RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: **TECH-T08**

Back to Basics: How to Create Effective Information Security Policies

Chuck Kesler

Chief Information Security Officer
Pendo.io
@chuck_kesler

What's worse?*

having a poorly executed policy that no one follows

-or-

having no policy at all?

*with credit to the CISO Security Vendor Relationship Series Podcast (https://cisoseries.com/)

What's worse?

being granted permission to publish whatever policy you want

-or-

having to explain and justify the policies you want to implement

Agenda

- The Foundation for Good Policies
- Writing Effective Policies
- Successfully Implementing Policies

RSAConference2019

The Foundation for Good Policies

Why do policies fail?

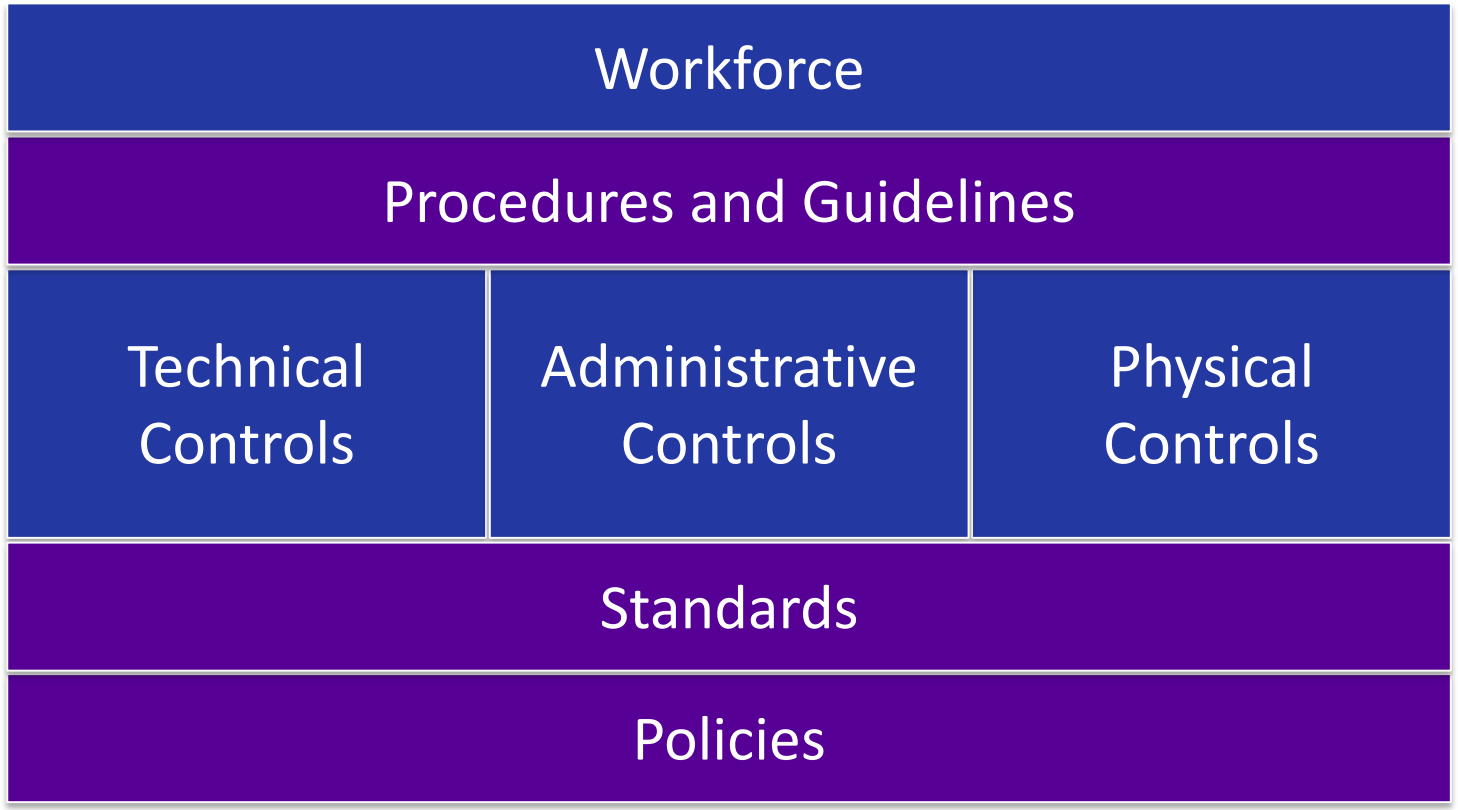
- C-Suite doesn’t buy-in
- The “why” isn’t understood
- Too complex
- Lack of monitoring and enforcement
- Re-using someone else’s policy
- Creating audit fodder

