policy, how will the new policy statement change organizational objectives compared to the last
- Will this affect other policy areas?
- be careful to fully understand the effects of change to prevent bad situations where you change one statement and it affects another
  - Lemma: be careful to keep policies separable or at least explicitly define dependencies so you can trace them later if needed



Write / Modify Policy

Policy Writing Overview

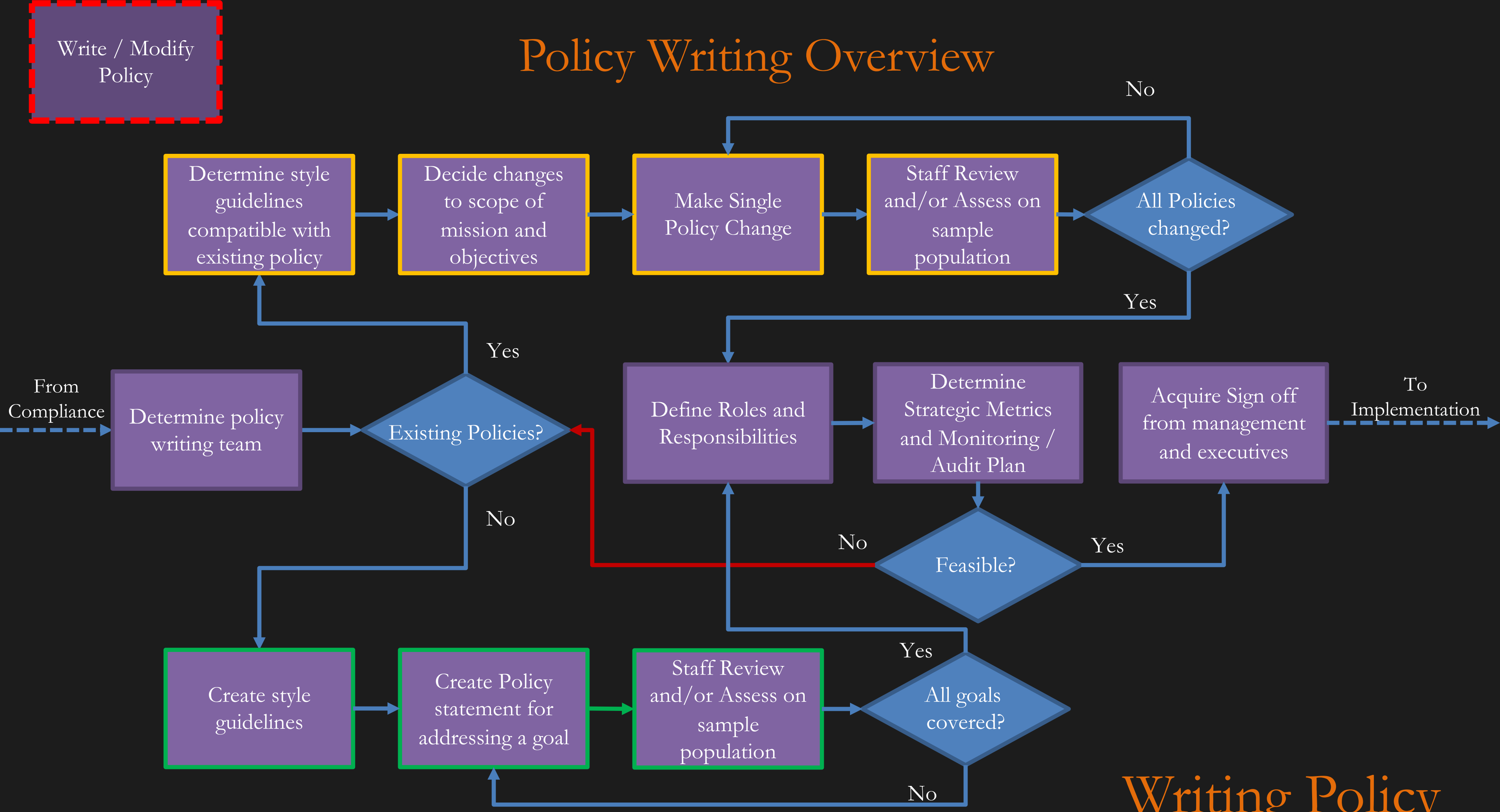

From Compliance
Determine policy writing team
Existing Policies?
Yes
Determine style guidelines compatible with existing policy
Decide changes to scope of mission and objectives
Make Single Policy Change
Staff Review and/or Assess on sample population
All Policies changed?
No
Yes
No
Create style guidelines
Create Policy statement for addressing a goal
Staff Review and/or Assess on sample population
All goals covered?
Yes
No
Define Roles and Responsibilities
Determine Strategic Metrics and Monitoring / Audit Plan
Feasible?
No
Yes
Acquire Sign off from management and executives
To Implementation

Writing Policy

Step 4a and 5b: Test out the policy

- Its important to review the policy you are making with actual users and see the effects
- This can produce insights that might otherwise be missed
- Think of it as beta testing:
  - companies beta test so that a small group of people can get mad and effect change instead of alienating the entire consumer based
- This will also help going forward when the case is presented to management.

Policy Writing Overview



Write / Modify Policy
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
Define Roles and Responsibilities
Determine Strategic Metrics and Monitoring / Audit Plan
Feasible?
No
Yes
Acquire Sign off from management and executives
To Implementation
No
Create style guidelines
Create Policy statement for addressing a goal
Staff Review and/or Assess on sample population
