



Policy Management by Design

Blueprint for an Effective, Efficient & Agile Policy Management Program

Michael Rasmussen, J.D., GRCP, CCEP

The GRC Pundit @ GRC 20/20 Research, LLC

OCEG Fellow @ www.OCEG.org

Our Agenda . . .

1) **PART 1: Policy by Design**

Why Policies Matter

2) **PART 2: Policy Governance**

Blueprint for Effective Policy Management

3) **PART 3: Policy Management Lifecycle**

Managing Policies from Creation to Dissolution

4) **PART 4: Policy Management Architecture**

Enabling Information & Technology Management of Policies

PART 1

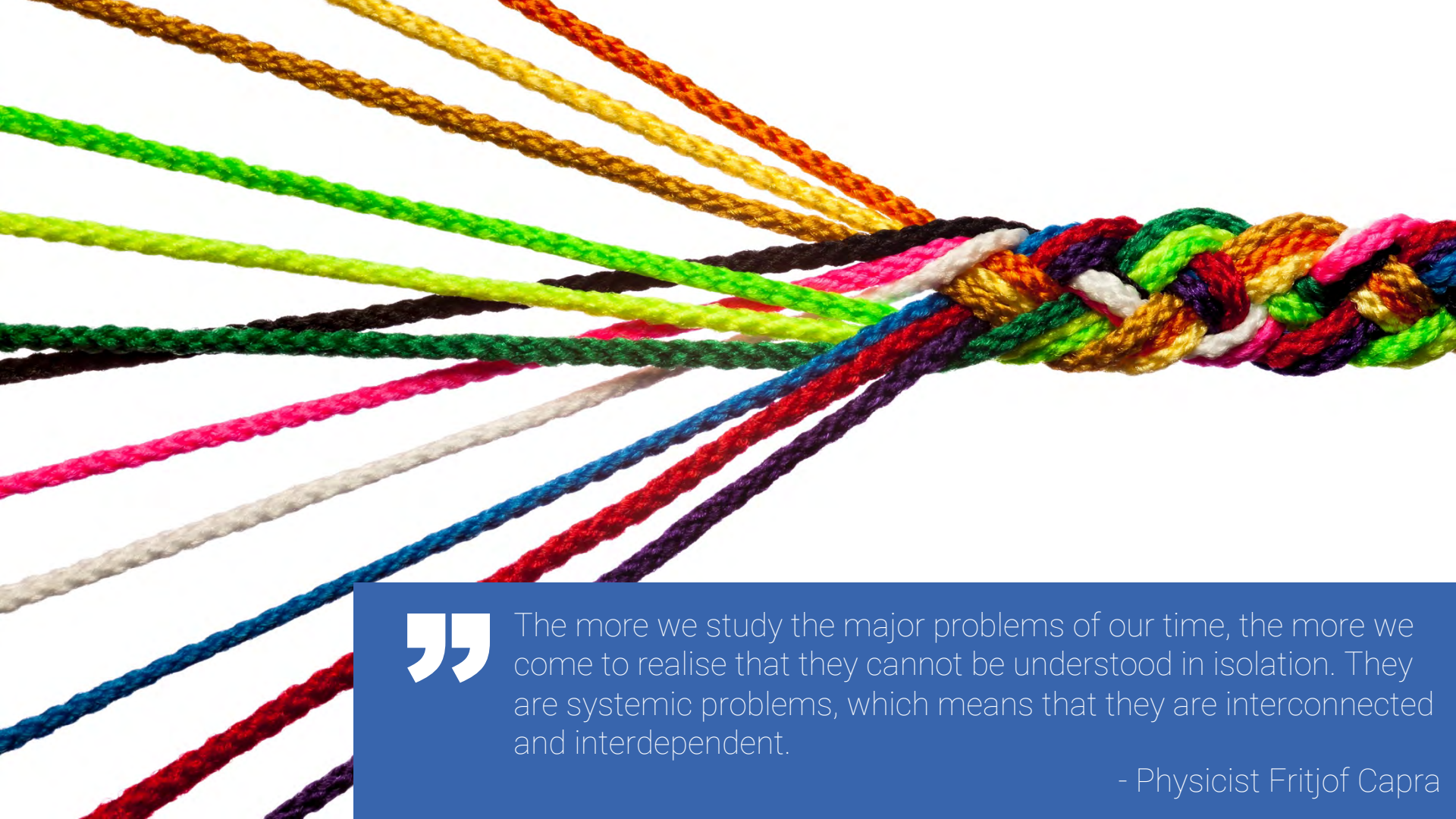
Policy by Design: Why Policies Matter?

Learning Objectives . . .

- ❑ Policies in Disarray
How organizations mismanage policies
- ❑ Policy Exposure
How mismanaged policies expose the organization to risk
- ❑ What Effective Policy Management Achieves
Policy management's role in GRC
- ❑ Case Study in Effective Policy Management
A look at Morgan Stanley
- ❑ Interactive Group Discussions



Navigating Chaos



”

The more we study the major problems of our time, the more we come to realise that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.

- Physicist Fritjof Capra



”

” *Realize that everything connects to everything else.*

Leonardo da Vinci

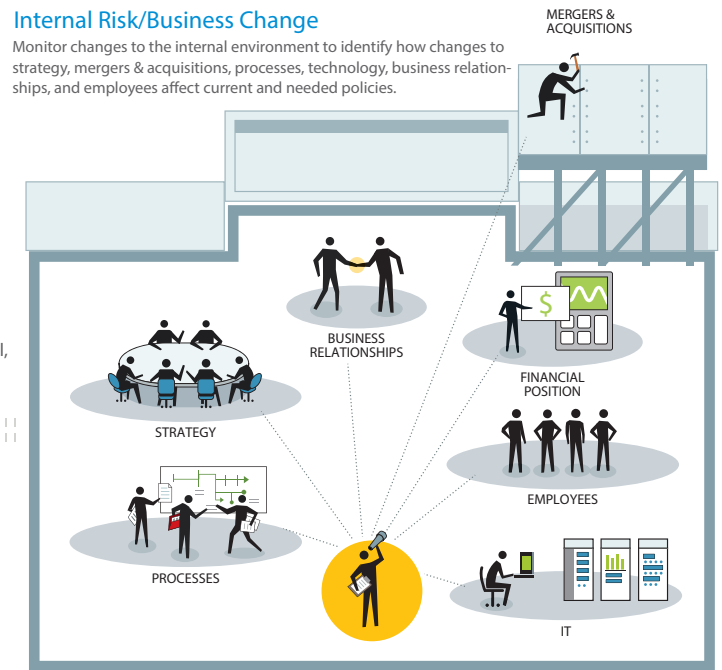
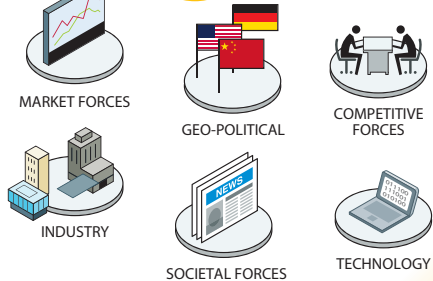
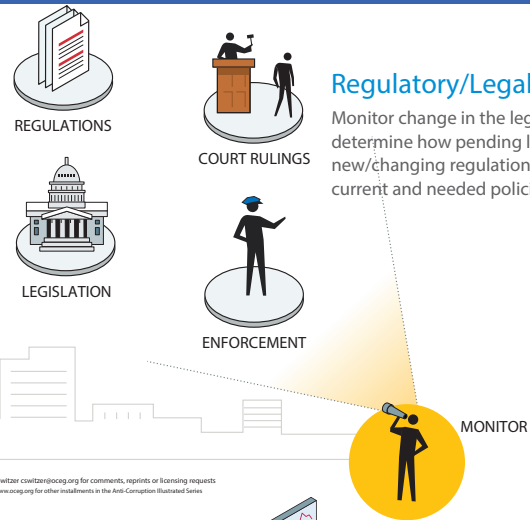
The Chaos of Compliance Interconnectedness



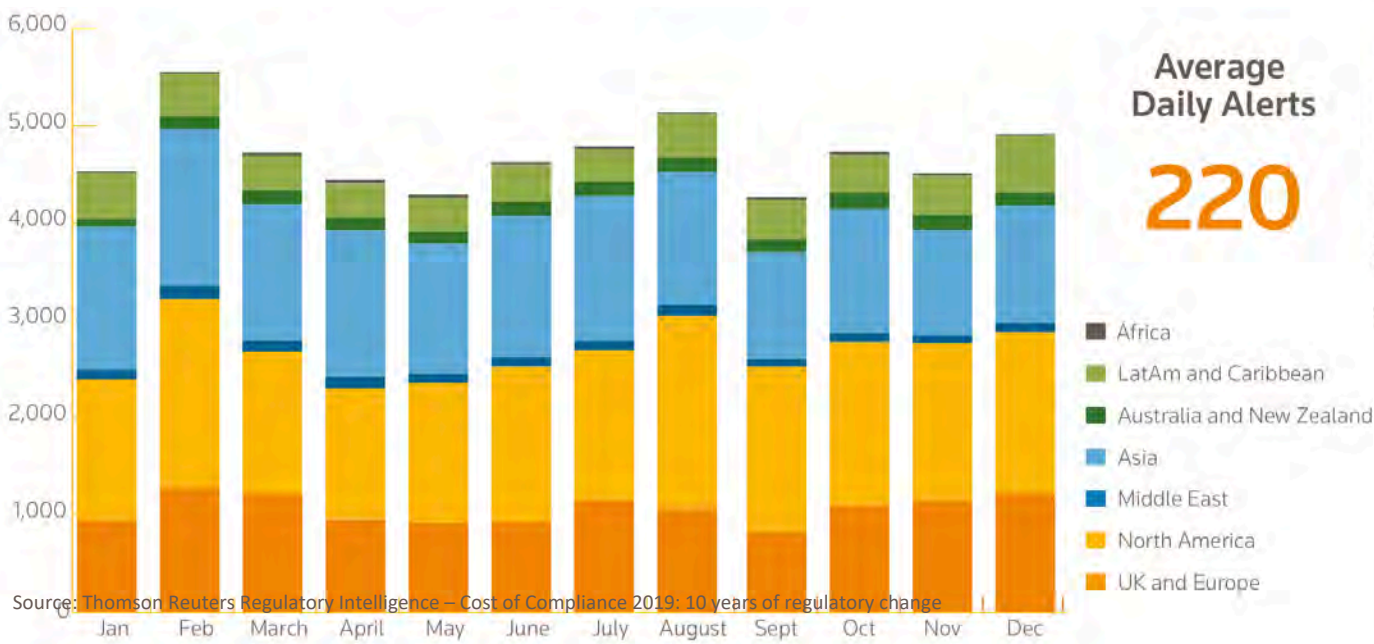
” *Realize that everything connects to everything else.*

Leonardo da Vinci

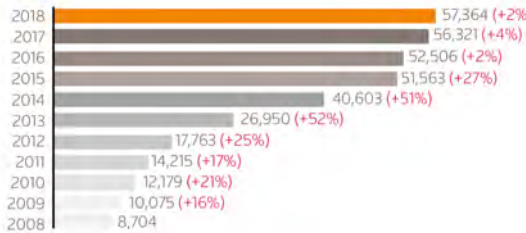
Change is the Greatest Challenge Impacting Policy Management



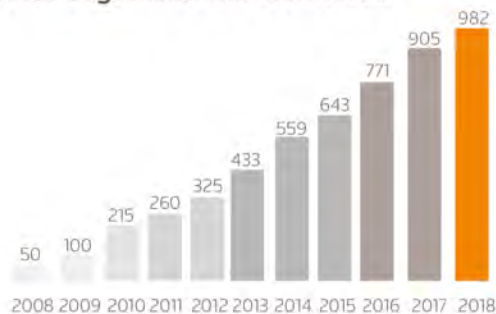
Regulatory Activity in Financial Services 2008 to 2018



Total Yearly Alerts



Total Organisations Monitored



Compliance in Transition: From Old Ways to New Ways



UK Senior Managers Regime/Certification Regime



One [REGULATION] to rule them all, One [REGULATION] to find them [RISK, COMPLIANCE, CONTROL], One [REGULATION] to bring them all, and in the [ENFORCEMENT] bind them.

ACCOUNTABILITY **VS** **RESPONSIBILITY**

(a subtle but very powerful difference)

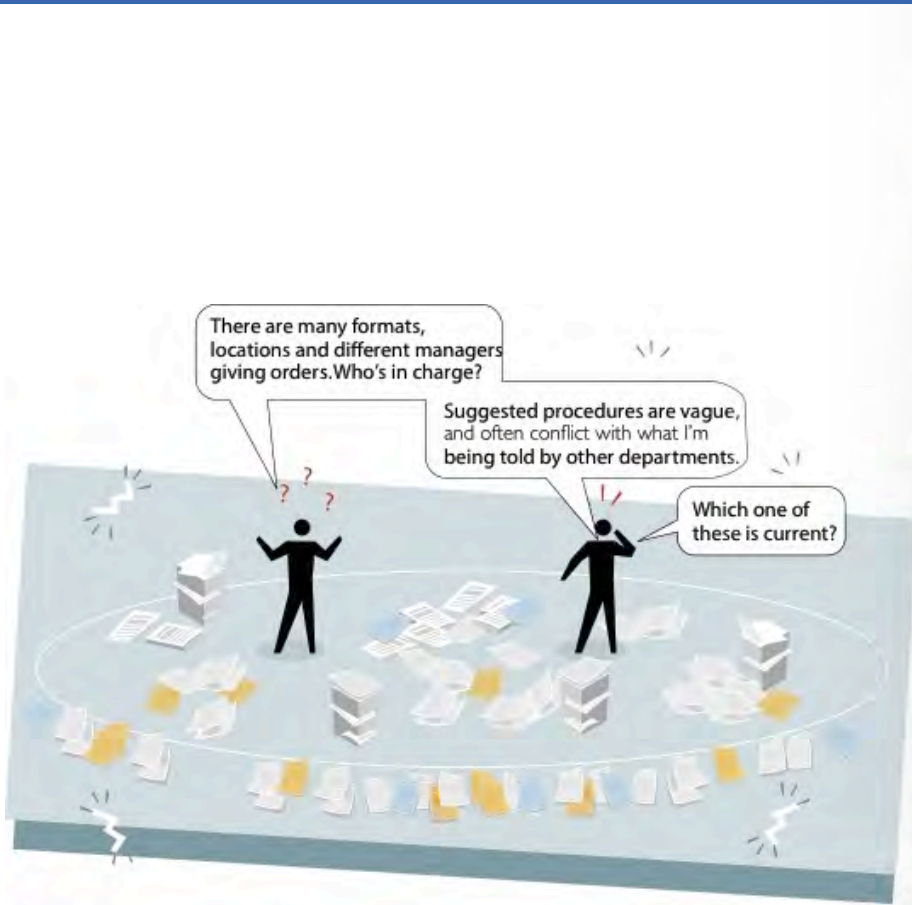
Inevitability of Failure: Too Many Documents & Manual Approaches



Battling the Hydra of Ineffective Policy Management



... Confusing Policy Management User Experience



... And We Hope Nothing Fails

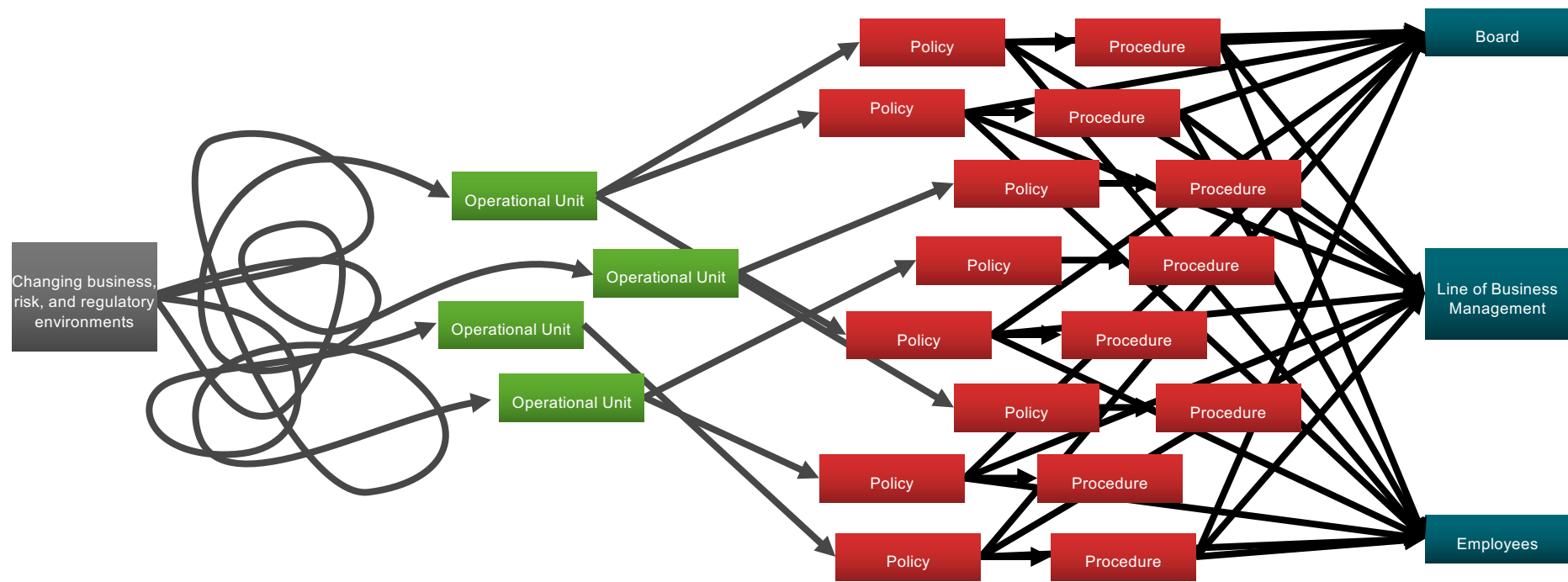
- Inability to gain clear view of policy interdependencies;
- High cost of consolidating policy compliance information;
- Difficulty maintaining accurate policies;
- Failure to trend and measure policies;
- Redundant approaches limit correlation, comparison and integration of policy management; and
- Lack of agility to respond timely to changing risks, regulations, laws, and situations.



Having a Well Written Document is Not Enough



Business Reacting to Policies From Every Direction





The Organization Has to be Able to See . . .

- ❑ The Tree. The individual policy
- ❑ The Forest. The interconnectedness of policies

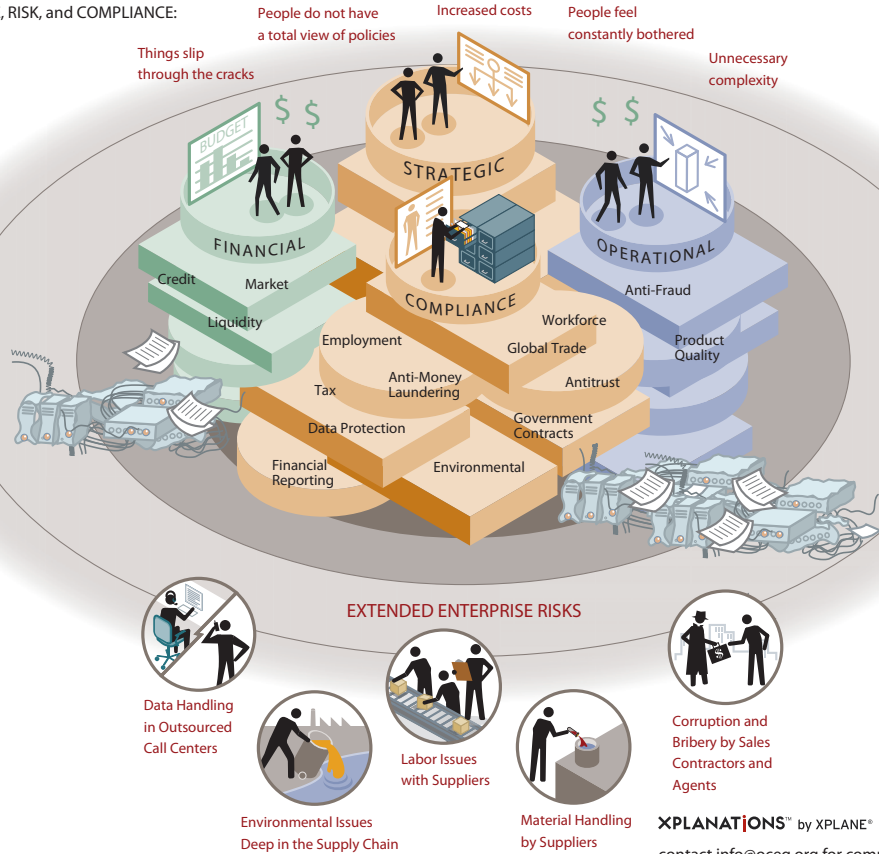
We Have to Communicate Policies Across 3rd Party Relationships



Policy Discovery & Inventory: Do You Know Where Your Policies Are?

First, it's important to understand your current environment— in particular all of the existing policies across the organization and it's . . .

SILOS OF GOVERNANCE, RISK, and COMPLIANCE:



XPLANATIONS™ by XPLANE® ©2008 OCEG®
contact info@oceg.org for comments, reprints or licensing requests

Balancing the Right Amount of Policy

NO GUIDANCE OR SUPPORT (UNDER-CONTROL)



OVER-CONTROL



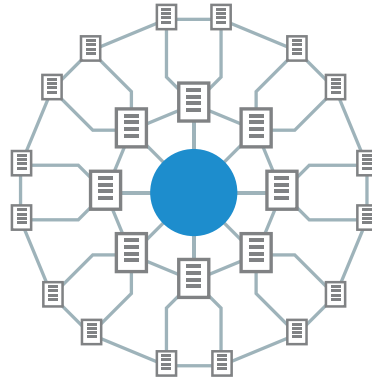
Drivers in Policy Management



Why Policy Management Matters

Strong, well managed policies that are integrated across the business help to:

- Define, articulate, and communicate boundaries and expectations
- Communicate risk limits
- Establish a culture of compliance
- Guide desired conduct
- Protect the organization
- Achieve business objectives
- Explain governance and accountability structures



In many organizations, policies are scattered throughout the entity with no central repository and suffer from:

- Inconsistent styles
- Unauthorized issuance
- Lack of ownership
- Poor lifecycle management
- No mapping to exceptions or incidents
- No cross-reference to standards, rules, or regulations



What policies are all about . . .



Not every enterprise would describe itself as a “fast car,” however, most organizations want to drive toward objectives – while avoiding bumps in the road

FASTEST CARS
have (should have) the **BEST BRAKES**

Policies are a foundation for all aspects of GRC . . .



GRC is a capability that enables an organization to:

G) reliably achieve objectives

R) while addressing uncertainty and

C) acting with integrity.

SOURCE: OCEG GRC Capability Model



Governance

Define the organization's governance culture and structure: Without good policy as a guide, corporate culture and control morphs, changes and takes unintended paths.



Risk Management

Articulate a culture of risk: Policy addresses risk and establishes risk responsibility, communication, appetites, tolerance, and risk ownership. Without clearly written policy, risk governance is ineffective.



Compliance

Establish a culture of compliance: Policy establishes how an organization meets its obligations and commitments and how it will stay within legal, regulatory, and contractual boundaries.

Policies Define the Foundation of Corporate Culture

As a company, we may document internal governance requirements and practices for a number of reasons, including to:

- Meet legal, statutory, regulatory or contractual requirements;
- Clearly state expectations for employees' actions;
- Promote consistency across departments, business units or markets;
- Promote assurance of results based on individual actions; or
- Clarify accountability for employee-based processes.

Does management and the organization as a whole behave with integrity?

ETHICS CULTURE

Do you feel pressured to compromise our values?



GOVERNANCE CULTURE

Here is the plan...

CEO

I need to challenge you on that...



RISK CULTURE

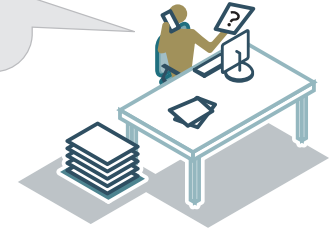
This deal is really important for this quarter.

But it is not in-sync with our risk appetite.