First… what are the differences between policies, standards, procedures, and guidelines?

	Purpose	Approved By	Frequency of Update
Policy	Defines management intent for addressing risk; provide support for other controls	Executives	Infrequent
Standards	Provides technical details to support policy implementation	Directors	Occasional
Procedures	Step-by-step directions for implementing one or more aspects of a policy	Managers	Often
Guidelines	User-focused tips that support the objectives of a policy	Managers	Often

Note: most of what is presented here can be applied equally to policies, standards, procedures, and guidelines

Relationships between controls



Foundations for a good policy

- Setting a clear tone from the top
- Gaining broad-based input and support
- Focusing on adding value, not just checking a box
- Aligning with the enterprise risk appetite
- Aligning with the business

Elements of policy alignment

- Regulations
- Frameworks
- Business engagement
- Governance
- Leadership

Alignment with regulations and frameworks

- Understand the regulations (e.g. GDPR, HIPAA, PCI) that apply
  - Identify areas of risk to address
  - Provide boundary conditions where risk may/may not be acceptable
- Leverage frameworks (e.g. NIST, ISO) to guide the process
  - Provides best practices for creating controls
  - Meet multiple regulatory requirements with a single set of controls
  - Caution: not usually easy to use! Need to put in context of the business
  - May need a hybrid of multiple frameworks

Business alignment: input from stakeholders and SMEs

Stakeholders

- Board
- C-Suite
- Compliance/Audit
- Engineering/Operations
- Customer-facing functions
- GenOps functions
- Customers

Subject Matter Experts

- Peer organizations (e.g. ISACs)
- Professional groups (e.g. ISC^2)
- Consultants (e.g. benchmarking)
- Informal networking with peers

Business alignment: requirements and constraints

Requirements

- Regulatory
- Legal
- Contractual
- Business plans

Constraints

- Financial
- Operational
- Technology
- People

The importance of governance

- Use a governance committee for stakeholder input and buy-in
  - Include representatives from all key stakeholder groups
  - Right-size the group
  - Have a regular meeting cadence
  - Include agenda time for handling exceptions
  - Maintain transparency

Leadership: the CISO's role in policy making

- The CISO should:
  - Understand and be part of the business
  - Help the business balance risk vs. value
  - Educate the business on information security risks
  - Calibrate the organization's moral compass on data privacy
  - Act as a "choice architect" for leadership
  - Understand that there will be differences of opinion on risk vs. value
  - Not be afraid to take a stand against egregious or negligent behavior

Leadership: the CISO's role in policy making

- The CISO should not:
  - Not behave as if above the business
  - Expect to win every battle
  - Always take a hard line and refuse to budge… you will be marginalized

RSAConference2019

Writing Effective Policies

The keys to writing effective policies

- Readability
- Structure
- Maintainability
- SMART Content

Readability

- Write with the audience in mind
- Don’t go overboard with legalese
- Keep policies to a manageable length
- Remember: if the policy can’t be easily understood, it probably won’t be followed!