All goals covered?
Yes
No

Writing Policy

Shared step: Defining Roles

- Once a policy is tested, define roles and responsibilities for following, executing, and managing a policy
- Questions to ask:
    - Who will be forced to follow it? How will they be forced?
    - Who will execute it? Are there any issues with this?
        - e.g. is there one person in the basement who gets to look over email?
            - if so it's a bad policy
        - Who watches the watcher?
    - Who will ensure its followed, what are the carrots and sticks to be used?

Shared step: Strategic Metrics

- Every policy should be measureable
- Every statement should have defined metrics that signal when it is being followed/executed well and when it is not
- e.g.

Data encryption policy:

- All sensitive data involving financial, personal, and/or company/trade secrets must be protected using encryption before being placed on a network or stored on storage media

Metrics

- Total sensitive data placed on networks *minus* Total encrypted sensitive data on networks
- Total sensitive data stored on disk *minus* Total encrypted sensitive data on disk

Think of policy statements in terms of scientific method.

If statements are non-testable or non-measurable they are bad.

I won the lottery because my psychic aura made me win.

We live in the matrix

There is no freedom of choice. Everything is pre-destined

Coworkers should respect each other

All company representatives should have positive attitudes

Policy statement mistakes affecting metrics

- If you can’t determine metrics or if assessing them is untenable, there might be a problem with the scope of a policy statement or the statement itself
- this may prevent enforcement of the policy or (worse) lead to ambiguity
- e.g.

Data encryption policy:

- Sensitive data should be protected

Metrics

??

Problems

- What is ‘sensitive data’?
- What is ‘protected’?
- How do we know when its protected?