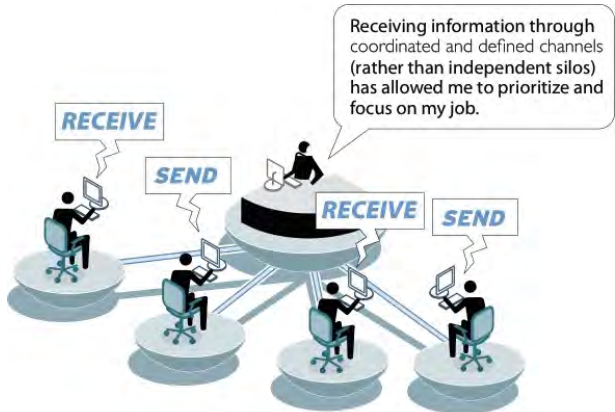


WORKFORCE CULTURE

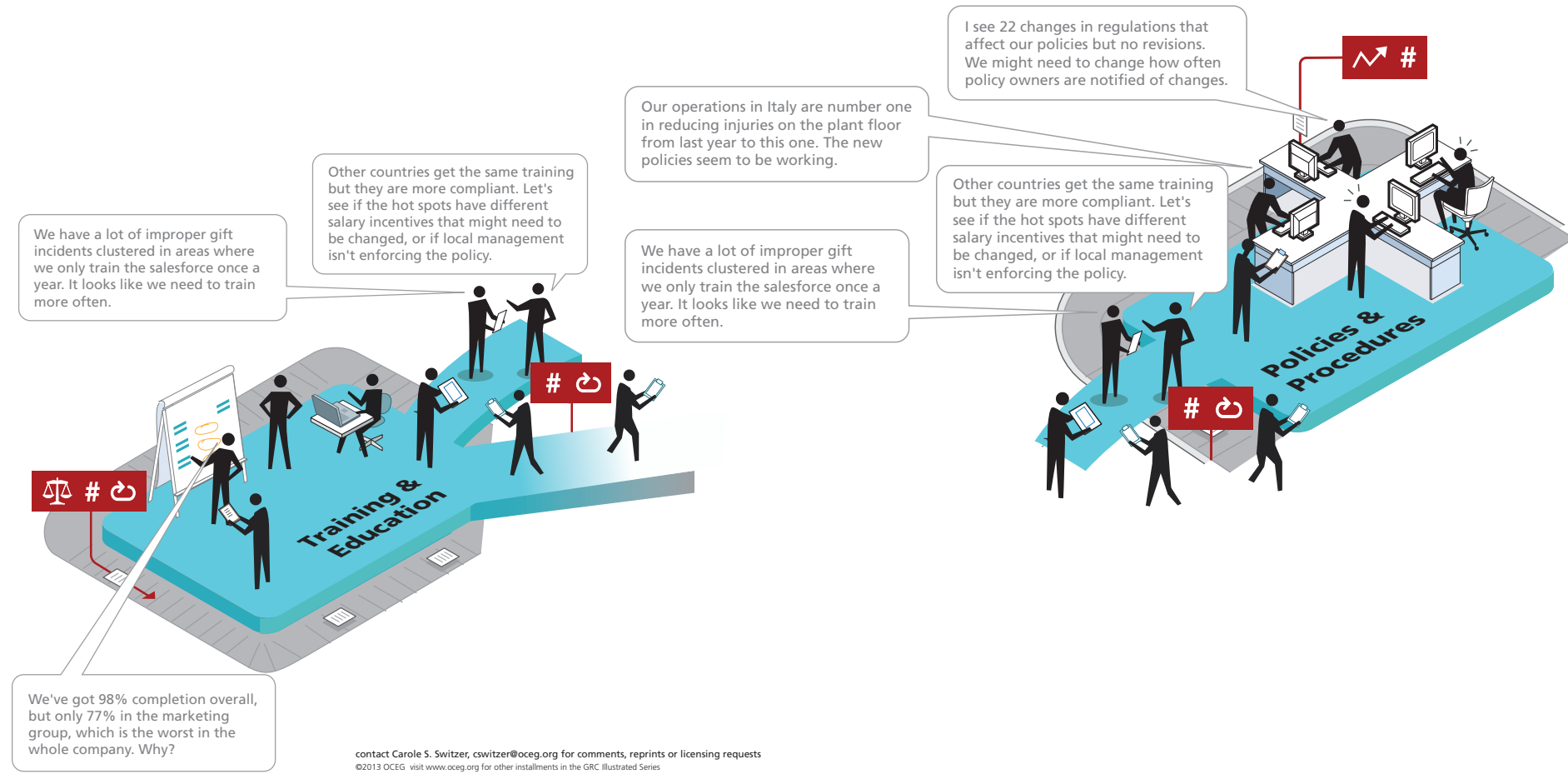
I know where I fit and how to succeed!



Employee Engagement Gets the Message Across



Getting a Handle on Policies Improves Governance, Risk Management & Compliance



contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests
©2013 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

Morgan Stanley: Case Study in Effective GRC Engagement

"Morgan Stanley ***maintained a system of internal controls*** meant to ensure accountability for its assets and to prevent employees from offering, promising or paying anything of value to foreign government officials. Morgan Stanley's ***internal policies, which were updated regularly to reflect regulatory developments and specific risks***, prohibited bribery and addressed corruption risks associated with the giving of gifts, business entertainment, travel, lodging, meals, charitable contributions and employment. ***Morgan Stanley frequently trained its employees on its internal policies***, the FCPA and other anti-corruption laws. Between 2002 and 2008, Morgan Stanley trained various groups of Asia-based personnel on anti-corruption policies 54 times. During the same period, Morgan Stanley trained Peterson on the FCPA seven times and ***reminded him to comply*** with the FCPA at least 35 times. Morgan Stanley's compliance ***personnel regularly monitored transactions, randomly audited particular employees, transactions and business units, and tested*** to identify illicit payments. Moreover, Morgan Stanley ***conducted extensive due diligence on all new business partners*** and imposed ***stringent controls*** on payments made to business partners."

Emphasis added to illustrate elements of effective GRC management and engagement. Source of this statement is at: <http://www.justice.gov/opa/pr/2012/April/12-crm-534.html>.

In a report in November 2012, the DOJ and SEC stated they:

"have often encountered companies with compliance programs that are strong on paper but that nevertheless have significant . . . violations because management has failed to effectively implement the program even in the face of obvious signs of corruption."

POINT: Regulators are tired of paper-based compliance programs that look good on paper but fail in operations and employee engagement.

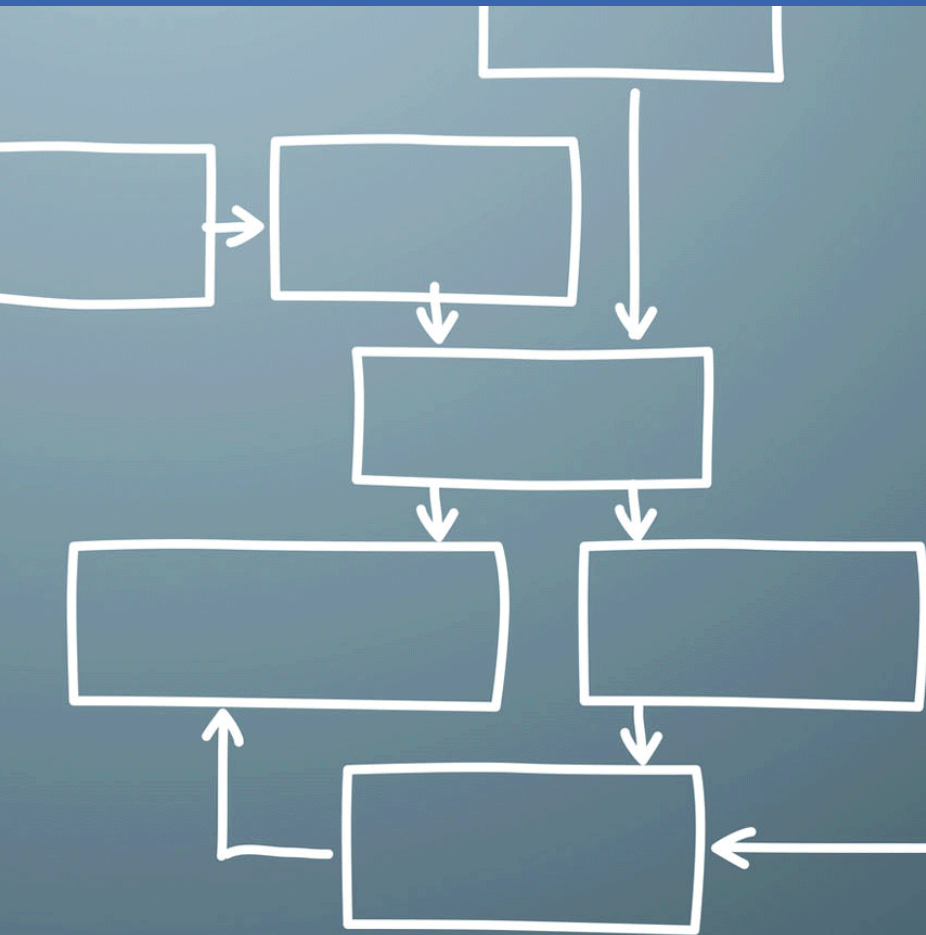


Policy Assurance: Do the frontlines understand policies?



Policy Assurance: Is the organization collaborating on policies?

A person in a dark suit is standing next to a chalkboard, holding a black pen and drawing a flowchart. The flowchart is composed of several white-outlined rectangular boxes connected by white arrows. The flow starts from the top, goes down to a box, then left to another box, then down to a third box. From this third box, the flow splits into two parallel paths, each leading to a box. These two boxes then converge into a single path that leads to a final box at the bottom. A red rectangle highlights one of the boxes in the middle section of the flowchart.





Policy Assurance: What analytics and metrics do you have on policies?

Mobility: Policy Communication Done & Delivered Anywhere at Anytime



Table 1: Estimated Monthly Sales

Month	Q1	Q2	Q3	Q4	Annual Total
Jan	1.2M	1.3M	1.4M	1.5M	5.4M
Feb	1.3M	1.4M	1.5M	1.6M	5.8M
Mar	1.4M	1.5M	1.6M	1.7M	6.2M
Apr	1.5M	1.6M	1.7M	1.8M	6.6M
May	1.6M	1.7M	1.8M	1.9M	7.0M
Jun	1.7M	1.8M	1.9M	2.0M	7.4M
Jul	1.8M	1.9M	2.0M	2.1M	7.8M
Aug	1.9M	2.0M	2.1M	2.2M	8.2M
Sep	2.0M	2.1M	2.2M	2.3M	8.6M
Oct	2.1M	2.2M	2.3M	2.4M	9.0M
Nov	2.2M	2.3M	2.4M	2.5M	9.4M
Dec	2.3M	2.4M	2.5M	2.6M	9.8M
Total	21.0M	22.0M	23.0M	24.0M	90.0M

Table 2: Estimated Monthly Sales

Month	Q1	Q2	Q3	Q4	Annual Total
Jan	1.1M	1.2M	1.3M	1.4M	5.0M
Feb	1.2M	1.3M	1.4M	1.5M	5.4M
Mar	1.3M	1.4M	1.5M	1.6M	5.8M
Apr	1.4M	1.5M	1.6M	1.7M	6.2M
May	1.5M	1.6M	1.7M	1.8M	6.6M
Jun	1.6M	1.7M	1.8M	1.9M	7.0M
Jul	1.7M	1.8M	1.9M	2.0M	7.4M
Aug	1.8M	1.9M	2.0M	2.1M	7.8M
Sep	1.9M	2.0M	2.1M	2.2M	8.2M
Oct	2.0M	2.1M	2.2M	2.3M	8.6M
Nov	2.1M	2.2M	2.3M	2.4M	9.0M
Dec	2.2M	2.3M	2.4M	2.5M	9.4M
Total	20.0M	21.0M	22.0M	23.0M	86.0M



Workshop Activity

Our Agenda . . .

1) PART 1: Policy by Design

Why Policies Matter

2) **PART 2: Policy Governance**

Blueprint for Effective Policy Management

3) PART 3: Policy Management Lifecycle

Managing Policies from Creation to Dissolution

4) PART 4: Policy Management Architecture

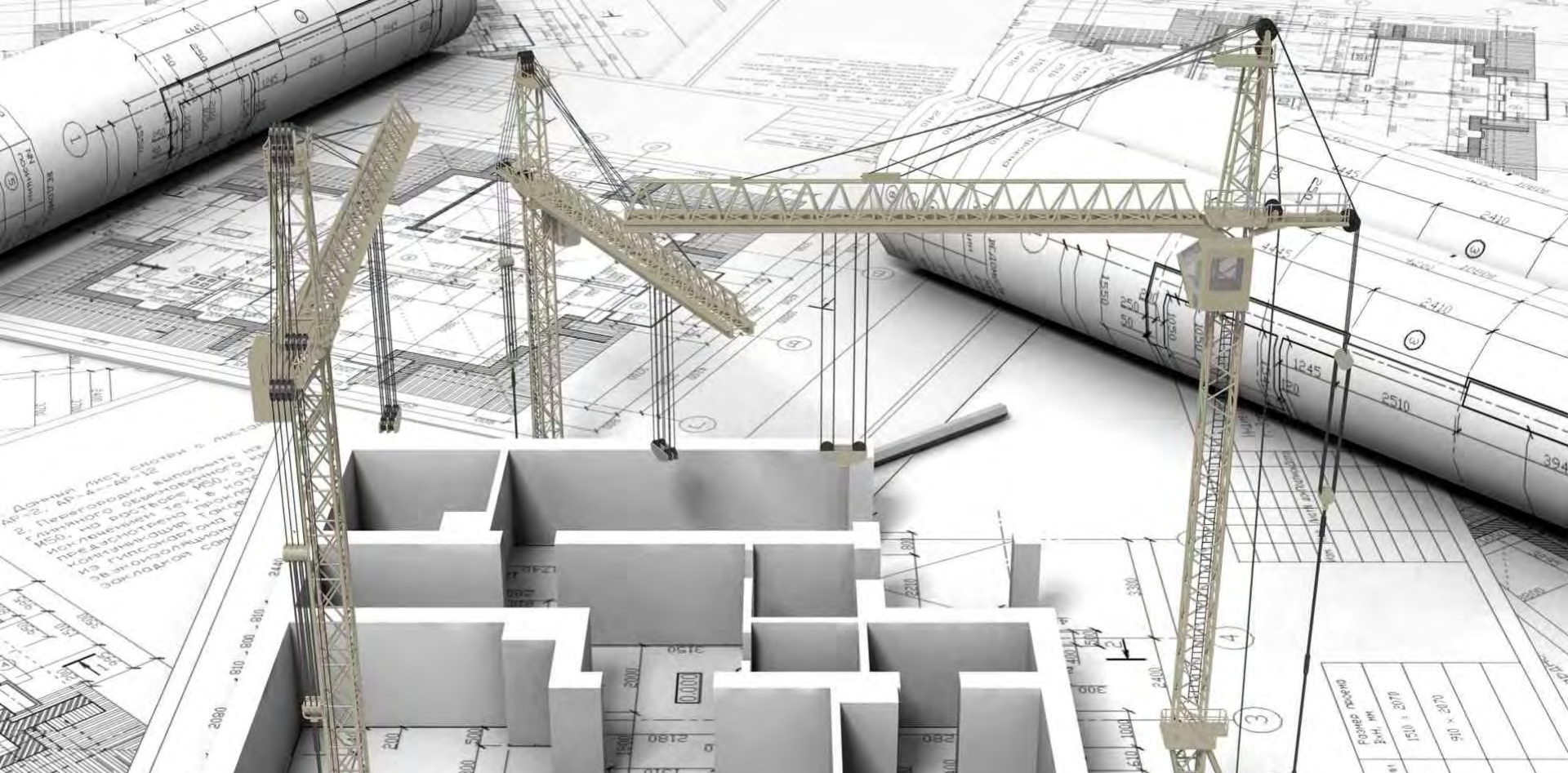
Enabling Information & Technology Management of Policies

PART 2

Policy Governance: Blueprint for Effective Policy Management

Learning Objectives . . .

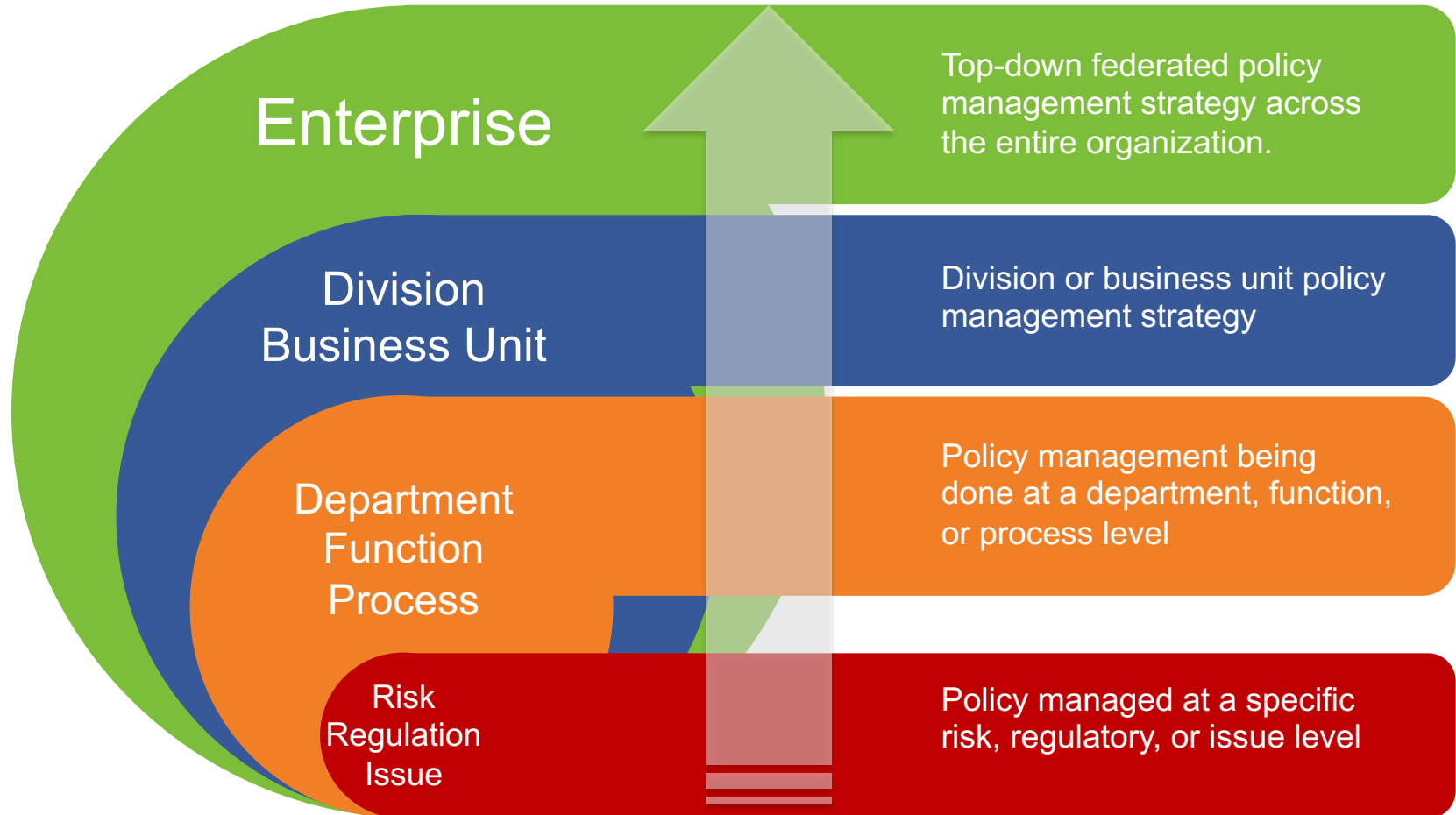
- ❑ Policy Committee & Collaboration
Bringing together policy roles and responsibilities across the organization
- ❑ Policy Management Charter
Defining a structure to govern policies
- ❑ The Meta Policy
The organization's policy on writing policies
- ❑ Style Guide
Ensuring policies are written consistently to the organization's voice
- ❑ Interactive Group Discussions



What if we could design policy management?

ПОЯСНЕНИЕ		Пояснение	
№	пояснения	№	пояснения
9	1500 x 2070	10	900 x 2070
11	1500 x 2100	12	2100 x 2170

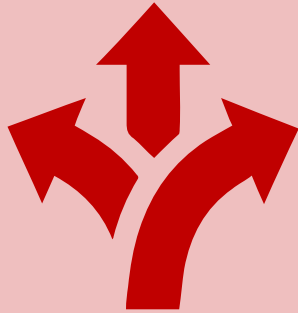
Varying Levels of Policy Management



What is Your Approach to Policy Management?

Distributed Policy Management

- Disconnected departments managing policies in different ways with little or no collaboration with other departments



Federated Policy Management

- An integrated approach that balances policy management centralization with distributed participation and collaboration





Policy Management Strategy



Policy Management Process



Policy Management Information

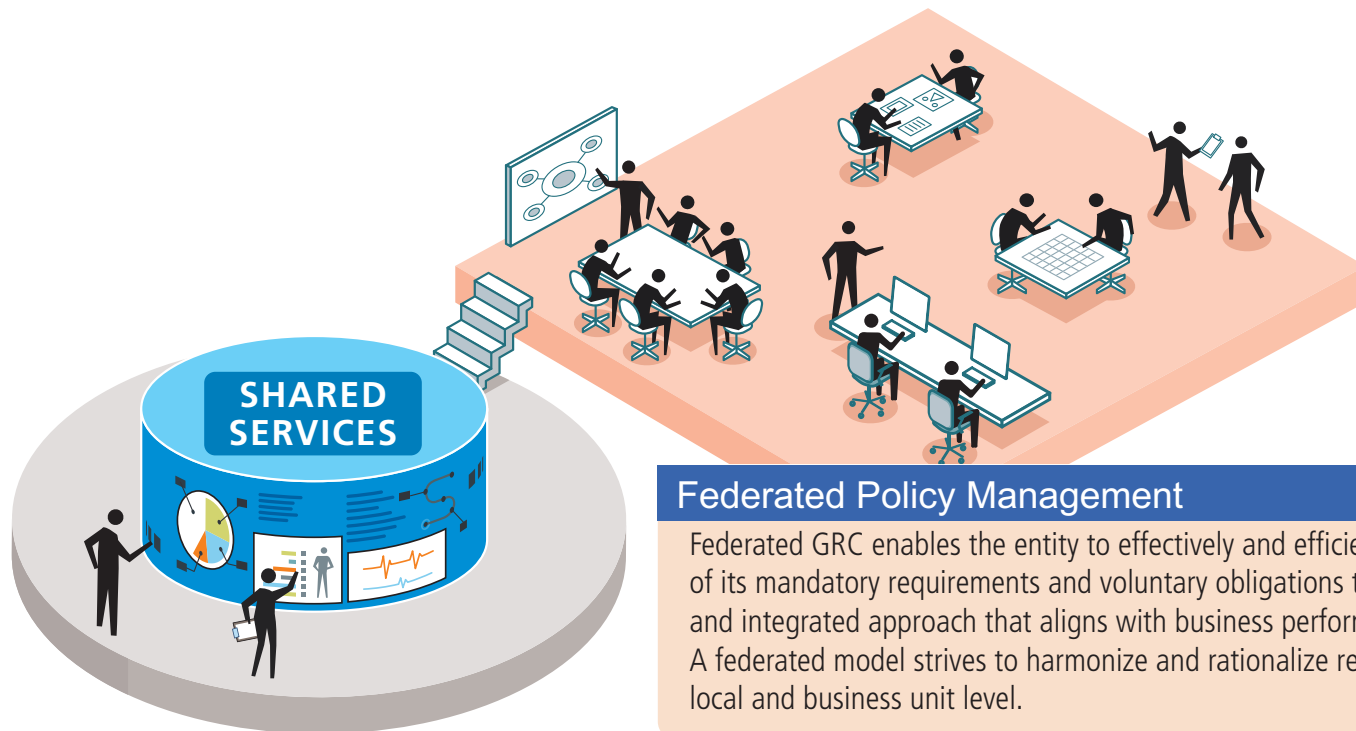


Policy Management Technology

GRC Capability Model v3.0: Iterative Cycles of Change & Improvement

改
KAI
“CHANGE”
善
ZEN
“GOOD”





Federated Policy Management

Federated GRC enables the entity to effectively and efficiently identify and manage all of its mandatory requirements and voluntary obligations through a common framework and integrated approach that aligns with business performance and risk management. A federated model strives to harmonize and rationalize requirements at the global, local and business unit level.