Policy structure

- Use consistent structure to enhance policy readability; example:
  - Scope
  - Purpose
  - Policy statements
  - Roles and responsibilities
  - Exceptions
  - Revision history
  - Approvals
  - Definitions
  - Cross-references to regulatory and/or framework requirements

Maintainability: consider using a glossary

- Need to keep terminology definitions consistent
- This is challenging when terms are repeated across policies
- Defining commonly used terms in a glossary improves manageability

SMART policies

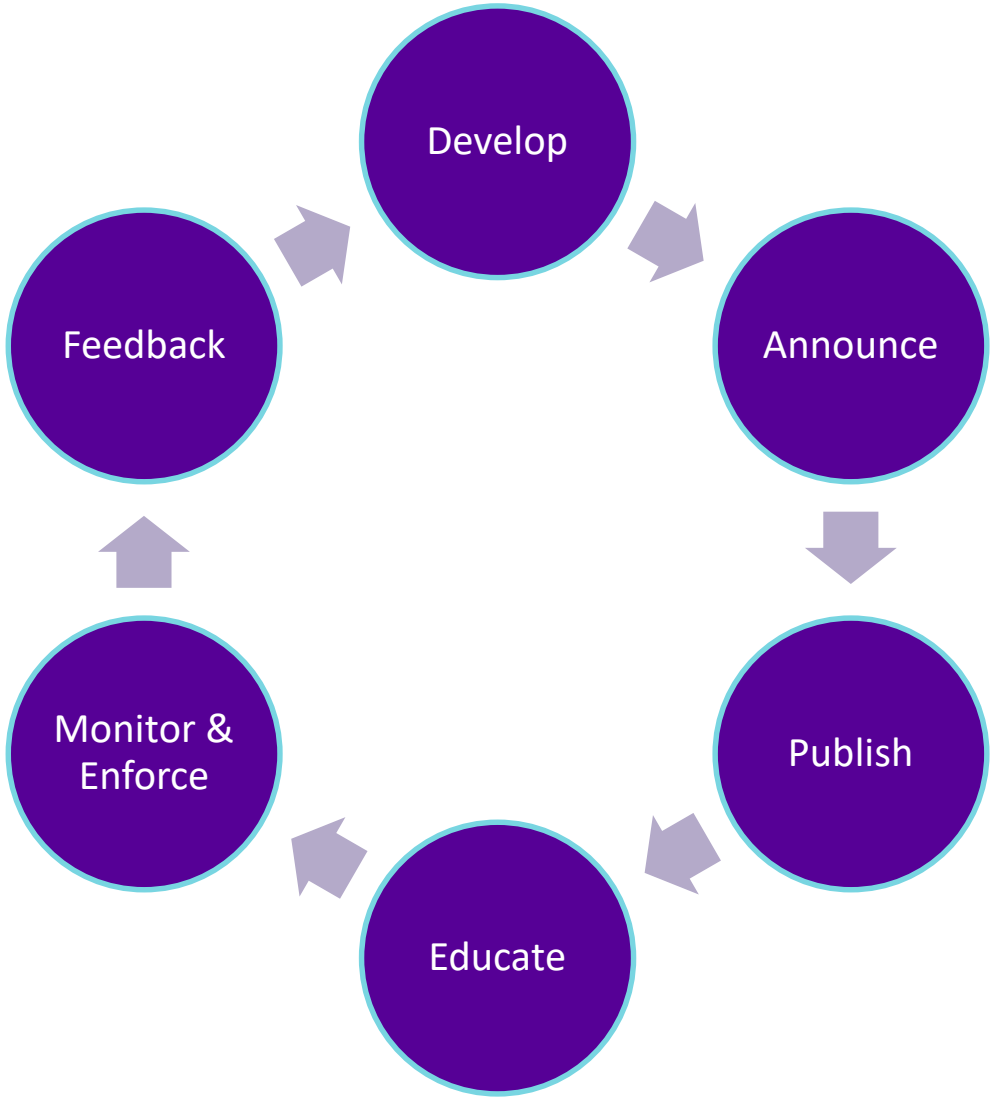
- **S**pecific: the policy addresses specific, clearly defined issues
- **M**easurable: there is a means to measure the effectiveness of the policy
- **A**chievable: the policy can be implemented in a reasonable manner
- **R**elevant: the policy addresses the needs and risks of the business
- **T**imely: the time required to implement the policy is appropriate