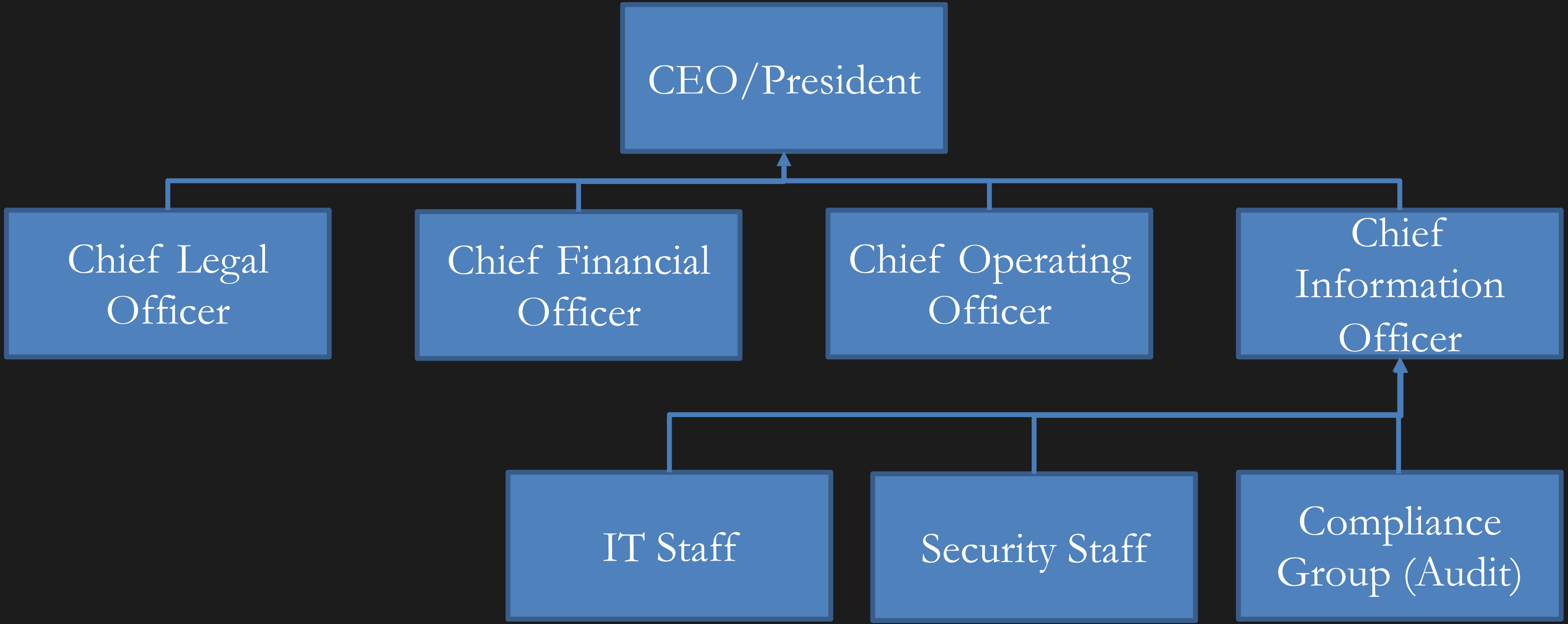
“Smart” policy is: Specific, Measurable, Agreeable, Realistic, Time-bound

Once (good) metrics are identified an auditing / monitoring plan should be developed to ensure policy compliance.

The last step is managerial signoff

Once a policy has been finalized and all of the questions have been answered the team should present the plan to management for approval.

Standard Reporting structure



Writing Policy

Example: High Level Info. Sec. Policy Categories

- Network Security
- Access Control
- Authentication
- Encryption / Key Mgmt
- Segregation of Duties
- Auditing / Logging / Monitoring / Review
- Application Security
- Physical Security
- Awareness and Training
- Incident Response
- Configuration Management
- Procurement and Contracting
- System / Project Development Lifecycle
- Document retention

Example: UNO Policies

Restricted Data Security Policy

https://www.unomaha.edu/human-resources/_documents/uno-restricted-data.pdf

Systems Access Policy

https://www.unomaha.edu/campus-policies/systems-access-control.php

Electronic Content Resources Policy

https://www.unomaha.edu/campus-policies/electronic-content-resources.php

Example: Style Guide

- Font and tone
- Signature sheet style
  - for doc approval
  - for staff acknowledgement
- Header footer information
  - title / document ID
  - dates
  - review
  - revision
- Change tracking and revision history
  - date format
  - change messages
  - storage method

- Purpose scope
  - glossary of standard terms
  - acronyms
  - supporting details
  - references to other documents
  - responsibilities

Reading

Brotby 4,5,6,8 (skip 3 and 7 for now)

Homework

No Required Homework. I will post some extra problems.

Questions?

Matt Hale, PhD

University of Nebraska at Omaha

Interdisciplinary Informatics

mlhale@unomaha.edu

Twitter: @mlhale_