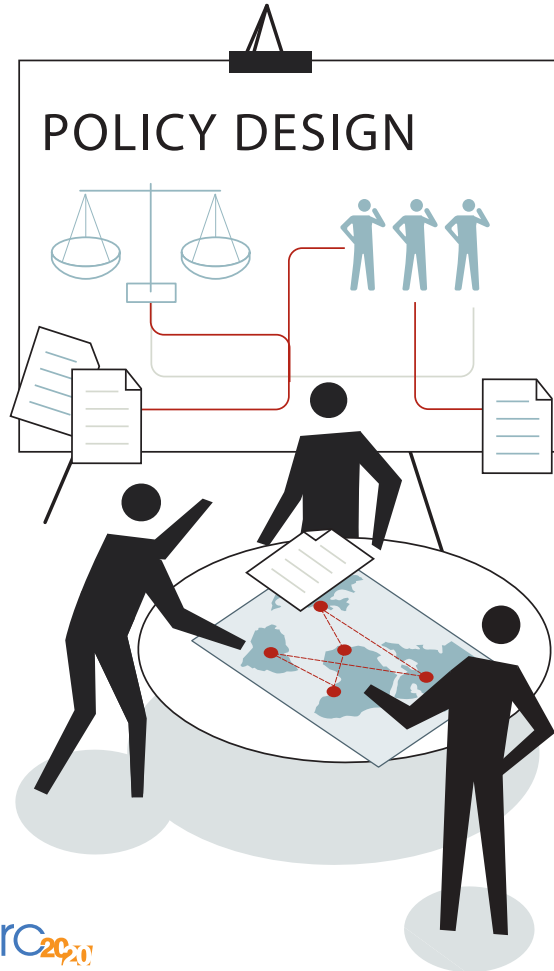
contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

©2013 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

Critical Elements of an Effective Policy Management Strategy

- ✓ Defined policy management lifecycle
- ✓ Policy program manager role
- ✓ Top down & bottom up approach for sharing ideas and concerns
- ✓ Delegation of authority from board or executive management via charter
- ✓ Common taxonomy & formal templates for policies, procedures, etc.
- ✓ Central repository of all policies (geographical, functional & retired) and related policies that all staff can access easily
- ✓ Method for communicating policies & supporting procedures to individuals
- ✓ Ability to demonstrate that individuals have read, attested to, or acknowledged policies
- ✓ Provisions to evaluate & measure staff compliance with the organization's policies
- ✓ Metapolicy codifying roles & responsibilities for achieving the above

Governing What Policies the Organization Has

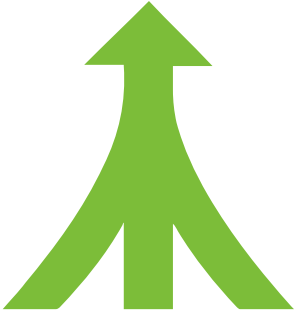


Establish a policy management organization structure with clear authority for identifying and creating policies

Determine what policies are required:

- ✓ Identify policies required by law and regulation and map each policy to the legal requirements it addresses, which may be more than one
- ✓ Determine what additional policies are desired
- ✓ Determine which types of policies must apply to vendors or partners and in what circumstances
- ✓ Determine gaps, redundancies, overlaps in existing policies
- ✓ Establish Policy Owners
- ✓ Establish methodology and triggers to update policies and keep current
- ✓ Create policy template

Federated Policy Management Governance Structure



An integrated approach that balances policy management centralization with distributed participation and collaboration

Looks holistically at policy landscape to ensure policy complies with:

- Organization's broad approach to policies & procedures
- All relevant laws and regulations
- Top of structure is Policy Management Office (PMO)
- Headed by Policy Program Manager (PPM)
- May include team of writers & analysts to guide Policy Owners

Advantages of this approach:

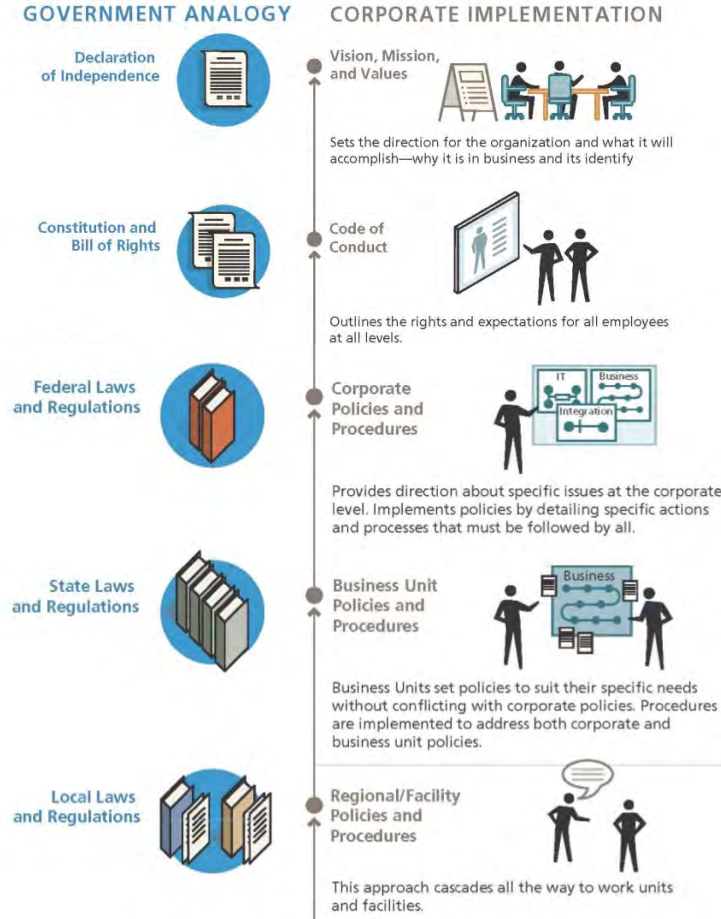
- Consistency
- Productivity
- Adherence to Metapolicy requirements & templates
- Referential integrity & adherence to governance principles

Federated Policy Management Governance Analogy



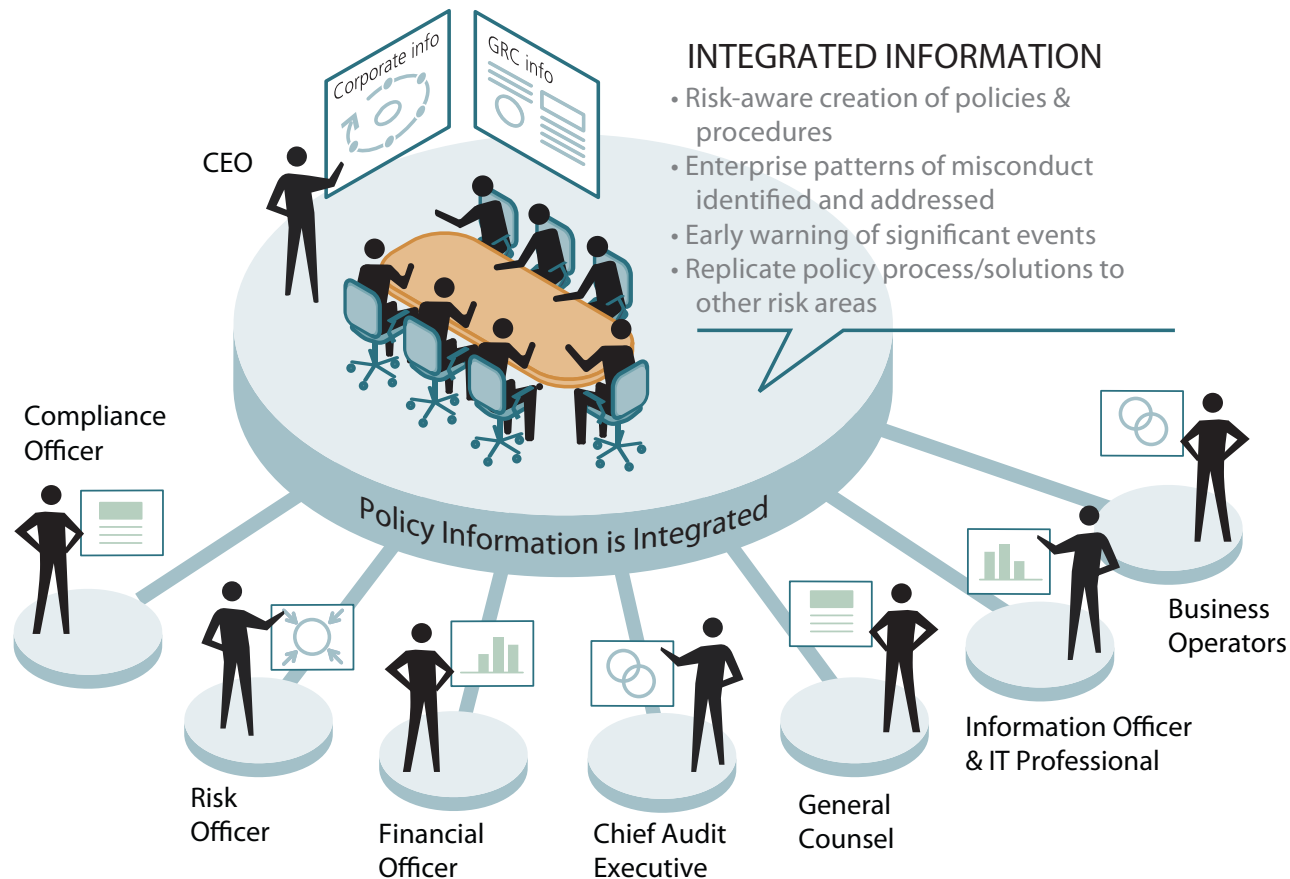
Policy management is done in layers

- ✓ Each layer can operate by a committee
- ✓ Each layer needs to conform to the policy management lifecycle
- ✓ Each layer must not conflict with the layer(s) above it



Herding Cats – Getting Everyone Working Together

- Who currently owns which policies?
- How do we prioritize policies?
- How are resources currently aligned to address policies?
- Is every risk area covered?
- Is there duplication?
- Are we relying too much on reactive response versus proactive prevention?
- Are we doing policy assessments?
- What techniques are being used?
- How do we prioritize risk? Is it viewed across the enterprise or in a manner?
- Who is writing the policies?
- Who is implementing the policies?
- Who is conducting the training?
- Is any of this work coordinated?
- How much burden are we putting on the business with information requests?



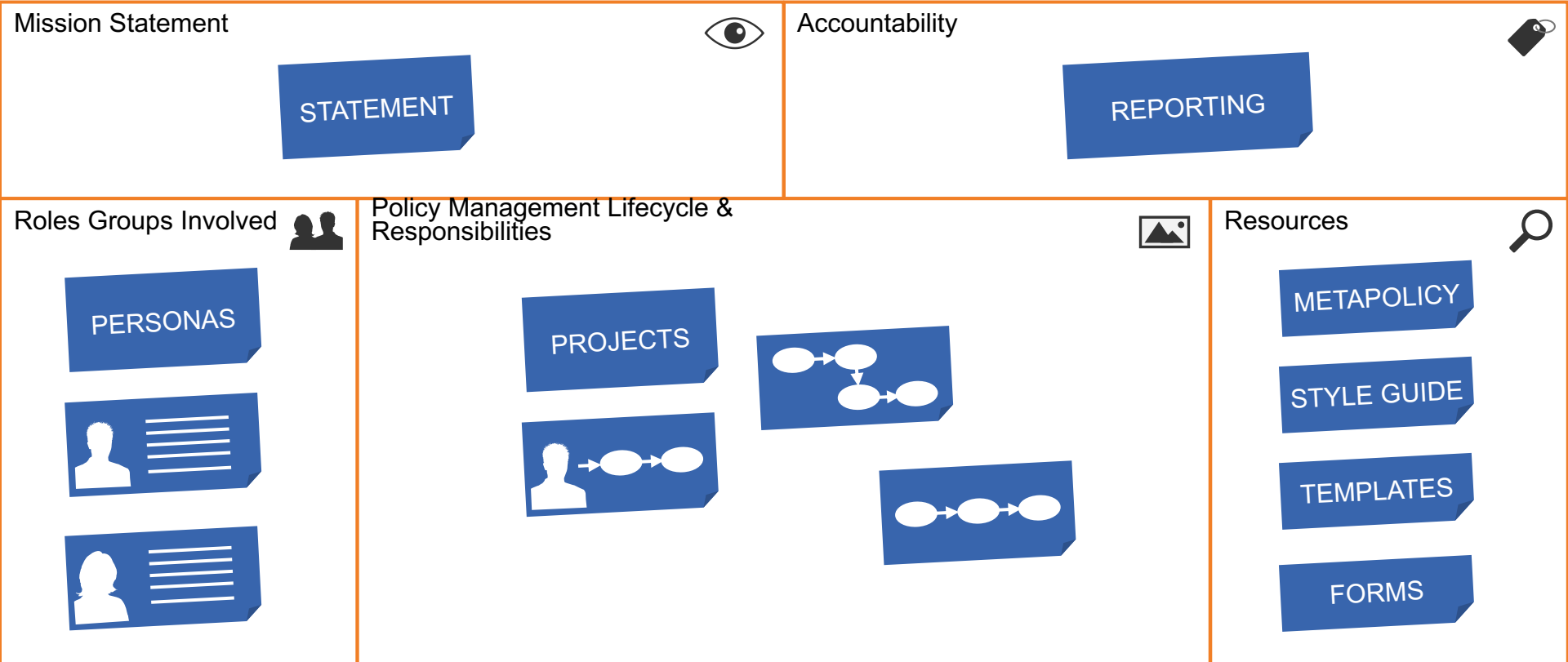
Design a Suitable & Scalable System



A SUITABLE AND SCALABLE SYSTEM

The key roles in the policy management program will be designed differently in each organization depending on size, nature of business and scope of policies. Some may combine author and owner roles; others may use a team to draft key policies; a few might have a team of assistant policy program managers and one or more policy review and approval committees.

Policy Management Charter



STEERING COMMITTEE

The policy steering committee represents departments or business units from across the organization and has the mission of establishing agreement about how policies are managed. The steering committee acts as the governing body for the policy management program, and should approve the templates, guidance and procedures developed by the policy program manager; then meet periodically to review and revise any basic structures of the program in light of changes in the business or operating environment.



PROGRAM MANAGER

Manages the policy development and approval process and may be responsible for the following tasks: guide policy owners and developers through the review and approval process; oversee policy approval committees; chair and facilitate the policy steering committee meetings; ensure the review and edit of all policies in a consistent format.



POLICY OWNER

Every policy needs to have an owner who must ensure that the policy remains accurate and relevant, is appropriately communicated, and continues to serve the purpose for which it was established. The policy owner evaluates changes in the underlying requirement or need for the policy and also determine if the policy needs to be edited or retired when there are changes in legal or other requirements, business operations, or risk profile of the organization.



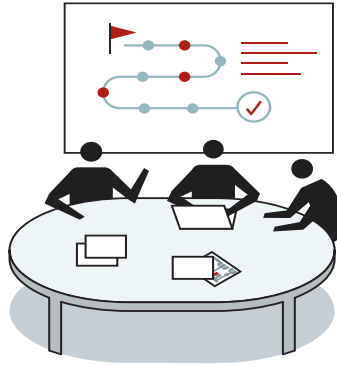
POLICY AUTHOR

The policy author drafts policies using the official templates; and works with the policy manager and owner to assure the policy meets the requirements of the style guide and established development process, as well as satisfying the purpose established when the need for the policy was identified.



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series

Roles & Responsibilities: Policy Steering Committee



The Policy Steering Committee (PSC) consists of line managers & subject matter experts representing business functions (e.g., HR, Legal, Risk, IT) across the organization.

The PSC primary responsibilities are to:

- Ensure policies and standards are aligned across the enterprise
- Review and approve new and updated policies and standards within Metapolicy scope (broad application and implication)
- Represent their business unit on issues brought before the PSC
- Conduct periodic review of policies and standards
- Provide guidance on communication, training, and enforcement of policies and standards
- Review escalated compliance issues
- Provide clear authority for policy and standard approval to:
 - reduce confusion
 - reinforce business accountability
 - increase enforceability

Roles & Responsibilities: Policy Management Office



The PMO generally does not make or write policy, except as related to the internal governance process. Its primary responsibilities are to:

- Advise policy owners and developers on format and wording of policies and the policy framework
- Facilitate the development of key policies and procedures
- Manage comprehensive submission and review process, with common definitions, templates, and formats
- Edit policies and standards with broad application before submission to the PGC
- Maintain one central repository for all enterprise-wide policies

Roles & Responsibilities: Policy Program Manager



The Policy Program Manager directs PMO and supports the PSC to:

- Review & edit policies before submission to PSC to ensure they:
 - Are written in a format consistent with approved templates and style guide
 - Are referentially consistent with other policies in the organization's portfolio
 - Comply with organization's governance principles
 - Are linked to applicable external laws and regulations (aka authoritative sources)
 - Have implementation plans for enforcement and communication
 - Have Executive and Legal buy-in
 - Guide Policy Owners through PSC review & approval process
 - Post approved policies to the central repository (system of record)
 - Chair, or assist PSC chair in facilitating PSC meetings
- Drive adherence to the Metapolicy
- Schedule & coordinate PSG meetings, including pre- and post-review meetings
- Prepare and distribute advance materials for PSC meetings
- Take minutes of PSC meetings

Roles & Responsibilities: Policy Owner & Policy Author



The Policy Owner's primary responsibilities are to:

- Assess need for new policy or modification to existing one
- Manage authoring and maintenance of policies
- Ensure content of policies is accurate and current
- Implement policies, e.g., train staff and promote awareness
- Periodically review policies; determine need for updates or retirement
- Decide outcome of disputes or determine resolution process

The Policy Owner may delegate any of the above responsibilities to another individual but ultimately retains accountability for assuring these duties are performed.



The Policy Author may writes the policy and is responsible to:

- Draft policies and related standards, procedures, and guidelines, using the official PMO templates
- Work with PPM and Owner to ensure policies meet requirements of the Metapolicy

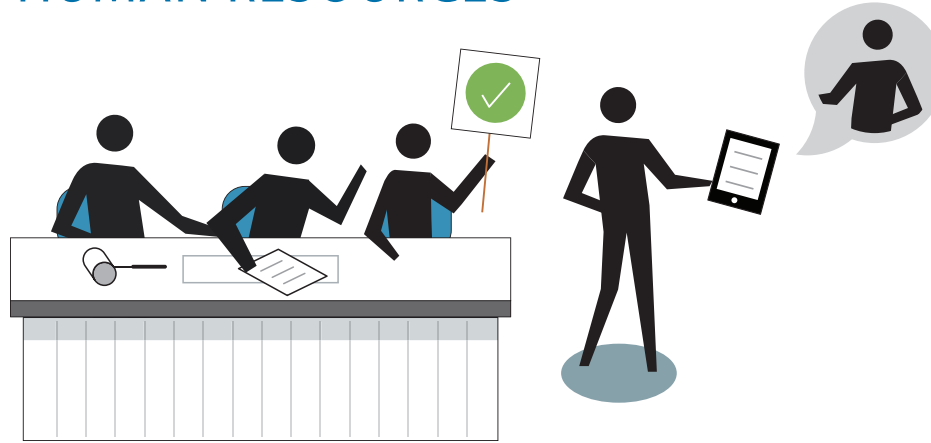
COMPLIANCE



The compliance department provides oversight and accountability by ensuring that policies are followed. Compliance monitors for actions of non-compliance and oversees action plans to correct them.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series

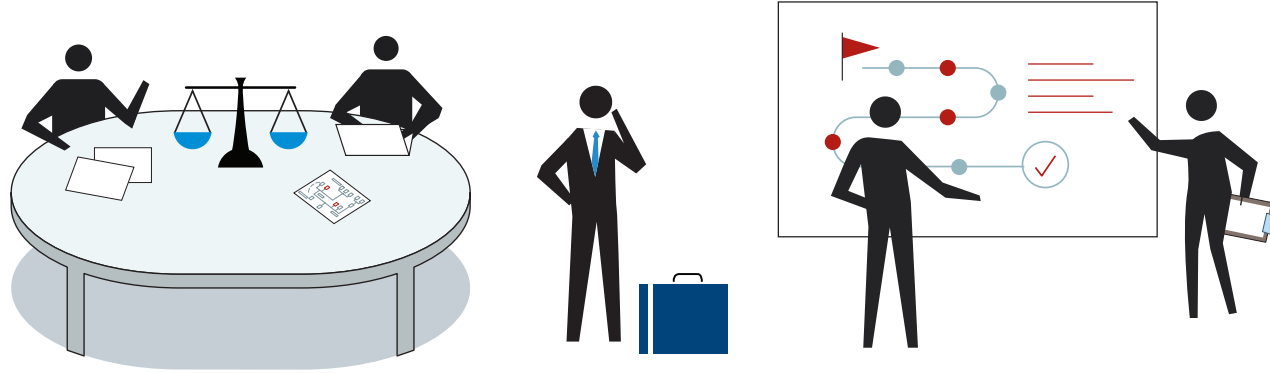
HUMAN RESOURCES



HR professionals not only ensure that policy adherence is covered in employee training and communication programs, but also that compliance is included in job descriptions, annual reviews and performance evaluations.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series

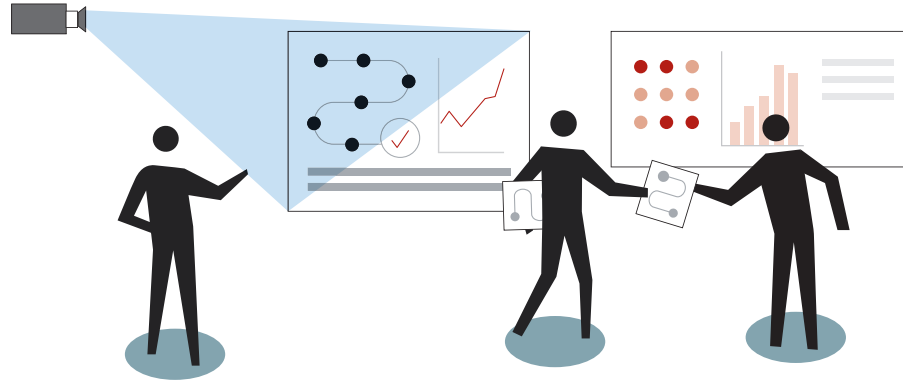
LEGAL



Legal provides regulatory guidance to the organization and ensures that incidents are investigated and resolved in a way that reduces risk and liability to the organization.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series

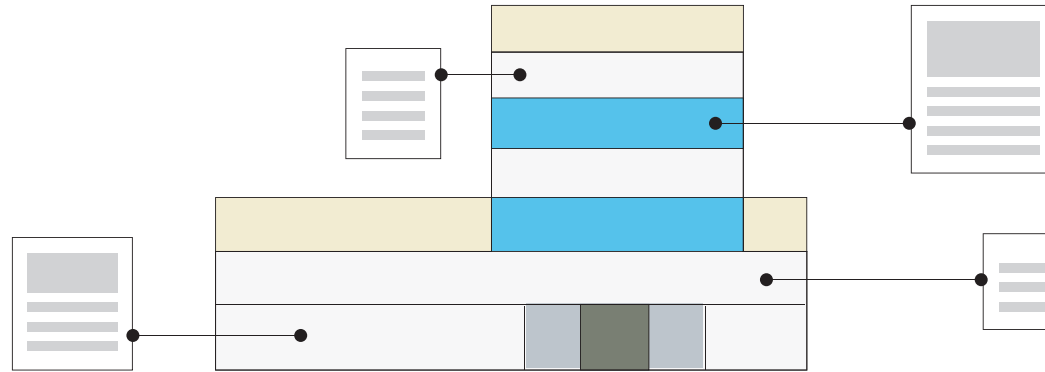
OPERATIONS



Policies are lived out in business operations and processes – it's where the 'rubber meets the road' in aligning the existence of policies with everyday organization behavior. Effective policies protect an organization and its operations without unnecessarily inhibiting them.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series

INTERNAL AUDIT



Internal Audit provides independent and objective assurance that policies are followed across the organization. Operational audits routinely include policy and policy conformance.