RSAConference2019

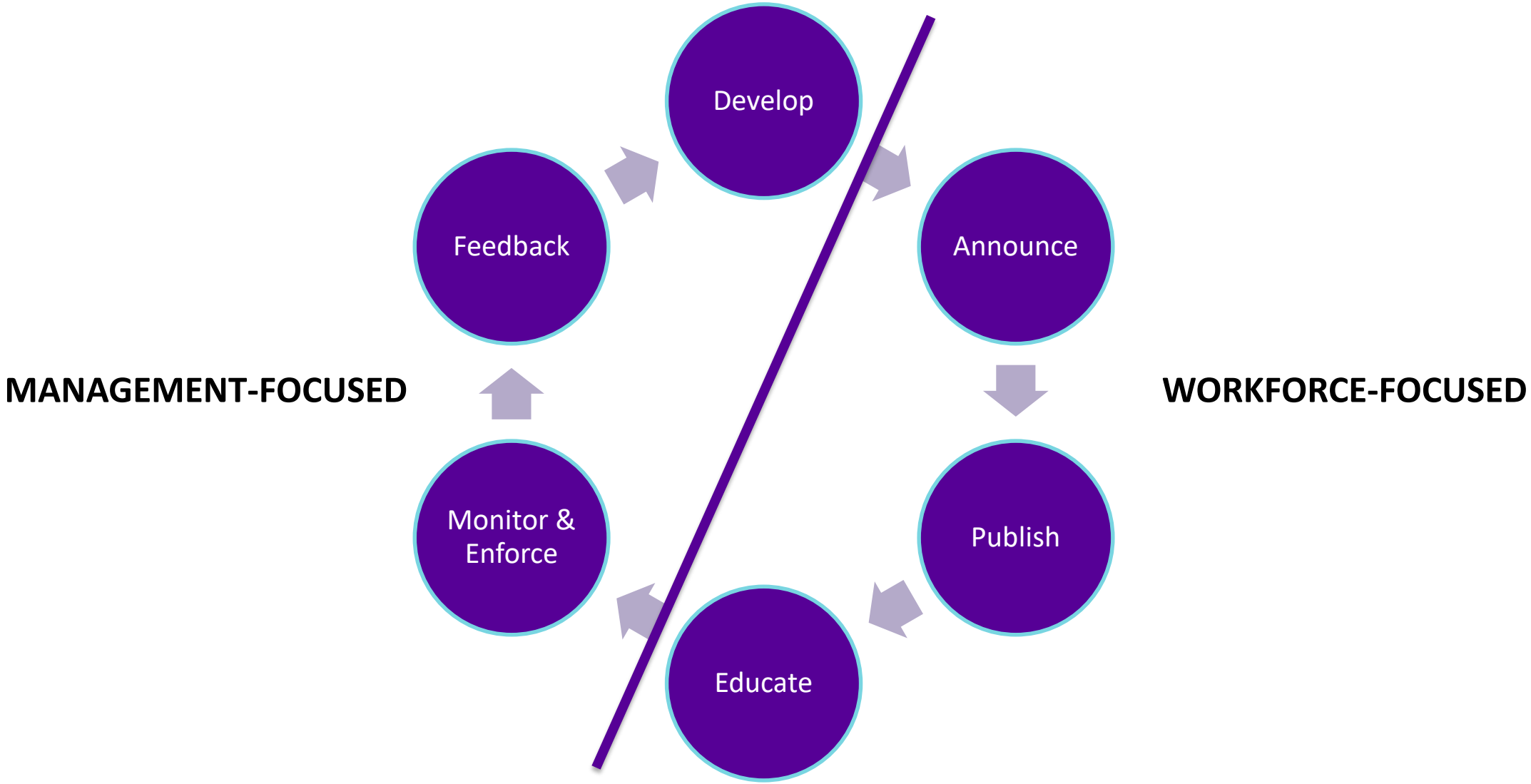
Successfully Implementing Policies

Policy implementation lifecycle

Hey, this looks like a Plan-Do-Check-Act Deming Cycle!