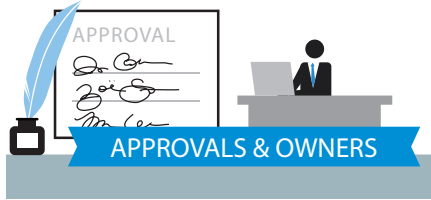
Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series



INVESTIGATIONS & REPORTING

Investigations, and related systems such as hotlines, provide insights into whether policies are being enforced and show that the organization takes policies seriously. Insight from investigations can tell us how policies are understood and operating.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Policy Management Illustrated Series



Existing Committees

- Multiple committees may have delegated authority to approve designated policies
- For example: Corporate Risk Committee may be delegated authority to approve Risk Management Policy
- Should have Charter that clearly defines policy approval responsibilities based on delegation of authority from CEO or Board
- Committee may have authority to delegate specific responsibilities to subcommittees or Senior Executives

Senior Executives

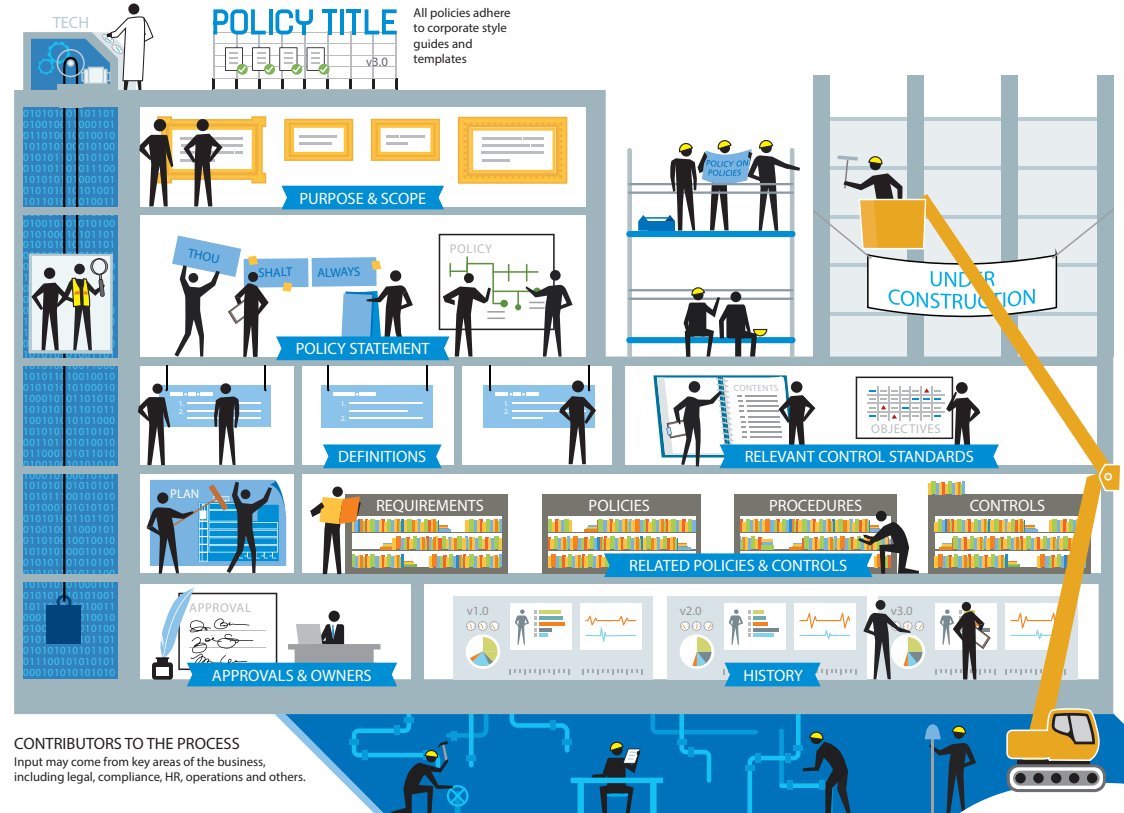
- C-Level executive of a function may have delegated authority to approve all policies owned by that function
- May have authority to delegate approval authority to line manager (e.g., CFO may delegate authority to approve Accounting Policies to Corporate Controller)

MetaPolicy: The Policy on Writing Policies



Start with a MetaPolicy that has **support from Executive Management**

- Brings integrity and value to policy management
- Provides accountability to policy management processes that are often scattered across the organization
- Enables policy management to work in harmony across organization functions delivering efficiency, effectiveness, and agility
- Well-governed and written policies improve performance, produce predictable outcomes, mitigate compliance risk & avoid incidents & loss



CONTRIBUTORS TO THE PROCESS
Input may come from key areas of the business,
including legal, compliance, HR, operations and others.

MetaPolicy – the “Policy on Policies”

Core components of MetaPolicy include:

- ✓ Roles, responsibilities and accountabilities
- ✓ Scope of what is governed by MetaPolicy
- ✓ Definitions of governance documents and resources.
- ✓ Structure and content
- ✓ Format & style requirements
- ✓ Use of templates
- ✓ Requirements for central policy repository
- ✓ Policy governance rules for creation, approval, retirement, updating/maintenance, and exceptions
- ✓ Assurance methodologies

Other Policy Resources

Core components of supporting policy resources include:

- ✓ Style guide
- ✓ Document templates
- ✓ Implementation plan template
- ✓ Executive summary template
- ✓ Exception/exemption request template

Policy

- Provides “WHY”
- High level and strategic
- Sets tone, context, and/or intent
- Relatively short by nature
- Changes infrequently

Standard

- Provides “WHAT”
- Specifies parameters of how to adhere to policy
- More specific
- Lengthier than policy
- Defines how to measure compliance
- Changes more frequently than policy

Governance Documents

- Provides “HOW TO” of policies and standards
- Guides implementation
- Audience specific and detailed
- Varies by department, process or technology
- Provides instructions for compliance to standard or policy
- Changes more frequently than standard and policy as business needs or obligations change

- “THOU SHOULD” instead of “THOU SHALT”
- Permissive by nature
- Not mandatory

- Provides framework of guidance where policies, standards and procedures do not govern

Procedure

Guideline

MetaPolicy: Guides the Consistency & Usefulness of Policies

IMPORTANT DESIGN CONSIDERATIONS

1. **CONSISTENCY.** There needs to be a common taxonomy and process for designing and developing policies and procedures; and a process for subordinate organizational units to provide input.
2. **ACCESSIBILITY** The right people need to have easy access to the right policies at the right time.
3. **INTEGRITY** There should be a single authoritative copy of each policy. Multiple copies and duplicates can easily get out of sync.
4. **USABILITY** The workforce must be able to understand and implement policies. Legalese should be avoided.
5. **MEASURABILITY & ENFORCEMENT** Compliance with policies should be evaluated and measured. Policies without monitoring or enforcement are empty words. Consistent enforcement is critical as it sends a signal to the workforce (and government) that policies actually mean something.



The policies and procedures align with my job and are written in a language I can understand. Consistently used terms, formatting, and the level of detail help me produce the expected results.

COMMON DIALOGUE

MetaPolicy Defines Policy Structure & Required Components

Section	Policy	Standard	Procedure	Guideline
Introduction	Required	Required	Required	Required
Purpose and Scope	Required	Required	Required	Required
Definitions	Optional	Optional	Optional	Optional
Policy Statement	Required	N/A	N/A	N/A
Requirements	N/A	Required	N/A	N/A
Procedures	N/A	N/A	Required	N/A
Guidelines	N/A	N/A	N/A	Required
Associated Governance Tools	Required	Required	Required	Required
Revision History	Required	Required	Required	Required

MetaPolicy Defines Policy Structure & Required Components

Introduction

- the context and driving need for the governance tool; and
- what law, regulation, contractual agreement, or higher-level governance tool is driving the need for this tool.

Purpose and Scope

- why the governance tool is needed;
- why it must be documented;
- what its scope is; and
- who is accountable to follow it (e.g., employees in specific countries or business units/departments, contingent workers, third parties).

Definitions

- lists words that may be unique to governance tool or topic and provides definitions
- in governance tools that have a lot of unique words, or that share words with other governance tools, may include reference directing reader to special glossary (see Definitions section above for language to be used)

Policy Statement

- addresses why the policy is needed;
- is high level and strategic;
- sets the tone, context or intent; and
- will be changed infrequently.

Requirements

- addresses what needs to be done;
- provides the parameters of how to adhere to the policy it supports;
- covers a specific area of activity or business; and
- can be lengthy, as it spells out the first level of how to measure compliance.

Procedures

- defines a particular course of action or way to proceed in support of a policy and/or standard;
- addresses how to do what needs to be done;
- is very specific and detailed;
- is audience specific and may vary from department to department; and
- provides exact instructions that will ensure compliance with a given standard.

Guidelines

- is a general statement or recommendation on how to achieve objectives;
- is permissive but not mandatory; and
- may provide a framework for the development of policies, standards or procedures.

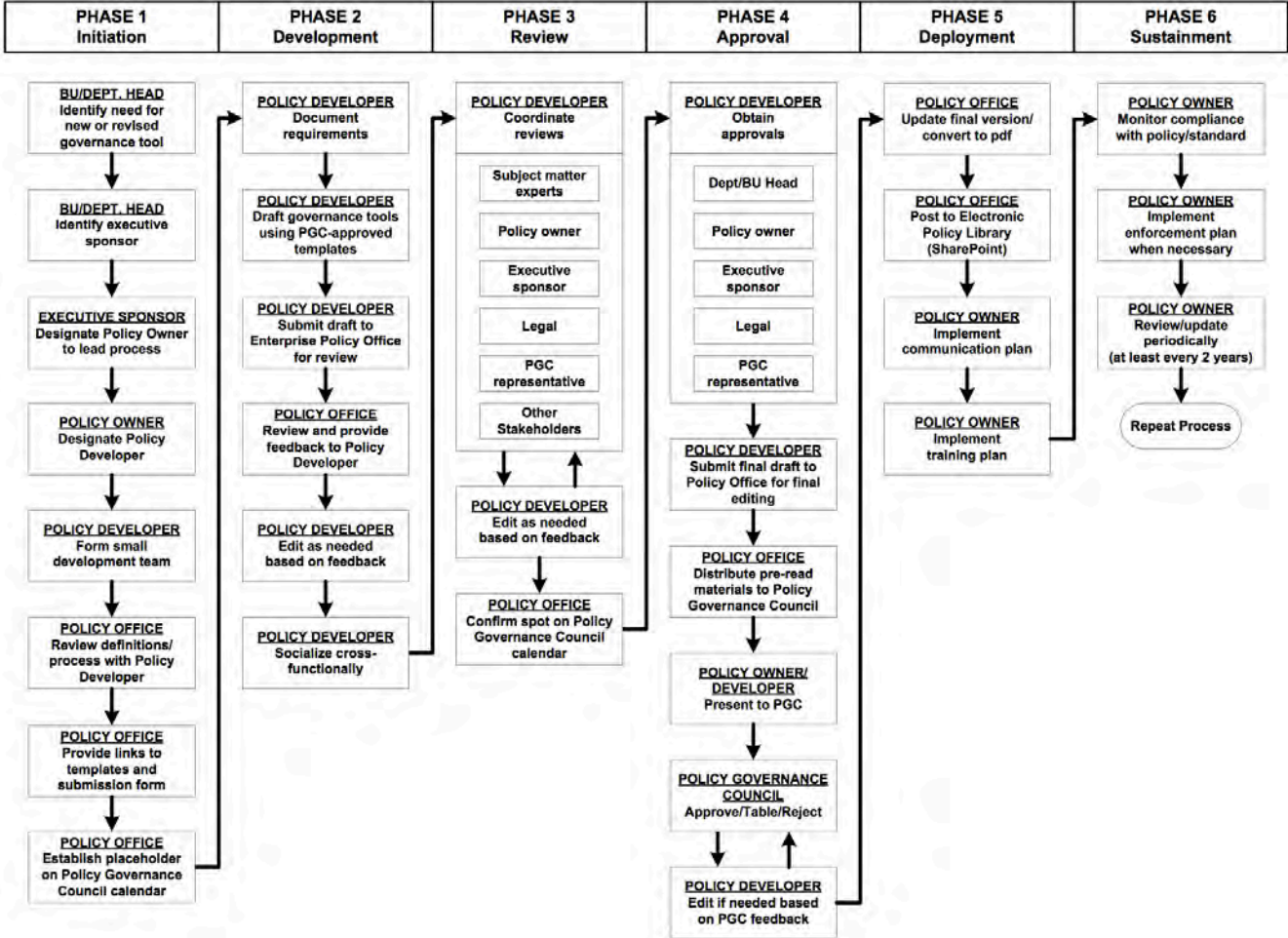
Associated Governance Tools

- identifies by title any other governance tools that are impacted by or that may impact this governance tool; at a minimum, this section should list all related policies, standards, procedures and guidelines for a particular policy package.

Revision History

- identifies the dates when major revisions were made to the governance tool; at a minimum, a final approved version will include:
 - the date of the first draft (may be shown as a range, such as May-July 2008),
 - the date when the Legal review was completed,
 - the date when the review by the Enterprise Policy Office was completed, and
 - the date when it was approved by the Policy Governance Council.

MetaPolicy Process Example 1: Policy Development Process



Style Guide: Purpose of the Style Guide

Well written polices are. . .

- ✓ Clear
- ✓ Correct
- ✓ Complete
- ✓ Concise
- ✓ Courteous



Well written policies . . .

- ✓ Illustrate corporate culture
- ✓ Demonstrate professionalism
- ✓ Show the organizations cares
- ✓ Help avoid expensive mistakes
- ✓ Provide consistency across the organization



Policy writing that is wordy and confusing is damaging to the corporate image and costs time and money

Summary

This Guide provides you with simple yet comprehensive quick reference tools to understand the choices that Company has made to help you achieve consistency in language, style, and format of our corporate policies and procedures.

It intentionally does not cover every grammatical rule or situation that can arise as you write, but highlights the basic structure, language and definitions we consider most important to achieve a consistent look-and-feel among our publications.

The ultimate goal is to help you write reader-centered documents that drive the correct action.

Sample Structure

The Guide is broken into five main sections with specific reference purposes. It is not designed to be read as a book, but rather referenced to solve specific problems or answer specific questions:

- ❑ Section 1: Principles of Style for Policies, Procedures and Guidelines — This section introduces eight straightforward principles of good writing to help you produce clear, consistent, readable documents.
- ❑ Section 2: Formatting and Layout — This section summarizes the standards for headings, fonts, bulleted and numbered lists, tables and other layout elements.
- ❑ Section 3: Spelling, Punctuation and Grammar — This section is a quick reference to the most important rules. While not exhaustive, it covers the most common questions and also sets a specific style for Company documents. References to more comprehensive sources are given, in case you cannot find your answer here.
- ❑ Section 4: Commonly Misused Words — This section is a quick reference for resolving some of the most common wording questions you face when writing (e.g., Do I mean “affect” or “effect”?, “Do I need to use “its” or “it’s”?”).
- ❑ Section 5: Quick Reference Tables — This section contains reference lists for the capitalization and hyphenation of words that are often confusing. It also contains a list to answer the question, “Is this One Word or Two”?

Summary

To support policy owners and policy developers, the Enterprise Policy Office and the Policy Governance Council, requirements and guidelines for writing, communicating, training, and enforcing governance tools will be developed to increase consistency and clarity surrounding policies at Company.

These guidelines aim for consistency across the multiple departments and business units that write policies, standards, procedures and guidelines. The EPO will adhere to these guidelines when reviewing and editing any governance tool or supporting materials to be submitted to the PGC for review and/or approval.







Sample Structure

Instructions For Using Templates

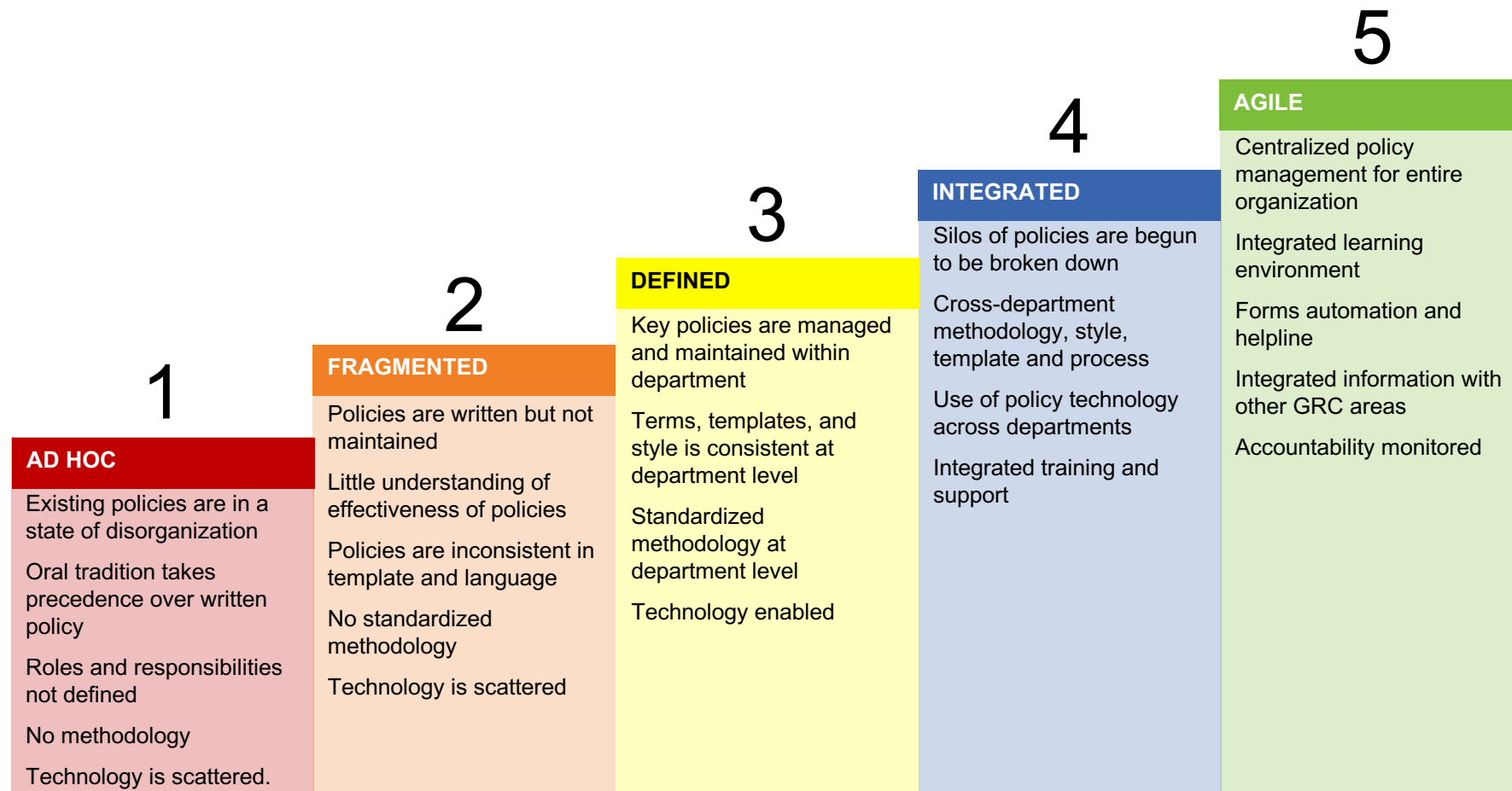
- Do not change the template margins, the formatting (e.g., font type/size, spacing) or the section titles (e.g., INTRODUCTION, PURPOSE AND SCOPE).
- Replace all verbiage between < > with correct language, including in headers and body.
- The templates have text boxes with explanatory information and guidance in yellow, green or red. Delete these text boxes before the you distribute the draft for review.
- In accordance with XYZ Company's style guide, only one space should be used after periods or colons.

- ✓ Fonts
- ✓ Margins And Alignment
- ✓ Titles Of Documents
- ✓ Style Conventions And Examples
- ✓ Acronyms and Abbreviations
- ✓ Active Voice, Use Of
- ✓ Capitalization
- ✓ Contractions
- ✓ Directives, Form Of
- ✓ Emphasis Techniques (Bolding, Italics, Underlining, And Quotation Marks)
- ✓ Forms Or Agreements
- ✓ Gender
- ✓ Language, Use of Imperative vs. Instructive
- ✓ Numbers And Units Of Measure
- ✓ Parallelism, Use Of
- ✓ Periods (Usage)
- ✓ Periods/Commas And Quotation Marks, Placement Of
- ✓ Plurals And Possessives
- ✓ Quotation Marks
- ✓ Semicolons Versus Dashes
- ✓ Spelling, Using U.S. Standards

Style Guide: Consistency in Language and What it Communicates

1 Structural Impact 	2 Paragraph Impact 	3 Sentence Impact 	4 Word Impact 	5 Punctuation Impact 	6 Story/Message Impact 
<ul style="list-style-type: none"> ▪ Frame the most important points ▪ Make points simple as possible, but not simpler. ▪ Use headings ▪ Format headings with an Arabic-numbered outline system <ul style="list-style-type: none"> ➢ Boldface large; boldface; boldface italic; italic ➢ Position headings flush left ➢ Put more white space above the heading than below 	<ul style="list-style-type: none"> ▪ Begin each paragraph with a topic sentence <ul style="list-style-type: none"> ➢ Don't end a paragraph with the next paragraph's topic ➢ But do bridge from one paragraph to another ▪ Connect sentences smoothly ▪ Provide signposts ▪ Break up long complex sentences. <ul style="list-style-type: none"> ➢ Average sentence length should be approximately 20 words ▪ Avoid tiresome repetitions 	<ul style="list-style-type: none"> ▪ Relax tone – avoid legalese ▪ Populate sentences – use names, personalize ▪ Use action verbs instead of be verbs ▪ Minimize the passive voice. ▪ Uncover buried verbs (such as those with –tion) ▪ Eliminate unnecessary prepositional phrases (such as those beginning with of) ▪ Don't separate a subject from a verb with a modifying phrase (if needed start with the modifier) ▪ Do not separate a verb from its object ▪ End your sentence with a punch ▪ Cut filler phrases such as there is and there are ▪ Cut unnecessary words ▪ Keep sentences to one main thought <ul style="list-style-type: none"> ➢ Combine only when it minimizes chopiness ▪ Use parallel constructions 	<ul style="list-style-type: none"> ▪ Replace boring phrases with snappy ones that spark interest ▪ State your ideas freshly ▪ Utilize distinctive nouns and verbs – minimize adjectives and adverbs ▪ Save syllables – the fewer the better ▪ Simplify wordy prepositions <ul style="list-style-type: none"> ➢ With respect to, as to, in order to ▪ Do not use However to start a sentence – But is better ▪ Use only recognized symbols and abbreviations ▪ Shun sexist language but do it invisibly ▪ Strike out and replace fancy words ▪ Challenge vague words ▪ Shun vogue words ▪ Toss out timid phrases 	<ul style="list-style-type: none"> ▪ Use dashes – not parentheses – to highlight interruptive phrases ▪ Be stingy with hyphens ▪ Use bullets ▪ Use serial comma 	<ul style="list-style-type: none"> ▪ Show, don't tell ▪ Say it well and say it emphatically ▪ Visualize the reader ▪ Do not write a sentence that you would never speak ▪ State squarely what you want the reader is to do

GRC 20/20'S Policy Management Maturity Model



Style Guide: Governs the Writing & Editing Process

Tips for the Policy writing process . . .

- Plan your writing by breaking it up in stages
- Start with brainstorming
- Develop the architecture
 - Define the structure
 - State the issues
 - Outline
- Write a draft straight through
- Proof after letting it sit for a bit
- Good writing requires multiple drafts
- Always read through what you've written before you send it
- Read it out loud so that you read what you've written, not what you think you've written
- If in doubt, ask for help
- Don't rely on spell-check for everything

Content Editing

- Verify accuracy of information
- Check for bias and use of language
- Audience
- Logic & consistency
- Clarity, consistency, & brevity

Language Editing

Punctuation
Grammar
Mechanics

Final Editing

- Compliance to style guide
- Formatting
- Consistency in language and style
- Factual check
- Integration with other policies & procedures



Workshop Activity

Our Agenda . . .

1) PART 1: Policy by Design

Why Policies Matter

2) PART 2: Policy Governance

Blueprint for Effective Policy Management

3) **PART 3: Policy Management Lifecycle**

Managing Policies from Creation to Dissolution

4) PART 4: Policy Management Architecture

Enabling Information & Technology Management of Policies

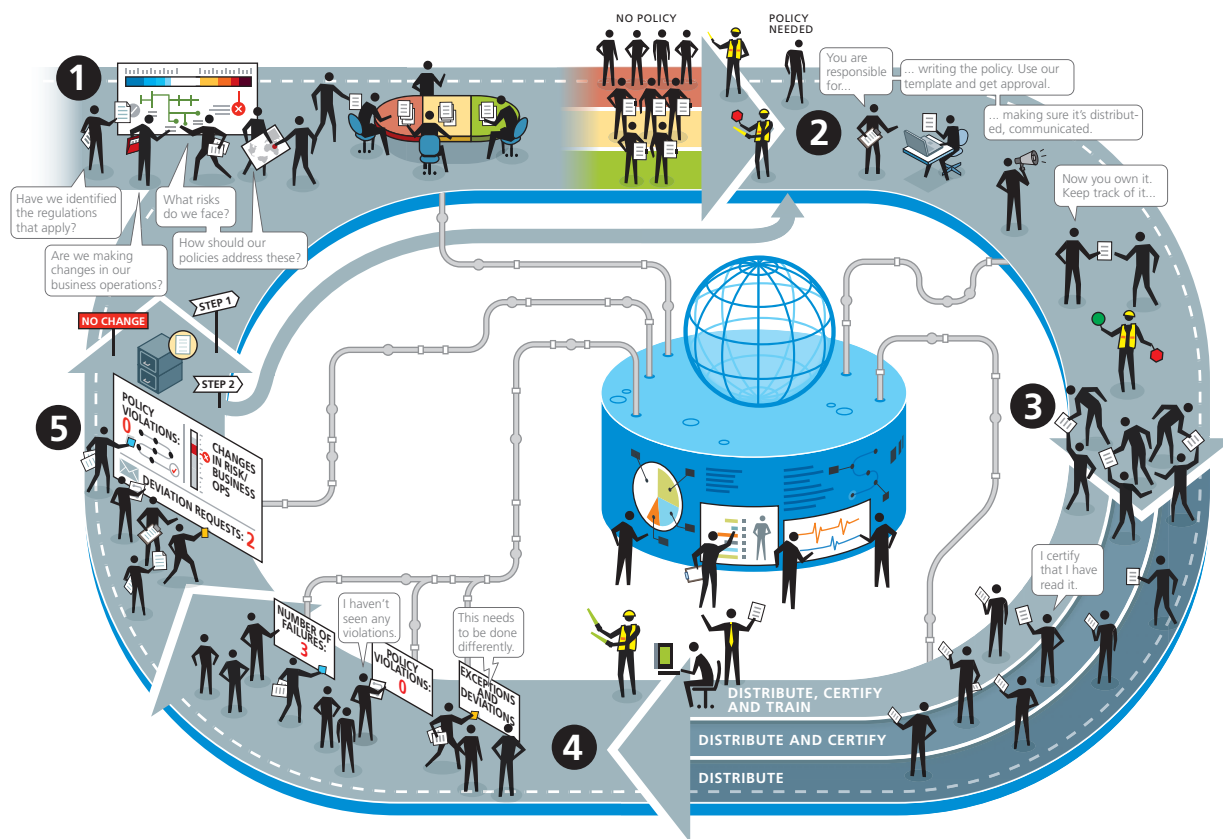
PART 3

Policy Management Lifecycle: Managing Policies from Creation to Dissolution

Learning Objectives . . .

- ❑ When to Write a Policy
Framework to determine need for a policy
- ❑ Policy Development & Approval
Policy authoring, review, editing, and approval
- ❑ Policy Communication
Policy awareness, communication, training and attestation
- ❑ Policy Monitoring
Managing exemptions, exceptions, and conformance to policies
- ❑ Policy Metrics & Maintenance
Measuring Policy Effectiveness and Keeping Policies Current
- ❑ Interactive Group Discussions

GRC 20/20's Effective Policy Management Lifecycle



- 1 Determine Need
- 2 Develop & Approve
- 3 Communicate & Train
- 4 Monitor & Enforce
- 5 Measure & Maintain

When to Write a Policy



Is the policy required by law, regulation, contract, or other obligation?



Does the organization's size, business, industry, or workforce justify having this policy?



Will the policy enhance business performance, improve productivity, effectiveness, or efficiency?



Will the policy enhance employee or customer experience?



Is the policy just creating another layer of bureaucracy?



Will the policy be consistent with the organizational culture?



How did we handle this without a policy?



Can an existing policy be updated to address the necessary items, eliminating the need to write a new policy?



Is the time and money required to administer the policy reasonable in relation to the benefits obtained?



Do we have the mechanisms to communicate and enforce the policy?

1 Determine Need

2 Develop & Approve

3 Communicate & Train

4 Monitor & Enforce

5 Measure & Maintain

When to Write a Policy

With the approval of the executive leadership of the enterprise, a business unit or department head may use policy-making as a tool for establishing requirements of the enterprise that relate to his or her area of responsibility. In this way, enterprise policies connect the XYZ Company's Mission Statement and Guiding Principles to individual conduct; clarify expectations; support compliance with law, regulations and contractual obligations; mitigate XYZ Company risk; and enhance productivity and efficiency in enterprise operations.

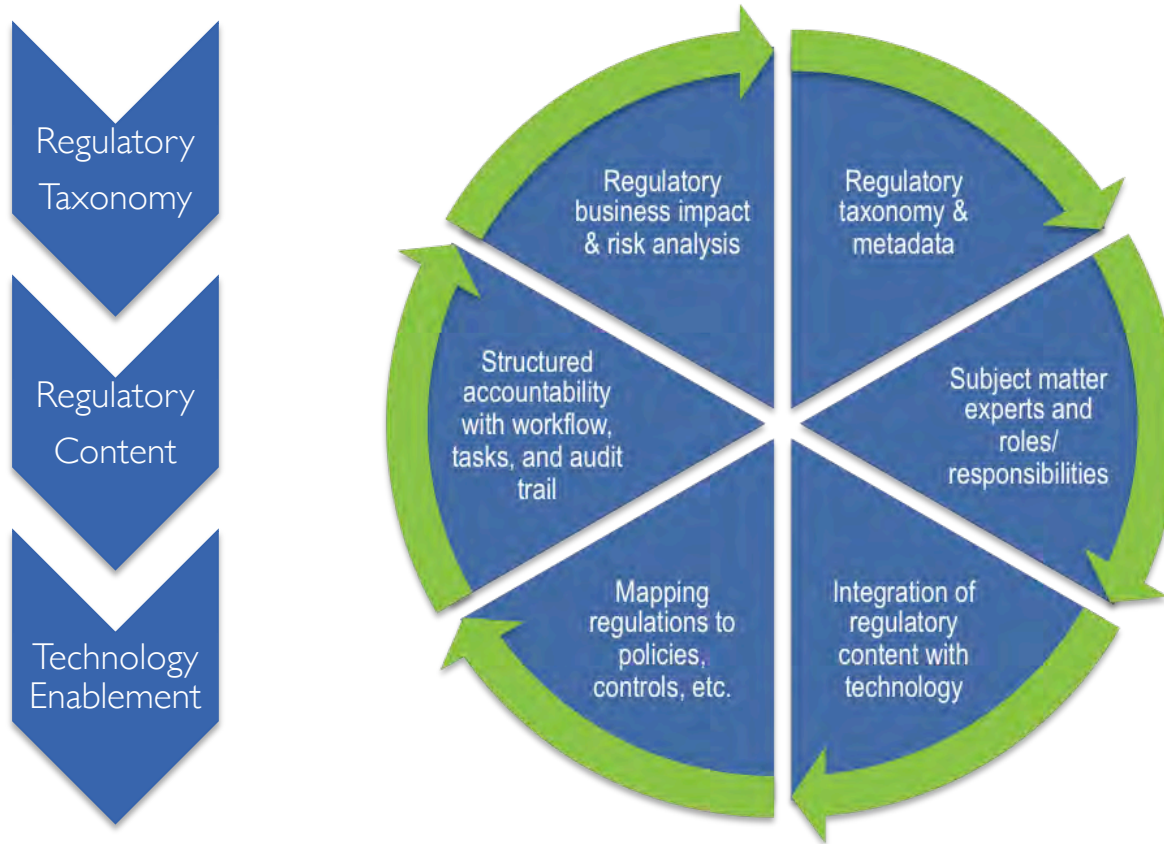
The Policy Developer of a governance tool should focus on creating a tool that provides both clear operating structures for employees and enough latitude to achieve business objectives. Factors to be considered when prioritizing and developing governance tools include:

- level of risk;
- impact on bottom line;
- weakness control;
- revenue leakage; and
- cost management.

The following questions should be addressed:

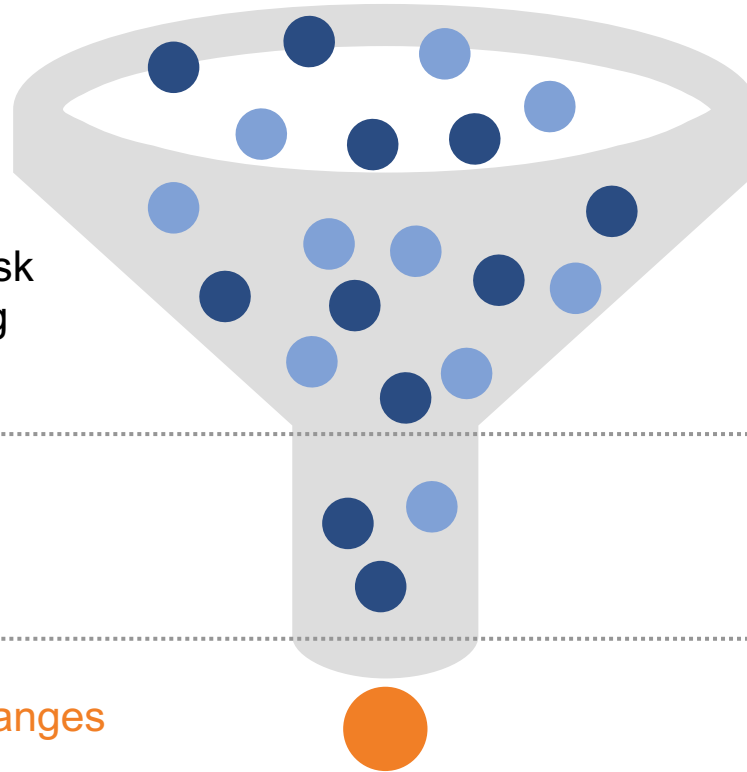
- Is the governance tool required by law or contract?
- Does XYZ Company's size, business or workforce justify having this governance tool?
- Will the governance tool enhance business performance; improve productivity, effectiveness, or efficiency; or enhance the employee or customer experience, or is it just creating another layer of bureaucracy?
- Does enforcing this governance tool accomplish corporate goals?
- Will the governance tool be consistent with XYZ Company management/business philosophy?
- What has been done in the past to resolve issues related to this governance tool?
- Have other options been considered?
- Is there an existing governance tool that can be updated to address these topics, eliminating the need to write a new governance tool?
- Is it possible to simplify or integrate existing procedures instead?
- Can this governance tool strike a proper balance between management flexibility and fairness to employees?
- Is the time and money required to administer this governance tool reasonable in relation to the benefits obtained?
- Will this governance tool require a significant revision in the near future?

Developing a Framework to Manage Policies in Context of Regulatory Change

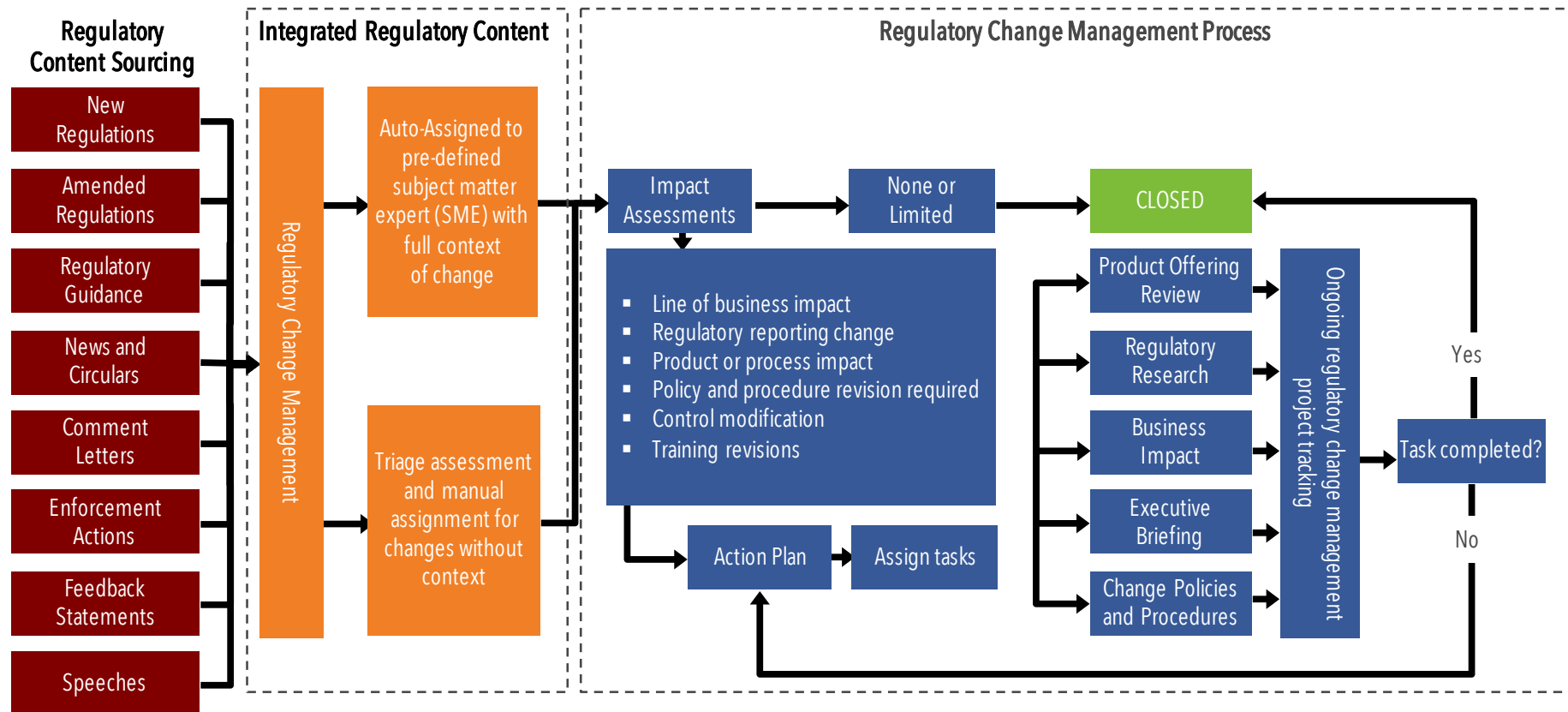


Filtering Changes to Identify Synergies and Change Needed

- 1 Understand organization, regulatory, and risk change impacting policies
- 2 Determine synergies
- 3 Identify policy changes

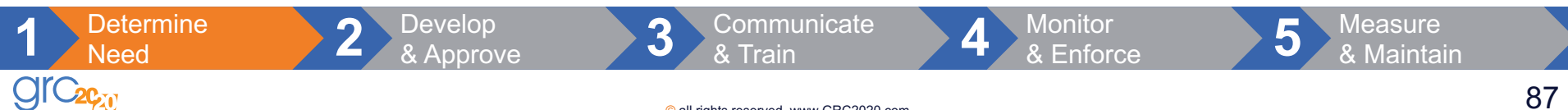


Regulatory Change Management Process

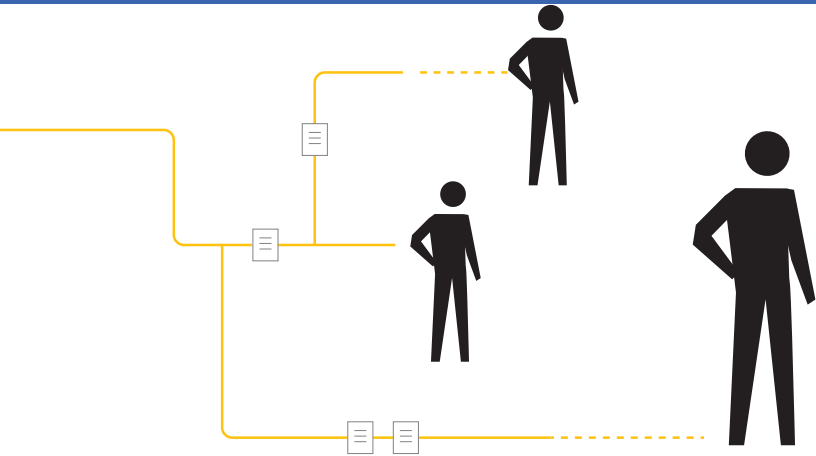


Keys to Success to Manage Change and Policies

- 🔑 Identify content sources to keep current on regulatory change
- 🔑 Develop a regulatory obligation taxonomy that establishes the categories of change that impact the organization
- 🔑 Assign subject matter experts (SME) to each category of the taxonomy who are responsible to track changes and their impact on the organization
- 🔑 Map risks, policies, procedures, reporting, assessments, training, and other GRC items to the taxonomy so that when a change is identified the SME knows what to evaluate
- 🔑 Use technology to route changes to the SME and track accountability and follow-through
- 🔑 Implement a standard business impact analysis process to determine the degree a change impacts the organization
- 🔑 Integrate the change monitoring process and technology with policy management and enterprise GRC process and technology to integrated flow of information and analysis and ensure that nothing slips through the cracks



1) Route Change to the Write Subject Matter Expert

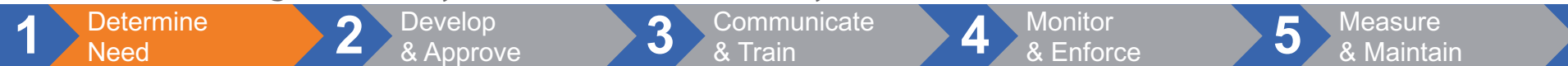


"SOURCING TEAM" OF SMES

EXPERTS IN THE BUSINESS

1 ROUTE INFORMATION

The change is logged to the proper subject matter expert, who vets the change, and may route it to further analysis.



Analyze the Change in Context of Business and Determine Action

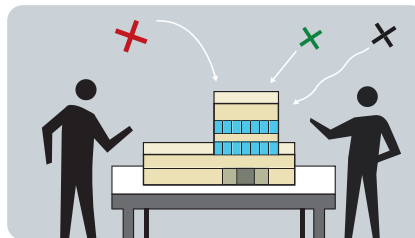
2 BUSINESS ANALYSIS

The expert and the business conduct an impact analysis to determine how the change impacts the organization and its policies and controls.

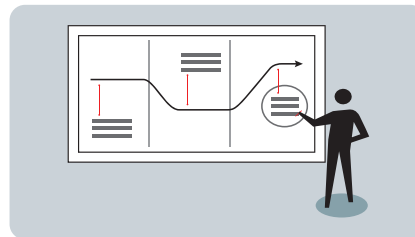
This analysis includes multiple parts that focus on risk, company history and overall industry practices.

As well as review of existing policies, current controls, processes/ infrastructure and current capabilities.

ANALYZE RISKS



UNDERSTAND HISTORY



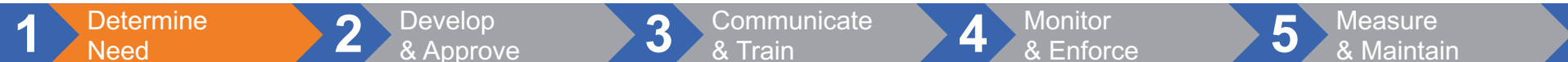
REVIEW EXISTING POLICIES



3 DETERMINE ACTION

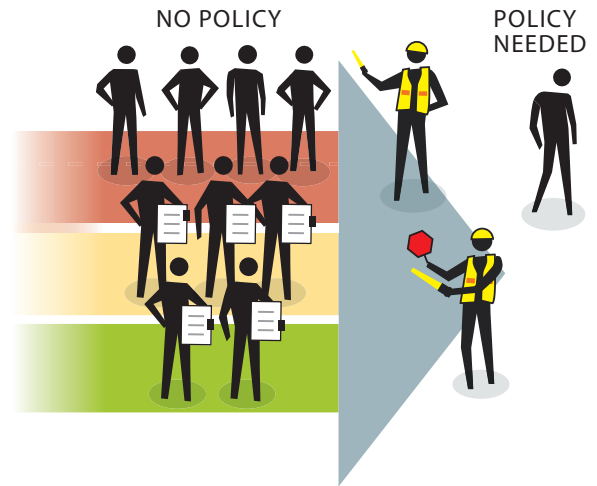
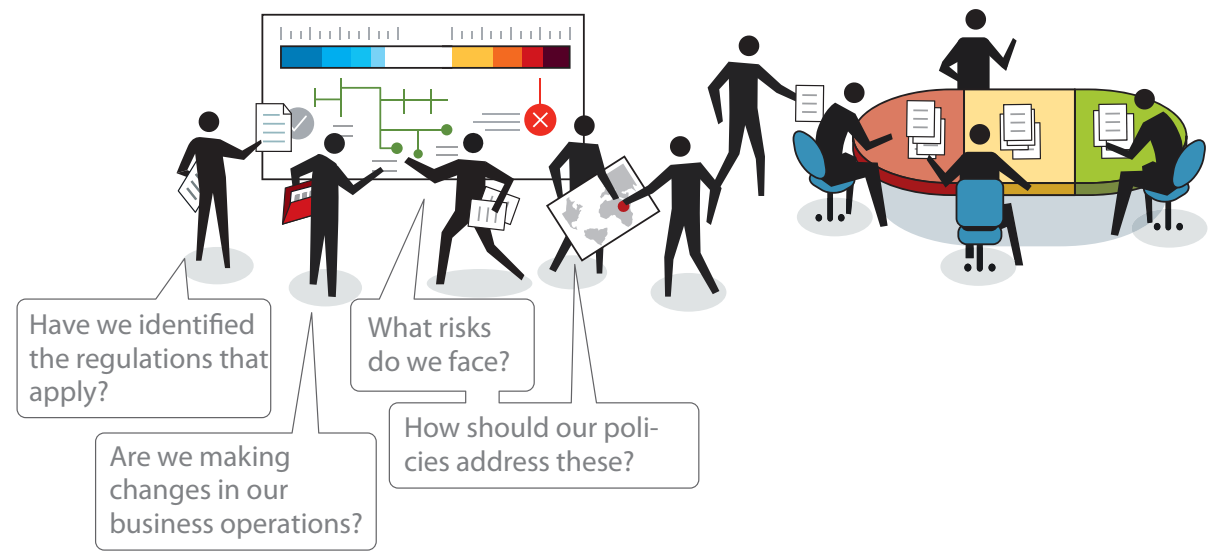
Determine if a new policy should be written, an existing policy updated, or if no change is required and identify projects to bring the organization in line with updated or new policies.

contact Carole S. Switzer cswitzer@ocag.org for comments, reprints or licensing requests
©2012 OCAG visit www.ocag.org for other installments in the Anti-Corruption Illustrated Series



Determine Policies that Need to be Changed

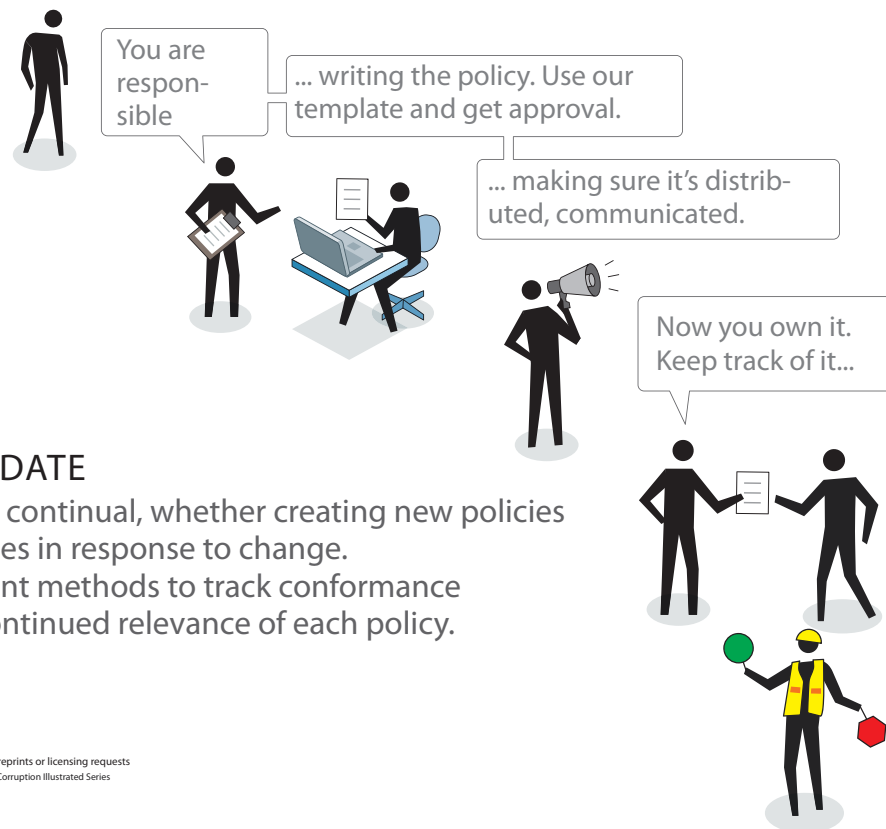
Only create policies when they define organizational values or mandates, address regulatory obligations, or manage potential risk or liability. Too many policies burden the organization and too few expose it to unnecessary risk. To identify when a policy is needed, monitor drivers and changes.



contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series

- 1 Determine Need
- 2 Develop & Approve
- 3 Communicate & Train
- 4 Monitor & Enforce
- 5 Measure & Maintain

Assign Policy Development Responsibilities

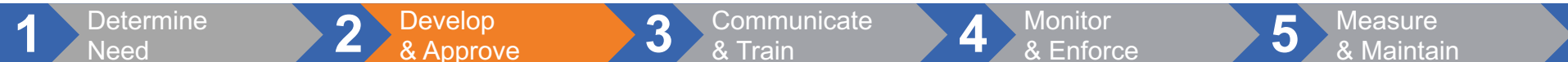


DEVELOP AND UPDATE

Policy development is continual, whether creating new policies or revising existing ones in response to change.