Policy implementation lifecycle



1. Develop

- Summarizing key points from earlier discussion:
  - Align with and seek input from stakeholders
  - Ensure readability and enforceability (e.g. with SMART principles)
  - Use governance processes to review and ratify

2. Announce

- Avoid surprises!
- Develop a communications plan
  - What will be happening (including any accompanying technical controls)
  - Why is it happening
  - Who is affected
  - When it will be happening
  - Where more information can be found
- Use multiple channels to communicate

3. Publish

- Use a central repository for storing and publishing policies
  - Usually on the intranet, but may be Internet-accessible
  - Must be available to all who must abide by the policy
  - GRC systems (e.g. Archer) can help
- Maintain a revision history
  - Follow best practices for change management
  - May be needed to support post-breach regulatory investigations

4. Educate

- Policies won’t/can’t be followed if they’re not understood!
- The level of required understanding may differ
- Plans for education before rolling out the policy
- Track completion and effectiveness of education activities

5. Monitor & Enforce

- Goals, metrics, KPIs, and targets should be used to monitor and manage progress, e.g.:
  - Goal: require the use of MFA by a certain date
  - Metric: number of users enrolled in MFA
  - KPI: % of users enrolled in MFA (is going up or down?)
  - Targets: 50% enrolled by X, 75% enrolled by Y, 100% enrolled by Z

5. Monitor & Enforce

- Policies should also include enforcement mechanisms
- Define roles and responsibilities for enforcement
  - Consider using RACI chart
- Have a mechanism to consider and approve exceptions
  - Must be done at an appropriate level in the organization
- Define penalties for failure to comply
  - Tie to HR processes

6. Feedback

- Continuous improvement is a must
- Learn from incidents
- Business requirements and constraints evolve
- Regulations change
- Rule of thumb: review all policies on a 1 to 3 year cycle

RSAConference2019

Wrap-up

Summary

- Policies usually succeed or fail based on the “tone from the top”
- Policies should underlie all other security controls
- Ensure policies are aligned with the business
- Write policies in a way that they can be understood and followed
- Regularly review and update policies
- Have reasonable consequences for non-compliance
- Effectively communicating policies is key to adoption

Apply

- Within the next month
  - Review current policies and note those that are out of date
- Within the next quarter
  - Map policies back to your compliance requirements and note any gaps
  - If you don’t already have one, start a governance committee
- Within the next six months
  - Begin addressing identified gaps with new or revised policies

References - articles

- https://www.sans.org/reading-room/whitepapers/policyissues/building-implementing-information-security-policy-509
- https://www.sans.org/security-resources/policies/
- https://frsecure.com/blog/differentiating-between-policies-standards-procedures-and-guidelines/
- https://www.csoonline.com/article/2124114/it-strategy/strategic-planning-erm-how-to-write-an-information-security-policy.html
- https://resources.infosecinstitute.com/key-elements-information-security-policy/
- https://adeliarisk.com/13-fantastic-resources-writing-information-security-policy/

References – example policies (universities)

- https://security.duke.edu/policies-standards-procedures
- https://policylibrary.gatech.edu/information-technology
- https://policies.iu.edu/categories/information-it.html
- https://www.wisconsin.edu/uw-policies/news/information-security-policies-and-procedures/
- http://policies.vpfa.fsu.edu/policies-and-procedures/technology/information-security-policy/