Establish and document methods to track conformance with the policy and continued relevance of each policy.

contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series



Draft the Policy, Review It, Edit It, and Approve It

Approved policy development process is the foundation for every policy.



1. Establish a 'policy on policies' that sets templates, style guides and development process.

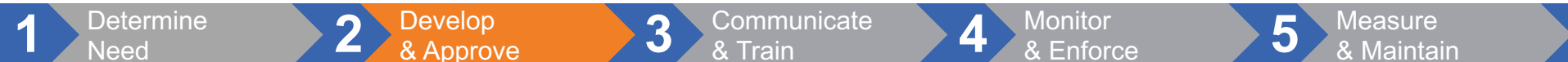
2. Determine need for new or amended policy based on analysis of changes in regulation, business operation and risk profile.



3. Draft policy with input from relevant subject matter experts.

4. Review new or edited policy to ensure compliance with 'policy on policies'.

5. Obtain final approval and sign off.



Policy Implementation Plan Template Sections

1

Implementation Plan

Key topics covered include description of impacted stakeholders; identification of cross-operational implementation team; barriers to implementation; assessment of affect on other policies, procedures, and processes; other collateral impacted; implementation risks and mitigations; and major implementation tasks, responsibilities and target dates.

2

Communication Plan

This identifies who needs to be informed, when, and how. Tell the policy story in context of role and operations. Communicate value and importance of policy, significant changes affecting each audience, upcoming challenges, and support tools available. If no communication is required, provide brief explanation of why no communication is warranted for this policy.

3

Training Plan

This identifies who needs what training, when they need to be trained and how training will be provided. If no training is required, provide brief explanation of why no training is warranted for this policy implementation.

4

Implementation Timeline

Provide implementation timeline, schedule, and tasks.

5

Approvals

Policy owner and policy approver sign off on policy implementation plan

6

Considerations Checklist

Identification of major implementation considerations and questions to aid the Policy Owner and Implementation Team in crafting strategies to deal with them, e.g.:

- Stakeholder Considerations
- Risk Management Considerations
- Communication Considerations

1

Determine
Need

2

Develop
& Approve

3

Communicate
& Train

4

Monitor
& Enforce

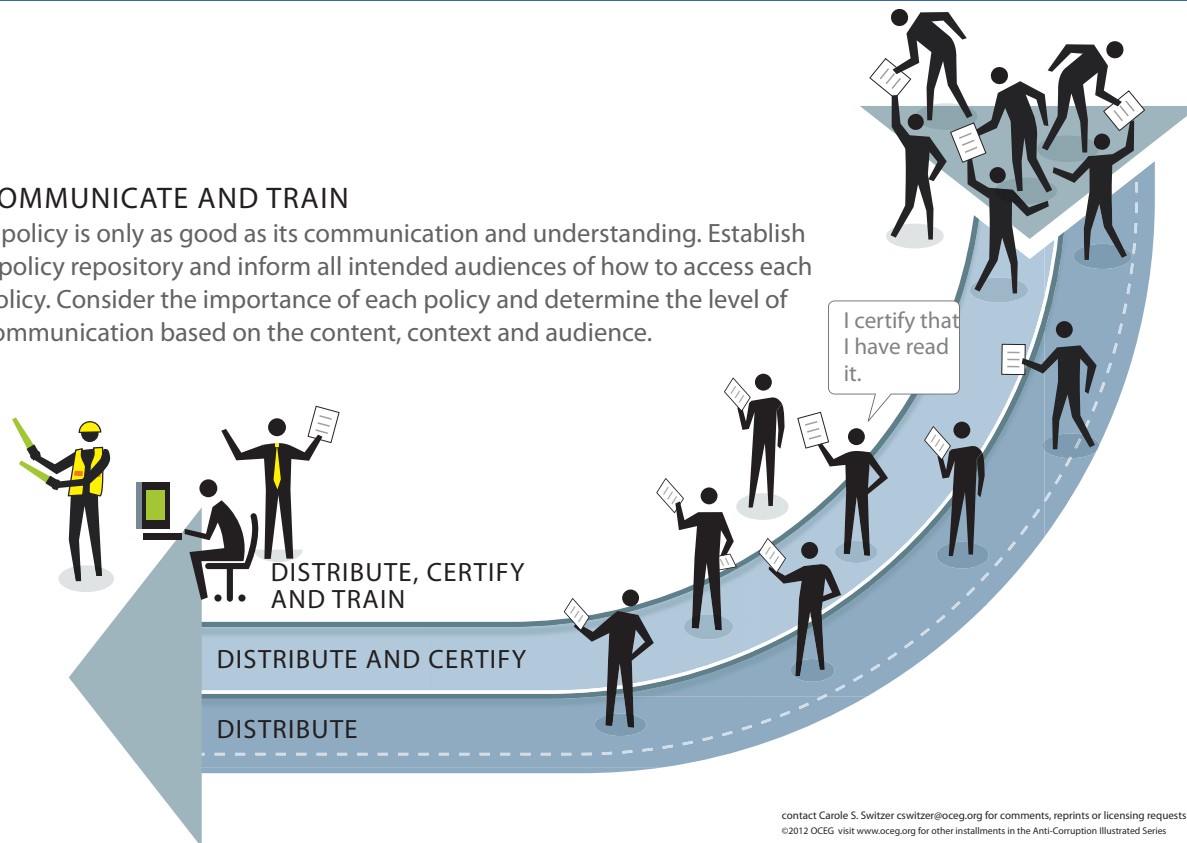
5

Measure
& Maintain

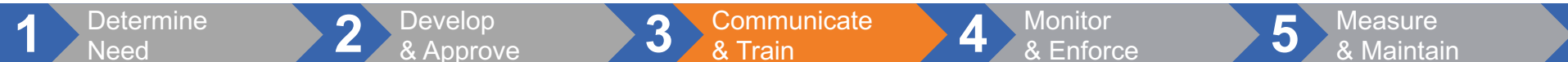
Now It is Necessary to Communicate the Policy

COMMUNICATE AND TRAIN

A policy is only as good as its communication and understanding. Establish a policy repository and inform all intended audiences of how to access each policy. Consider the importance of each policy and determine the level of communication based on the content, context and audience.



contact Carole S. Switzer cswitzer@ocec.org for comments, reprints or licensing requests
©2012 OCEG visit www.oceg.org for other installments in the Anti-Corruption Illustrated Series



Policy Pull and Policy Push Mechanisms

I'll check the gift policy to see if I'm at risk of violating it.



POLICY PULL

Methods for employees to find and understand a policy

- Allows employees to tag and organize policies
- Mobile technologies enable quick access
- Meta-data based policy search
- Context based help and FAQs
- Social features allow users to interact and share

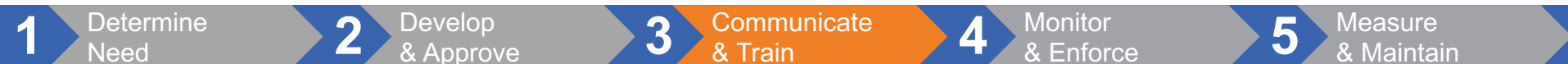
I'll send an alert out to the sales team to read and attest understanding of this new sales policy.



POLICY PUSH

Methods to push policies to employees to make them aware

- Changes in employee context pushes policy
- Maps policy to roles, processes and activities
- Monitors metrics on read and understood
- Multi-channel delivery (pop-up, IM, login)
- Measures reaction, questions and feedback



Best Practices to Make Policies Available and Increase Awareness

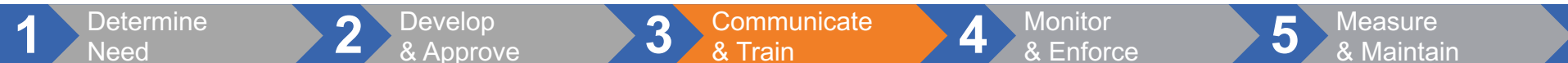
- 👍 Enable staff to log into a centralized policy repository to find all of the policies and procedures that relate to their role
- 👍 Write policies clearly in a consistent template and style that reflects the culture and tone of the organization
- 👍 Write policies so the intended audience can understand them
- 👍 Clearly communicate the process for acceptance and attestation and make it easy to accomplish
- 👍 Make it easy to ask for help and clarification on the policy
- 👍 Identify the policies that must have an interactive communication component in which the policy is explained to the individual, and that are integrated with the policy management system to enhance user experience, corporate value, and ease of use

Questions to Consider When Developing Policy Communication Plan

QUESTIONS TO CONSIDER




©OCEG, Contact support@oceg.org for comments, reprints or licensing




Elements of a Policy Communication Plan


ESSENTIAL ELEMENTS OF A COMMUNICATIONS PLAN




GOALS
Define specific communication goals and strategies for distribution, certification and training for each policy.




AUDIENCE
Write the communication and training plan to meet the unique needs of each target group.



RESOURCES
Assign the appropriate people, budget and other resources to ensure communication goals are met.




ACCESSIBILITY
Develop each policy training program to be accessible, understandable and actionable by



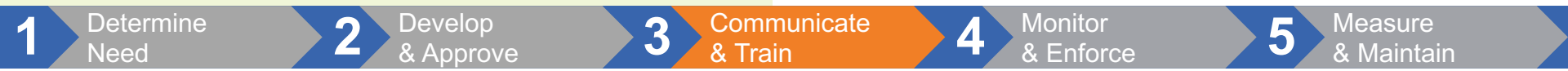
MEASUREMENT
Decide on metrics that will constitute 'success' for each phase of the communication process.



ALIGNMENT
Align communication and training strategies with the corporate culture. Gain support of executives and management.



STAKEHOLDERS
Collaborate with and enlist the support of internal stakeholders across the business.

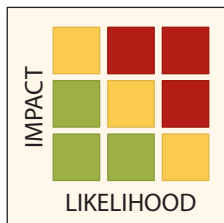


Understand Policy Communication Needs in Context of Risk and Role

ASSESS RISK

Assess the likelihood and impact of events that may negatively impact the organization.

What are the key risk areas for our business?



ANALYZE RELEVANCE TO EACH JOB

Any given risk area will be more or less relevant to each job family. It is helpful to categorize relevance so that resources are focused on the right people.



High Relevance

Jobs in the cross-hairs of a particular risk. Conduct in the face of this risk will significantly impact the organization.



Low Relevance

Low likelihood of the job facing the risk and relatively low impact risk to the organization at this level.



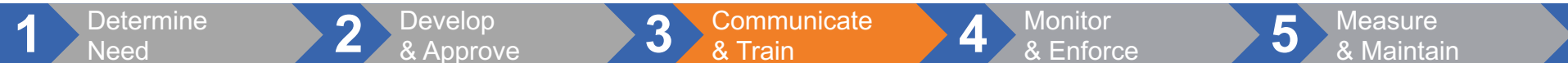
Medium Relevance

Jobs facing the risk on a regular basis and/or presenting a moderate level of impact to the organization if they mishandle the risk.



No Relevance

The risk is completely irrelevant. It is important to identify this so that education resources are not wasted.



Implement Policy Communication in Context of Risk Exposure

LEVEL OF SKILL REQUIRED

Measure the desired level of awareness required by someone in the job. Higher levels of awareness are required when a risk is relevant.

EXPERT: Evaluates When and How to Use Knowledge

Individuals in “high relevance” roles for a particular risk must be experts in addressing the risk. They should be able to evaluate and judge when and how to use knowledge and tools in diverse scenarios and under a variety of conditions. Experts are able to develop standards and tools for others to follow.

PROFICIENT: Applies Knowledge

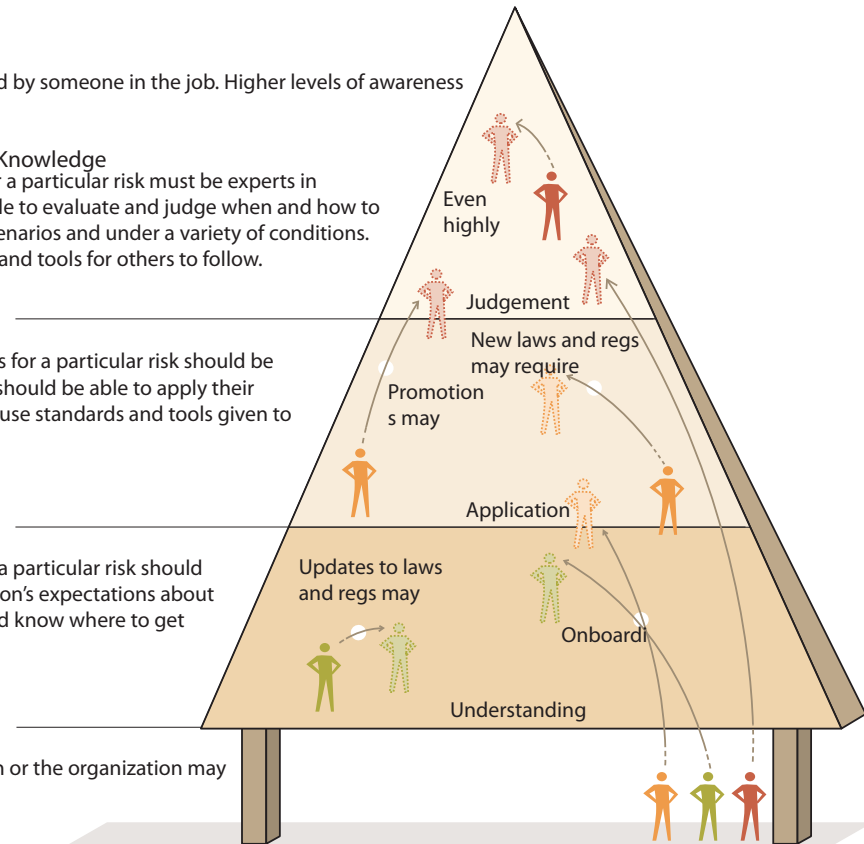
Individuals in “medium relevance” roles for a particular risk should be proficient in addressing the risk. They should be able to apply their knowledge to common scenarios and use standards and tools given to them.

NOVICE: Understands Knowledge

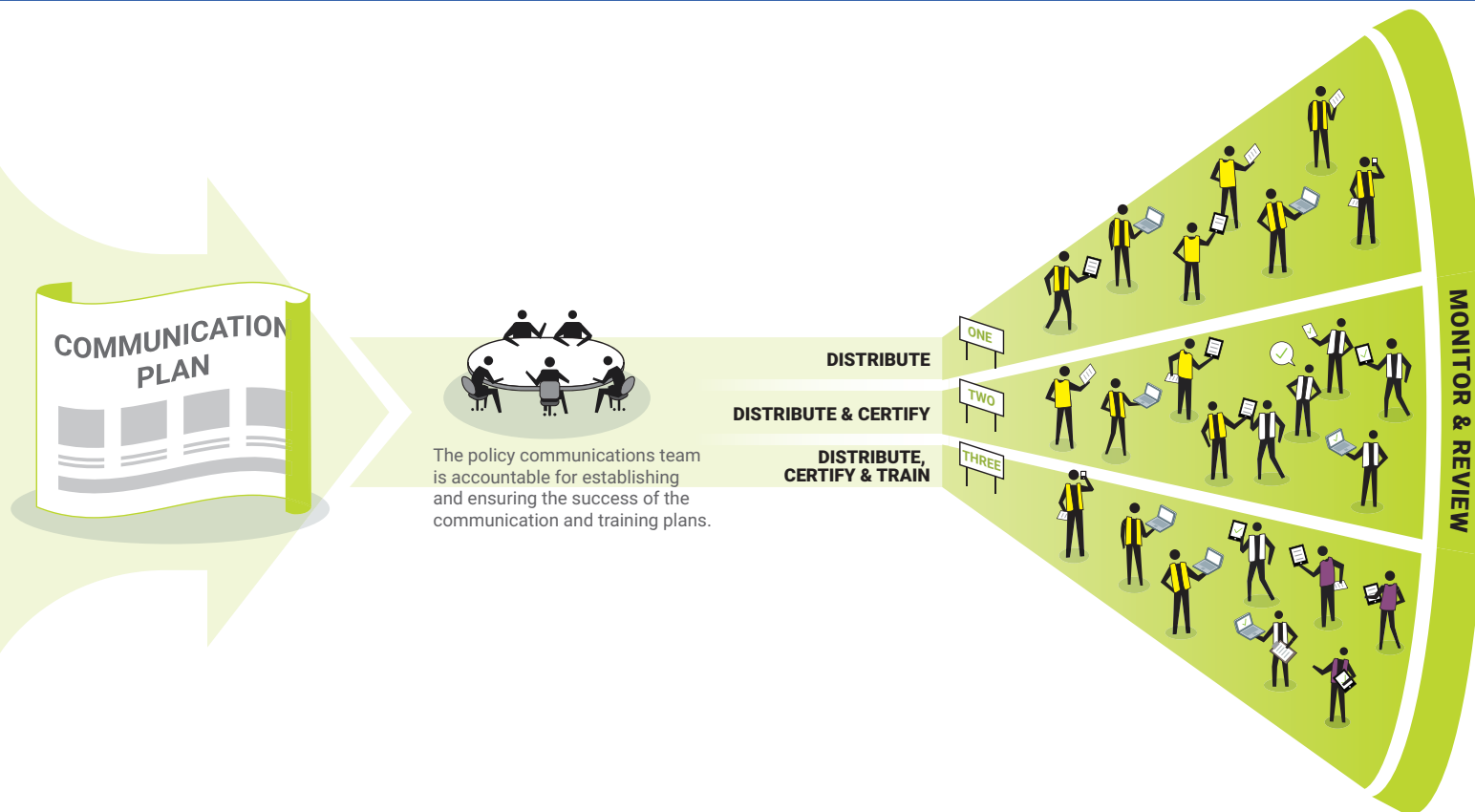
Individuals in “low relevance” roles for a particular risk should be aware of the risk and the organization’s expectations about how to address the risk. Novices should know where to get assistance in addressing a risk.

NEW HIRES

Individuals who are new to the position or the organization may need to start from the ground up.

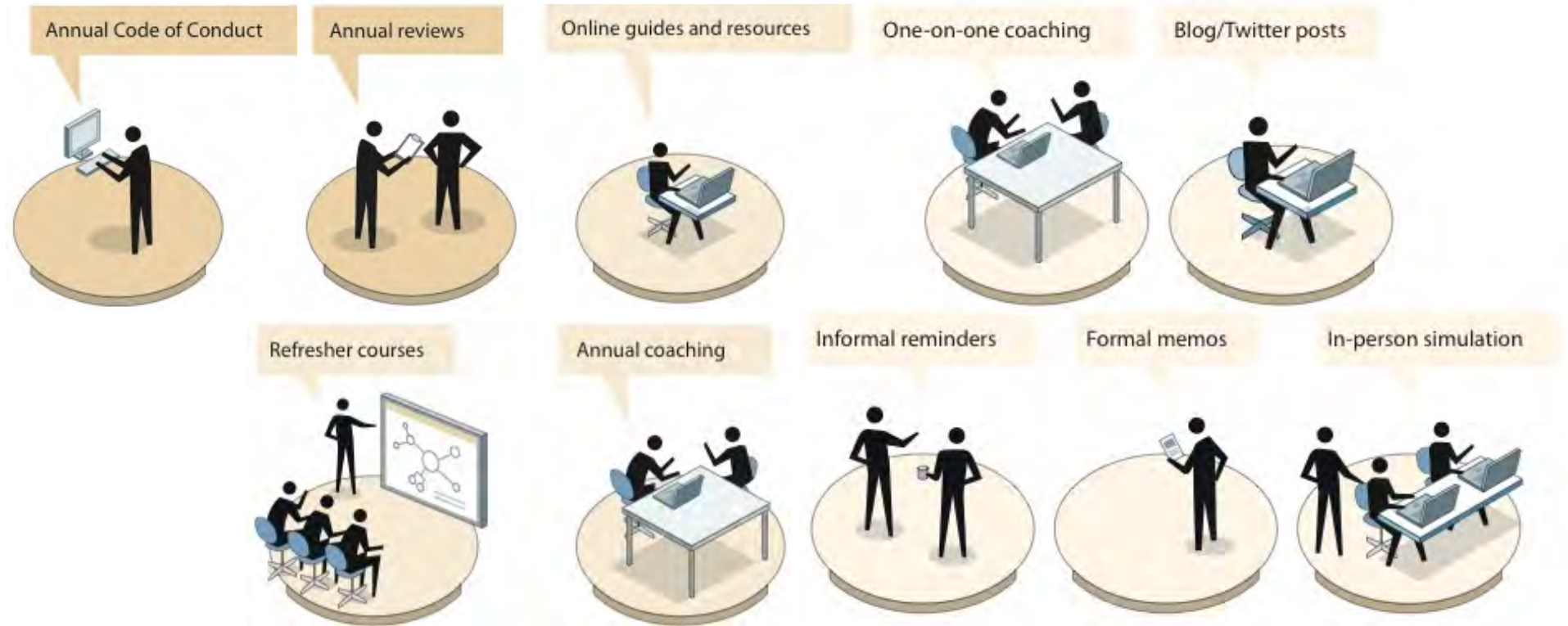


Policy Team Approves Plan & Initiates Communication



©OCEG, Contact support@oceg.org for comments, reprints or licensing

Methods to Communicate a Policy & Increase Awareness



Identify If and How Policy Needs to be Communicated to 3rd Parties

Minimal/None

You and the extended enterprise partner conduct business at arms' length and no policies or procedures are exchanged or agreed to.



Contractual Agreement

You and the extended enterprise partner agree to and include in contracts important operating principles and a code of conduct.



Periodic Certification

The extended enterprise partner signs and periodically certifies that they adhere to specified policies and procedures.



Integrate and Use

In this instance, the extended enterprise partner actually adopts and integrates your policies and procedures into their organization.



Monitoring and Audit

Beyond integration, usage and self-certification, the extended enterprise partner agrees to periodic monitoring and audit for compliance with policies and procedures.



Measure the Success of Policy Communication & Training

1. Do students believe that the training is useful?
2. Have students actually learned the material?
3. Have students translated knowledge into action?
4. Have these skills impacted the business?

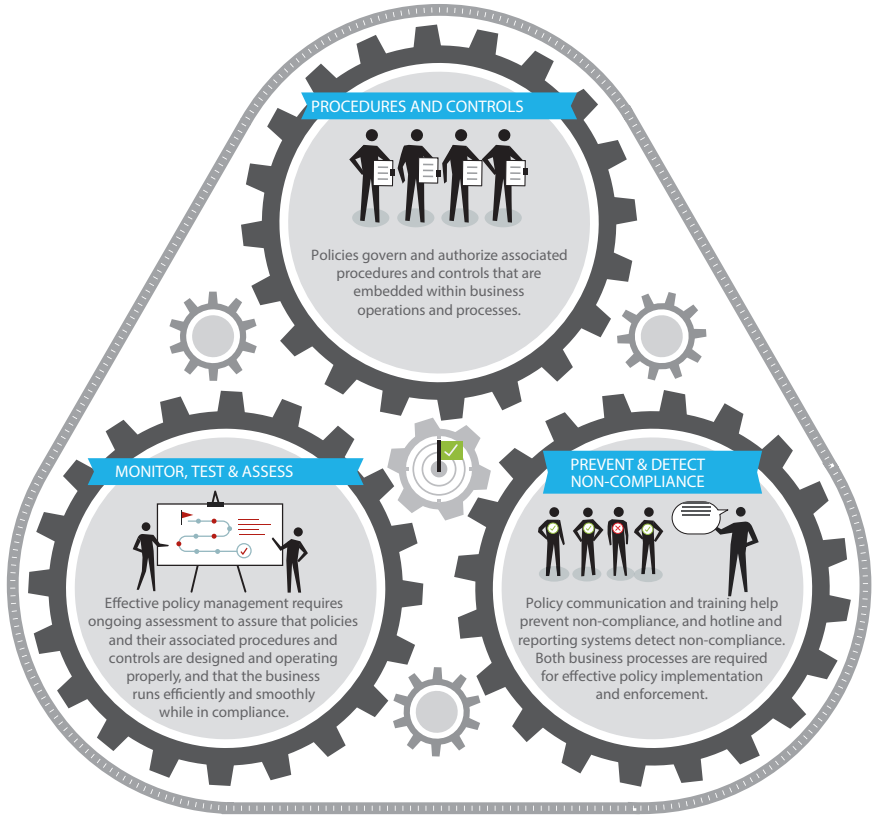




IMPLEMENT & ENFORCE

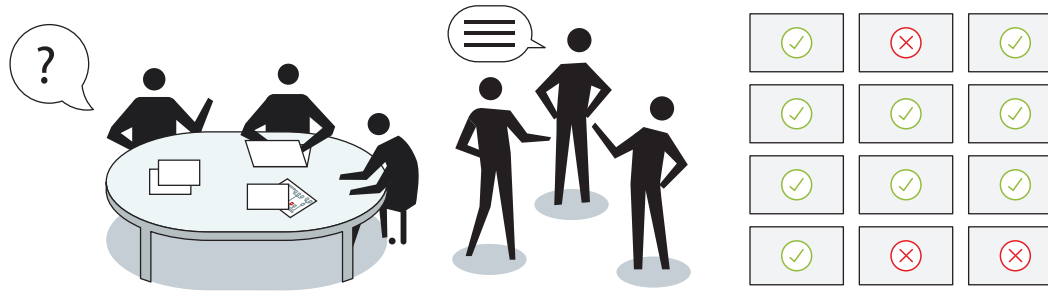
Even with good communication, policies aren't always followed. Implement controls that enable enforcement. Monitor those controls for effectiveness and adherence. Document and remediate violations, while considering what policy improvements should be made.

Monitor & Enforce Involves Related Procedures, Controls, and Assessments



- 1 Determine Need
- 2 Develop & Approve
- 3 Communicate & Train
- 4 Monitor & Enforce
- 5 Measure & Maintain

It is Critical to Document and Manage Policy Exceptions and Exemptions

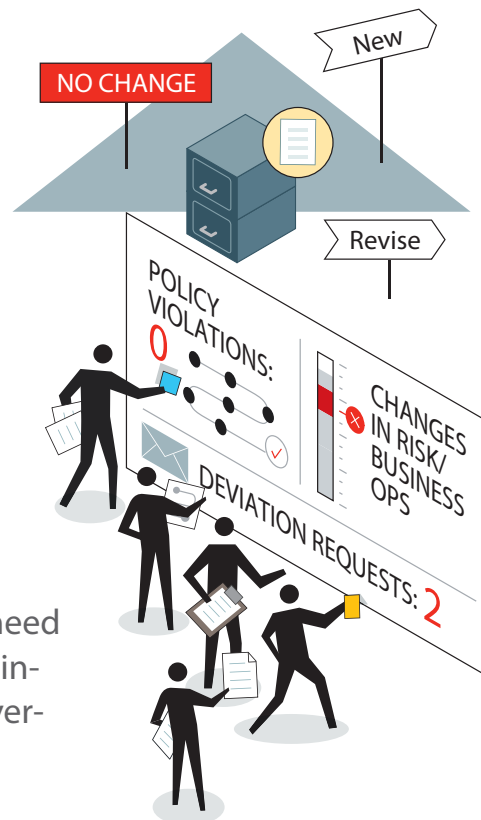


- Policy implementation and/or enforcement is not always possible. Exceptions can happen when the organization cannot comply with a policy, when the policy is too subjective, or requires excessive clarification.
- Organizations need processes to authorize, track, monitor and review exceptions.
- Those who authorize exceptions must have sufficient authority. Limits should be set so exceptions are regularly reviewed and not granted for extended or unreasonable time periods.
- Exceptions must be documented and available to auditors and regulators upon request. Organizations that demonstrate clear procedures for policy exception management are also better able to defend their policy management processes.
- Organizations should institute compensating controls as part of exception approval until policy revisions are made or the organization is brought into full compliance.

Contact Carole S. Switzer cswitzer@oceg.org for comments, reprints or licensing requests

MEASURE AND RE-EVALUATE

Periodically review each policy to ensure it remains relevant and correct. Design and implement standardized steps to determine need for revision, reauthorization or retirement. Maintain the version control and archives of each version and related management steps.



Design Effectiveness

- An organization begins with understanding if the policy system is effectively designed.
- To determine this, an organization documents policies and processes.
- Ultimately, the organization must judge if all of these policies, processes, and the system as a whole are designed such that it will satisfy stakeholders and regulators while managing risk, requirements, and obligations.



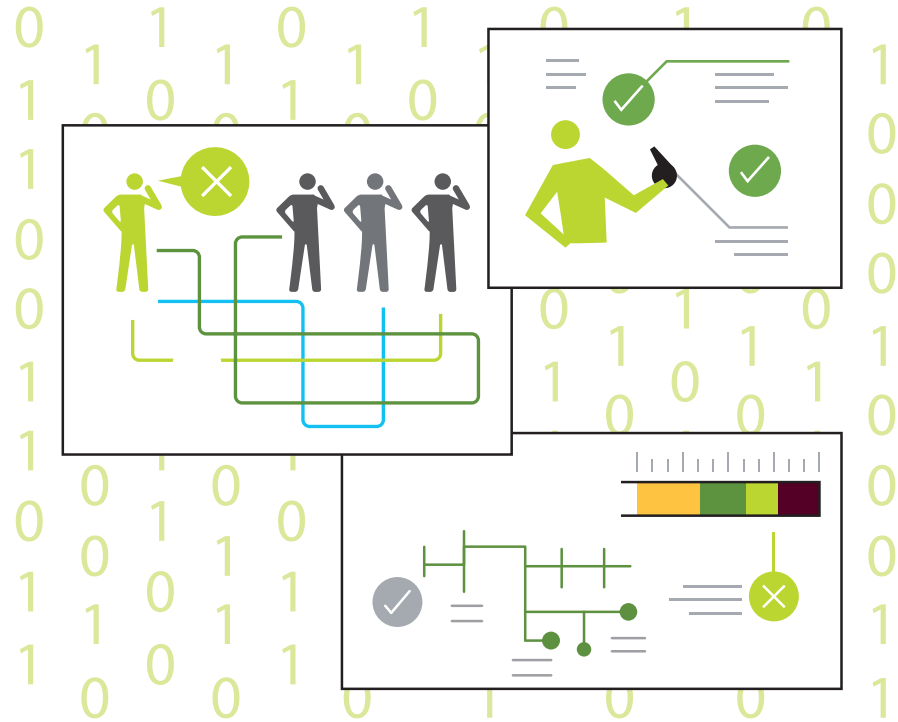
Operating Effectiveness

- On the other hand, an effectively operating policy system is one that considers how policy is being managed within business and its impact on the business.
- The organization should determine if the system actually operates as designed, and is that system supporting the needs of a dynamic business in a way that increases business agility while minimizing use of financial and human capital resources.

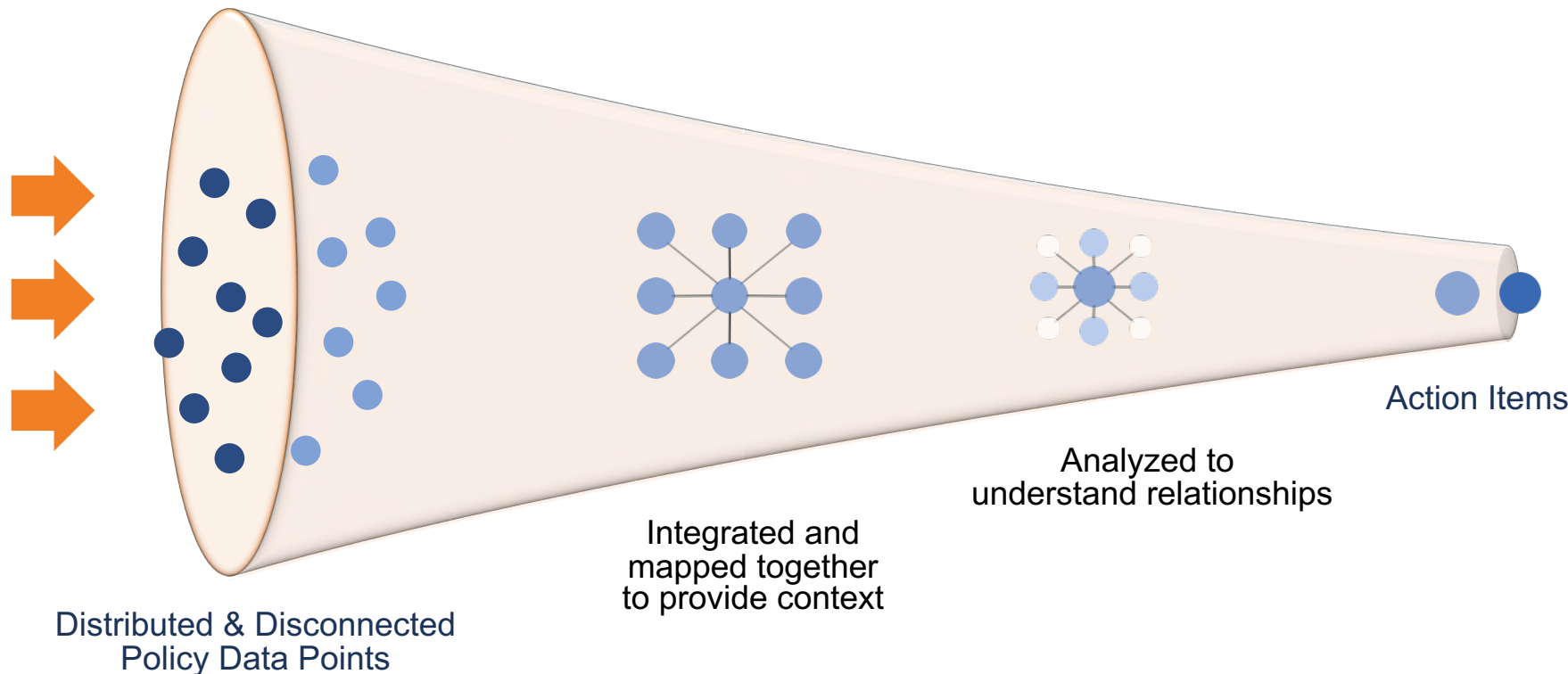


Establish Metrics that Provide Value to Improve Policies in a Business Context

Metrics can provide a solid foundation for continuously refining the organizational policy program. The right metrics will help ensure policies are effective at establishing desired behaviors efficiently, and agile enough to accommodate the demands of a dynamic and distributed business environment.



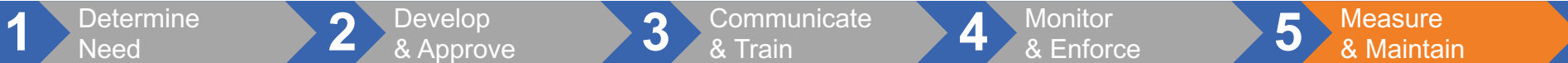
Measure Policies in Context of Integrated Metrics Across GRC Areas



- 1 Determine Need
- 2 Develop & Approve
- 3 Communicate & Train
- 4 Monitor & Enforce
- 5 Measure & Maintain

Areas of Policy Metrics & Measurement

AMBIGUITY Is a lack of understanding resulting in policy questions or non-compliance?	CLARITY Is the policy oriented appropriately to the intended audience?	APPROVAL How long has it been since this policy was last reviewed?	RISK EXPOSURE Does the policy mitigate risk within accepted boundaries of risk appetite and tolerance?	REGULATIONS What regulatory changes and enforcement actions impact this policy?	LEGISLATION What legislative changes impact this policy?	EXTERNAL RISK What socioeconomic, political, and industry changes impact this policy?	BUSINESS CHANGE What changes to the business such as mergers/acquisitions, strategy and operations impact this policy?
ISSUES How many hotline reports have been received in relation to this policy? What are the results of surveys and assessments related to this policy?	INCIDENTS How many substantiated policy violations have occurred and why? Are there repeat offenders related to these incidents?	EXCEPTIONS How many exceptions to the policy have been documented and approved? How long has it been since these exceptions were last reviewed?	NON-COMPLIANCE Is the policy being complied with? How many controls are in place to properly monitor the enforcement of the policy?	DELIVERY Is the policy communicated in the right formats and languages to best reach the target audience?	TRAINING Have employees successfully completed required training programs related to this policy?	ATTESTATION Have employees acknowledged and attested that they will follow the policy?	COMMUNICATION Has the policy been verifiably communicated to its audience in the past year?



Other Policy Metric Examples

Number

Number of regulations, individual requirements, enforcement actions, and other changes the organization monitors.

↻ Frequency

Frequency of alerts and regulatory changes impacting the organization by subject matter area over a period of time.

✓ Flagged

Status of changes that have been flagged for review/analysis to determine business impact and status of review.

⚖ Ranking

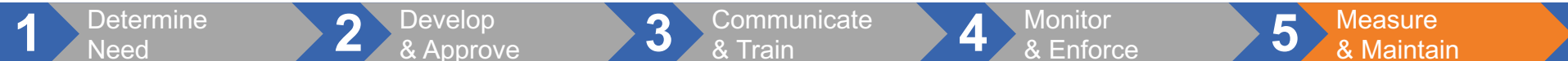
Summary of regulatory changes impacting their organization and the level of risk and resulting change impact on the organization.

↗ Trends

Trending of regulatory change alerts, analysis, and action items from one period to another impacting the organization.

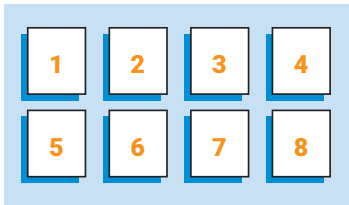
🔗 Relationships

Relationship of regulatory changes to impact on policies, procedures, controls, risks, training, reporting and other GRC activities.



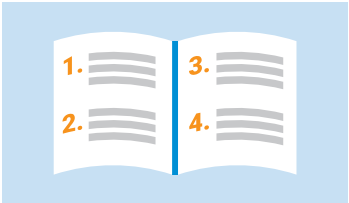
Preserve an Audit Trail and System of Records of All Policy Interactions

ELEMENTS OF DEFENSIBLE AND EFFECTIVE POLICY COMMUNICATION AND TRAINING



VERSION (DATE, TIME)

Effective policy and training programs can pinpoint, by individual, the version of a policy that was communicated and the communication/training activities surrounding that version.



TESTING UNDERSTANDING

To ensure understanding, the organization should test comprehension on critical/high-risk policies to ensure that they have been properly communicated and understood.



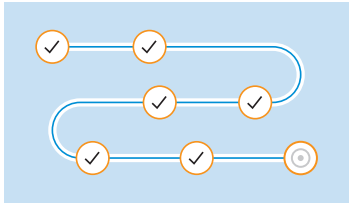
QUESTIONS & EXCEPTIONS

Communication plans should include how to ask questions on policies and request exceptions. Effective programs include ways to document, approve and periodically evaluate questions and exceptions in order to update policies and/or identify emerging risks.



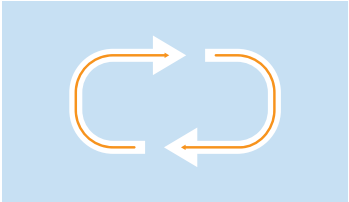
ACCESSING PAST RECORDS

Defending the organization in legal and regulatory actions requires that a 360 degree view of the history of the policy, interactions with the policy, and policy communications be accessible with defensible audit trails.



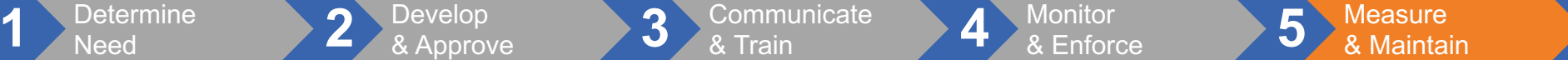
SYSTEM OF RECORD

To defend itself and validate an effective compliance/policy program the organization should be able to have a complete historical record of policy communication and training.



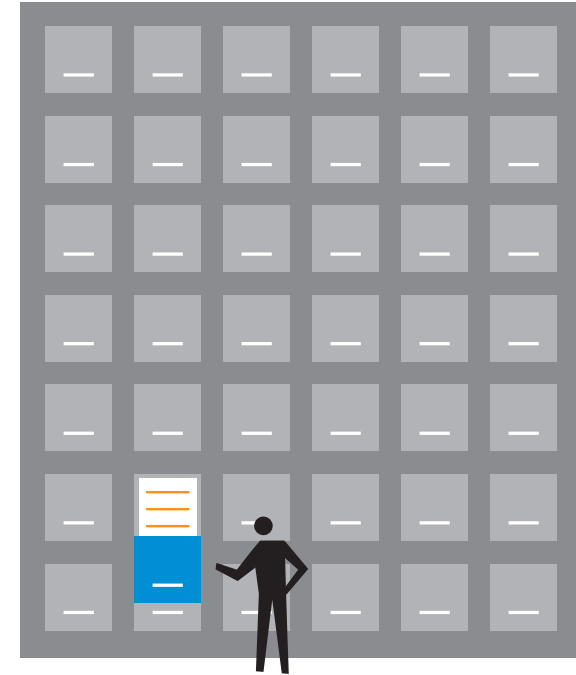
REPEATABLE CYCLE

Communication is never complete. Repetition using different methods and tones can increase understanding and compliance.



Provide a Full Policy Version History With the Audit Trail & Records

Every policy and its past revisions must be archived for referral at a later time. When an organization experiences an incident or is examined by an external auditor or regulator, it is often necessary to provide positive evidence of policy compliance. Preserving a full view of the policy history and audit trail (including key data points such as the owner, who read it, who was trained, acceptance acknowledgements and dates for specific policy versions) will help assert an accurate and complete policy control environment is operating effectively.



1 Determine Need

2 Develop & Approve

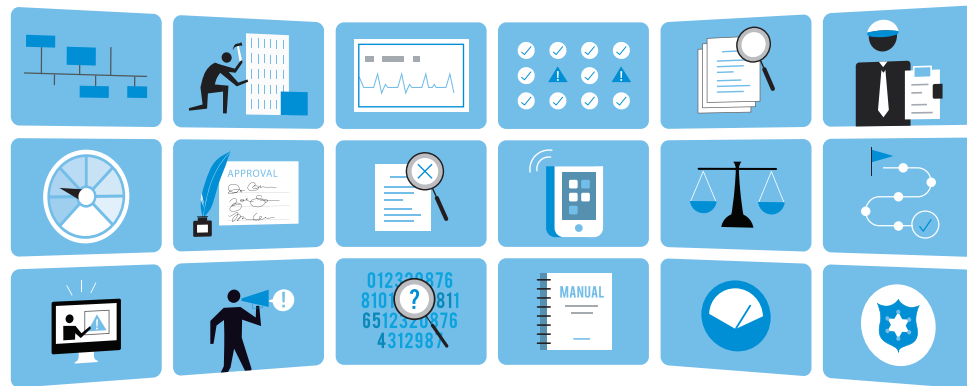
3 Communicate & Train

4 Monitor & Enforce

5 Measure & Maintain

Implement a Periodic Review Cycle to Maintain Policies

Frequent changes to policies should not be necessary in a healthy policy environment. Active diligence through regular review cycles will ensure policies remain appropriate and aligned to organizational needs and help minimize unnecessary exposure and liability. Policies found to be out of date should be revised or retired.



1 Determine Need

2 Develop & Approve

3 Communicate & Train

4 Monitor & Enforce

5 Measure & Maintain

Factors that Indicate a Policy May Need to be Revised

- ✓ Have changes to the business climate occurred that may impact this policy?
- ✓ Are there regulatory/legal changes that require a policy update?
- ✓ Is this policy clearly written for the intended audience?
- ✓ Have policy questions or ambiguities been identified?
- ✓ Are training and communication plans for this policy effective?
- ✓ Do we have an unacceptable amount of exceptions to this policy?
- ✓ Is this policy consistently enforced and complied with?
- ✓ How many violations of this policy have occurred and why?



Workshop Activity

Our Agenda . . .

1) PART 1: Policy by Design

Why Policies Matter

2) PART 2: Policy Governance

Blueprint for Effective Policy Management

3) PART 3: Policy Management Lifecycle

Managing Policies from Creation to Dissolution

4) **PART 4: Policy Management Architecture**

Enabling Information & Technology Management of Policies

PART 4

Policy Management Architecture: Enabling Information & Technology Management of Policies

Learning Objectives . . .

- ❑ Policy Management Information Architecture
Blueprint for managing policy content and related data
- ❑ Policy Management Technology Architecture
Blueprint for enabling policy processes with technology
- ❑ Policy Management Business Case
Articulating the value of effective policy management
- ❑ Interactive Group Discussions

Why a Common Policy Architecture?

CRITICAL SUCCESS FACTORS

- Standardized language
- Standardized definitions
- Standard data format and specification
- Standardized workflow
- Standardized processing and escalation rules
- Methodology to act on insights and improve the system

BENEFITS OF TAKING AN EXPANDED VIEW



Additional sources of information help management to detect and respond to incidents more rapidly



Leveraging a common system increases effectiveness while reducing costs



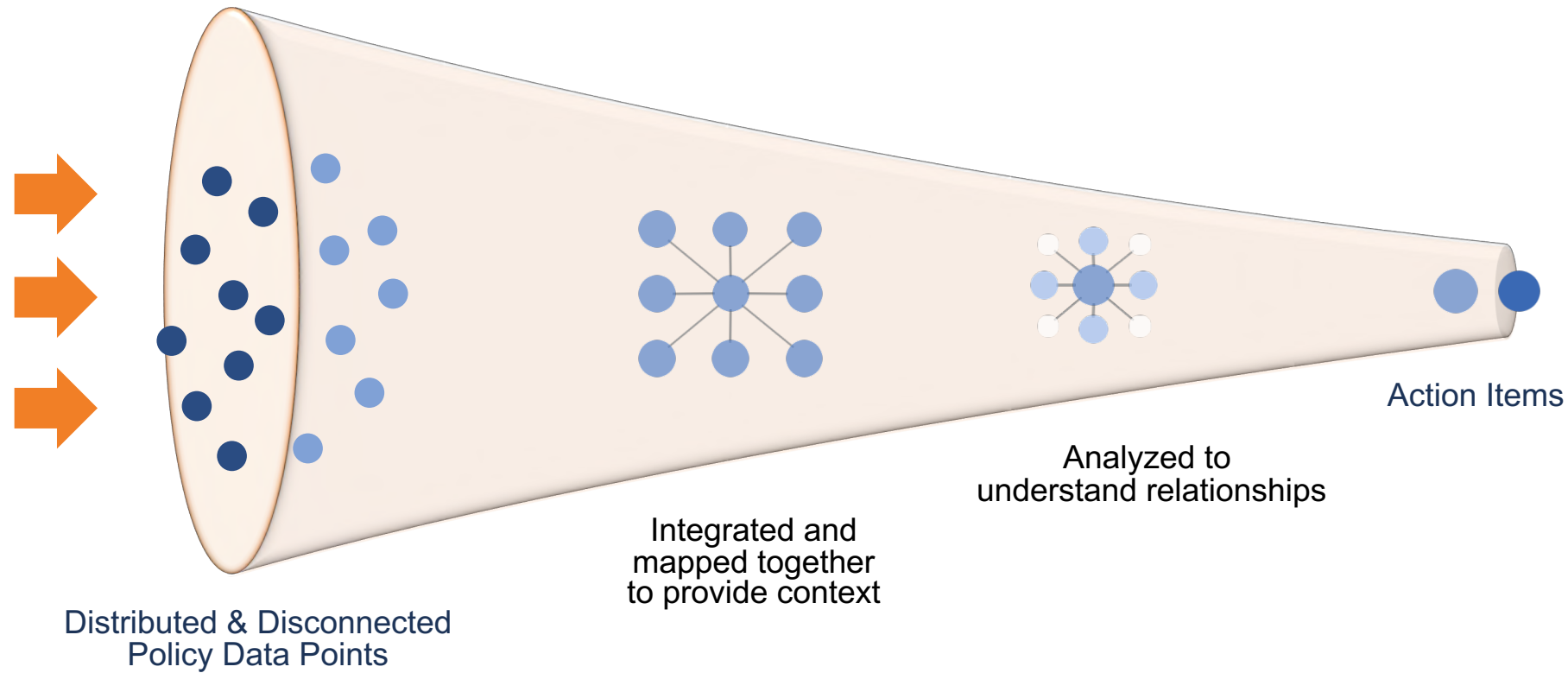
Automating the approach reduces the need for manual and often laborious gathering and reconciliation of disparate sources of information



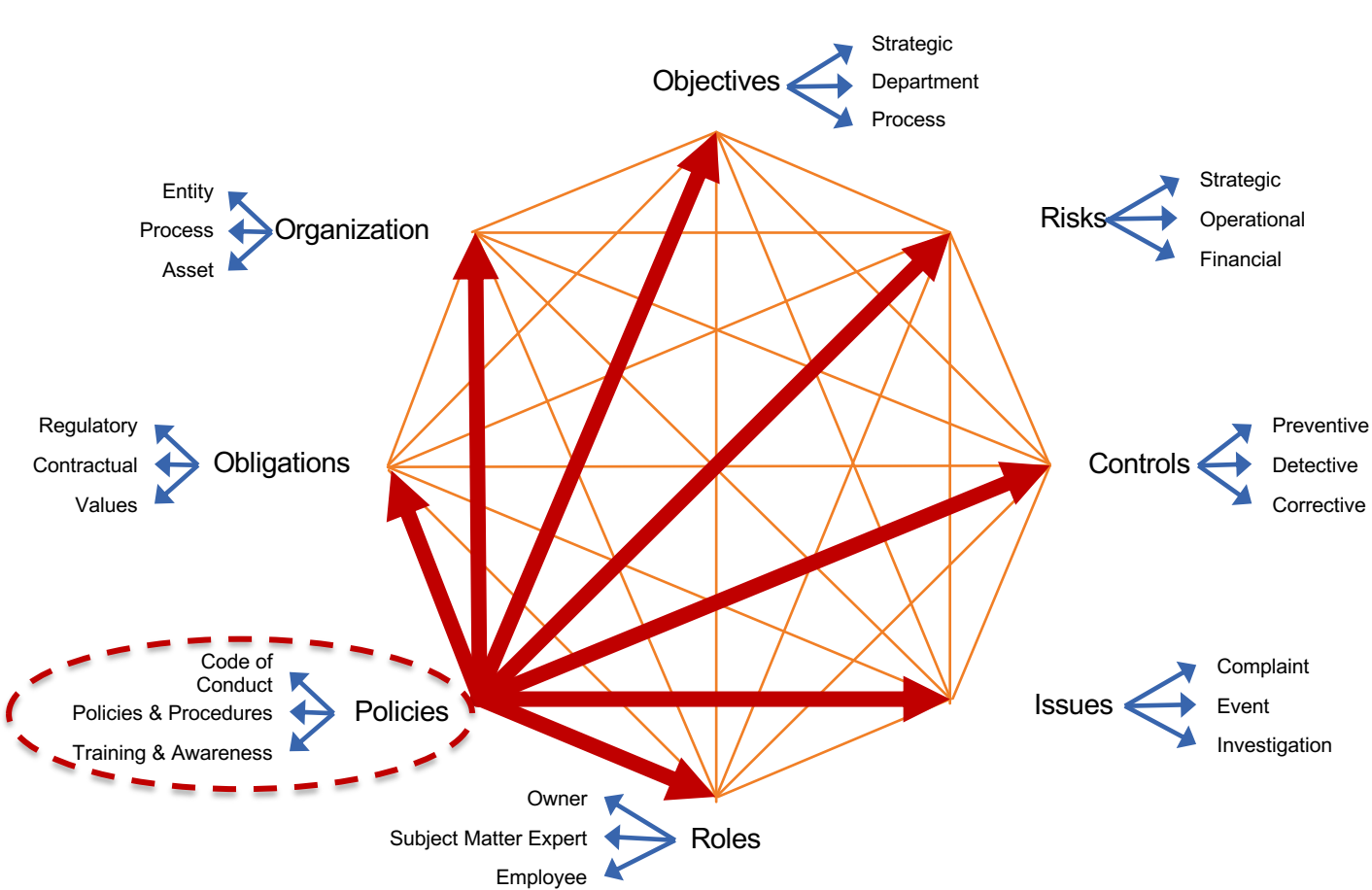
Information consistency makes it possible to examine trends across business units and analyze correlation with business performance



Better insight enables optimized allocation of capital to risks and requirements



Policy Information Architecture Provides 360° Contextual Intelligence



higher quality information

Integrating GRC information allows management to make more intelligent decisions, more rapidly.



process optimization

All non-value-added activities are eliminated and value-added activities are streamlined to reduce lag time and undesirable variation.



better capital allocation

Identifying areas where there are redundancies or inefficiencies allows financial and human capital to be allocated more effectively.



improved effectiveness

Overall effectiveness is improved as gaps are closed, unnecessary redundancy is reduced, and GRC activities are allocated to the right individuals and departments.



protected reputation

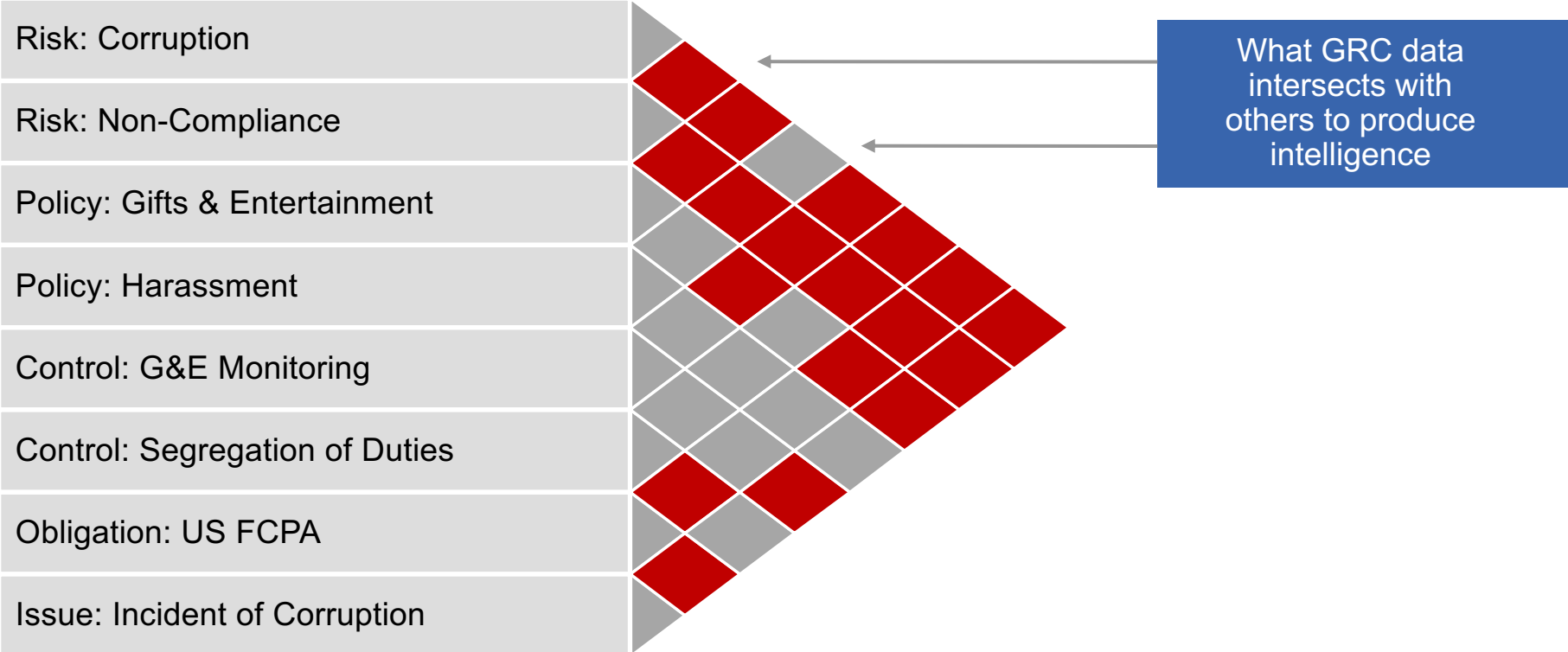
Reputation is protected and enhanced because risks are managed more effectively.



reduced costs

Reduced costs help to improve return on investments made in GRC activities.

Policy Data Interrelationships Matrix



Technology Enables Efficient, Effective & Agile Policy & Training Management

The bottom line: With today's complex business operations, global expansion, and the ever changing legal, regulatory and compliance environments, a well-defined policy management program is vital to enable an organization to effectively develop and maintain the wide gamut of policies it needs to govern with integrity.

In a complex business environment, technology is essential for successful policy & training management.



- ◆ Organizations often lack an auditable means of policy maintenance, communication, attestation, and training.
- ◆ An ad hoc approach to policy management exposes the organization to significant liability.
- ◆ If policy documentation doesn't conform to an orderly style and structure the organization is not positioned to drive desired behaviors in corporate culture or enforce accountability.

GRC Technology Market Segments



Policy & Training Management

Policy & Training Management Platforms

Policy Management Solutions

Training Management Solutions

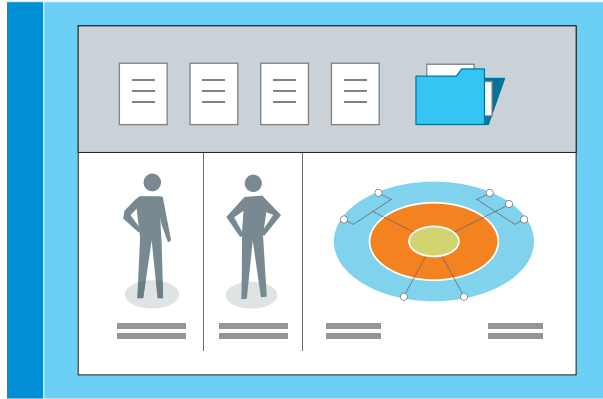
Policy Forms & Disclosure Solutions

Training & Gamification Solutions

Miscellaneous Policy & Training Mgmt Tools

Policy & Training Management technologies manage the development, approval, distribution, communication, forms, maintenance, and records of organization policies, standards, procedures, guidelines and related training and communication awareness activities. This includes solutions used to train individuals on policy and risk areas to employees and extended business relationships. Elements of gamification, eLearning, learning management, document/content management are part of this segment from a GRC perspective. Forms and disclosure management solutions (e.g., conflict of interest, gifts & entertainment/hospitality) are included in this segment as they relate and support organization policies.

Policy Management Technology Enables Management of Policy Processes



AUTOMATION AND TRACKING

Technology enables the change tracking and monitoring process by integrating information and content sources with software that automates and tracks workflow, accountability, and analysis of changes or additions needed in policies.

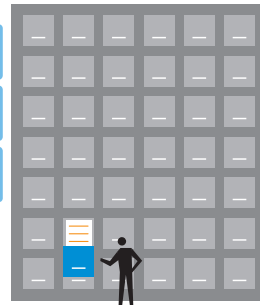
MANAGEMENT REPORTING

AUDIT TRAIL

WORKFLOW & TASKS

COLLABORATION

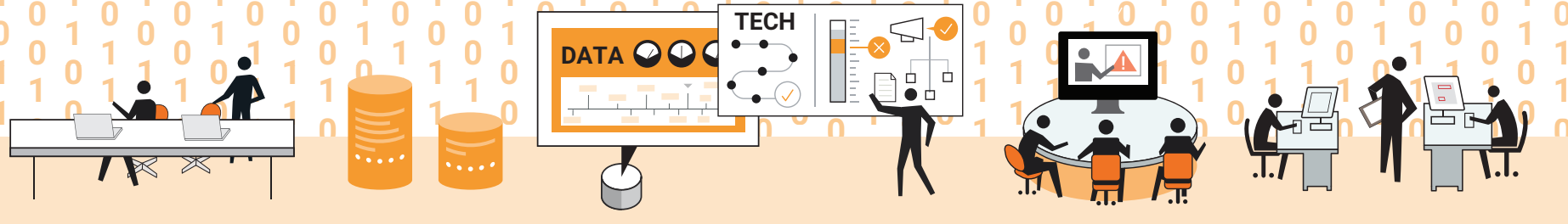
ENFORCEMENT



Benefits of Technology

Utilize technology as the backbone to implement and measure the effectiveness of your policies and your communication plans.

THE BENEFIT OF TECHNOLOGY



Integration

Technology integrates policy training and communication with other compliance program components like HR systems for holistic recordkeeping and data analysis.

Visibility

Technology permits permissions-based and enterprise-wide visibility on demand.

Global Reach

Technology delivers the correct version and language seamlessly.

Availability

Technology allows policies to be accessed, consulted, updated and managed without the confusion of email clutter.

How Technology Enables Policy Management

TECHNOLOGY

Policy management software can be leveraged to streamline policy development, alignment, change management, communication and performance monitoring. Policy training and awareness, acceptance, metrics gathering and archival can be automated to ensure the effectiveness of the policy program is understood in context.



Repository

Technology enables policy implementation and enforcement by creating a repository of all policies, procedures, and controls that are cross-referenced with one another and not treated as isolated documents.



Accountability

Technology provides for a complete picture and defensible audit trail of the 'who, what, when, where, how and why' including the role and actions of each individual.



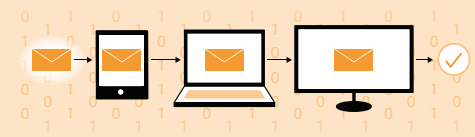
Consistency

Technology creates a consistent environment to conduct assessments, track issues of non-compliance, and take corrective actions. Technology allows organizations to more easily and efficiently manage its hundreds to thousands of individual documents especially during audits and assessments.



Automation

Technology enables the automation of workflows and tasks to complete audits and assessments related to policy compliance. No longer is the organization encumbered by unanswered or lost emails or documents that are out of sync.



How Technology Enables Policy Management

TECHNOLOGY

Policy management software can be leveraged to streamline policy development, alignment, change management, communication and performance monitoring. Policy training and awareness, acceptance, metrics gathering and archival can be automated to ensure the effectiveness of the policy program is understood in context.



- ✓ Consistently manage the policy life cycle
- ✓ Notify when changes to regulations, laws, standards and procedures affect policies
- ✓ Link policies to drivers, controls, owners, reporting pathways and training
- ✓ Provide a user-friendly portal for employees and other stakeholders
- ✓ Enable cross-referencing and linking of policies and procedures
- ✓ Provide a robust system of record for access/certification/training
- ✓ Establish a calendar view to streamline communications
- ✓ Restrict access and rights to individual policies
- ✓ Assign relevant policies based on target group
- ✓ Keep a record of all policy versions and histories
- ✓ Maintain accountable workflow
- ✓ Deliver comprehensive reporting

Solution Area Definition

Policy management solutions provide the capability to manage the development, approval, distribution, communication, forms, maintenance, and records of policies, procedures and related awareness activities.

This enables organizations to manage:

- Policy management process of development, approval, communication, monitoring, and maintenance. This includes workflow, task management, and content management capabilities with version control
- Policy portal for individuals to be able to access policies relevant to their role and responsibilities, access related resources and forms, and complete tasks related to policies and training.
- Policy evidence to provide a system of record and audit trail of all interactions, development, approvals, communications, training, exception, exemptions related to policies.

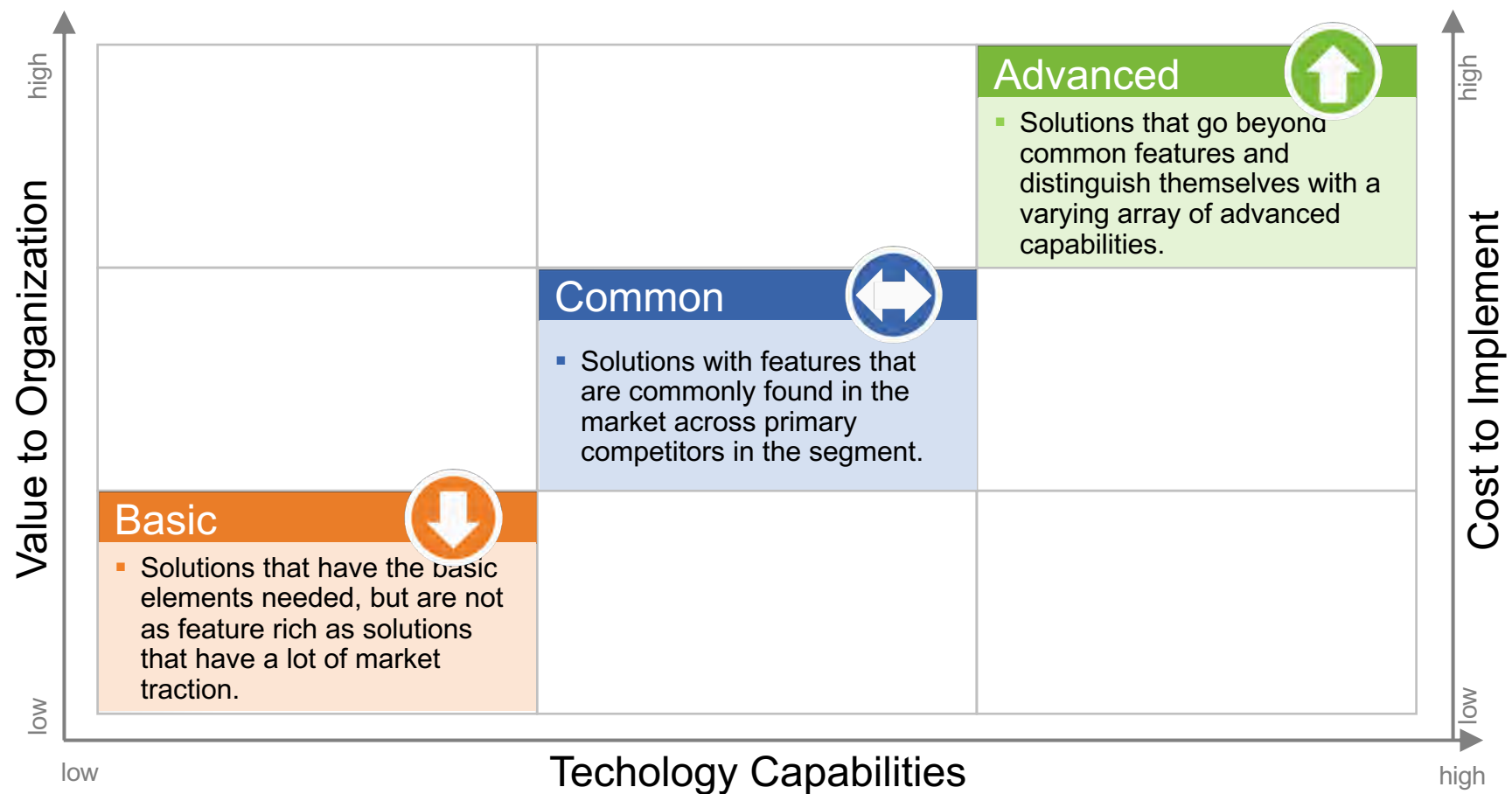


Critical Capabilities

- ❑ Manage policy lifecycle from development through maintenance and policy retirement
- ❑ Workflow, task management, and content management
- ❑ Integration w/ HR systems & business systems to identify change where policies/training need to be communicated
- ❑ Policy portal for individuals to access policies, training, forms, and related tasks
- ❑ Forms development and management for forms related to policies
- ❑ Editing capabilities and version control of policy content
- ❑ Ability to map policies to other GRC content and records
- ❑ Regulatory change management to keep policies current
- ❑ Exception/exemption management of policies
- ❑ Integration of training and LMS capabilities
- ❑ Audit trail of evidence of all policy interactions
- ❑ Mobility capabilities



Basic, Common & Advanced Solutions



What Differentiates Basic, Common & Advanced Solutions?



Characteristics: Basic Policy & Training Management Platforms

Basic policy management platforms focus on the workflow, forms, and tasks of policy management. The value focus is on task automation by removing inefficiencies of manual approaches of documents, spreadsheets, and emails and replacing this with a solution that can collect information, manage workflow and tasks, and simplify reporting. Policies are typically imported as documents.

Value = tends to be the lower cost solutions to acquire, focus is more on the small to medium sized enterprise deployments



Capabilities

- ✓ Supports back-end process of policy management
- ✓ Workflow
- ✓ Task management
- ✓ Reporting
- ✓ Notification
- ✓ Tracking attestations
- ✓ Tracking exceptions/exemptions
- ✓ Survey capabilities to measure policy awareness/understanding
- ✓ Audit trail/system of record of policy related activities



Limitations

- Policies are typically managed as documents (e.g., PDFs) that are imported into the system and not developed in the system
- Little to no integration supported with HR and other business systems to identify business changes in which policies need to be communicated
- User experience is typically poor as the policy portal has not been thought out and developed with an aesthetic appeal
- Many solutions do not have forms management and processing
- Limited capabilities to integrate training
- Typically designed for a department view of policies and not an enterprise view

What Differentiates Basic, Common & Advanced Solutions?



Characteristics: Common Policy & Training Management Platforms

Common policy & training management platforms have the range of features commonly found in Policy Management RFPs. They build upon the foundation of workflow, tasks, surveys, and forms with features to provide greater integration with other systems, and have forms management.



Capabilities

- ✓ Has workflow, task, survey, and content capabilities of Basic solutions
- ✓ Forms development and management related to policies
- ✓ Stronger integration with LMS systems (but does not have its own LMS)
- ✓ Supports editing of policies with the solution instead of managing policies as external documents that are imported
- ✓ Integration with HR and other business systems to identify changes in which policies need to be communicated



Limitations

- Mapping of policies to regulations is on a document to document level and not a 'chapter and verse' level within documents
- Limited integration of regulatory intelligence and change
- Most often has been focused more on the back-end of policy management with limited focus on the front-end user portal of policies



Characteristics: Advanced Policy & Training Management Platforms

Advanced policy & training management platforms are Common Platforms that have distinguished themselves from competitors by offering advanced capabilities in different areas.

Areas of Advanced Capabilities (note, a solution might have one or more of these):

- ✓ Mobility. Mobile capabilities that provide a policy and training portal on mobile devices.
- ✓ Policy awareness & communication planning. Ability to manage policy awareness plans for individual policies, groups of policies, and all policies with calendar, tasks, and reporting requirements.
- ✓ Integrated training/LMS. The solution has a fully functional LMS capability within the policy management platform.
- ✓ User portal. The solution has a strong, intuitive, engaging user portal for individuals across the organization to access and interact with policies.
- ✓ Gamification. The solution supports gamification in context of creating corporate avatars and tracking merits in policy and training completion tasks and activities, and supports interactive learning and games in context of policies.
- ✓ Contextual changes. The solution supports geo-location capabilities to identify when individuals visit a new location to make them aware of specific policy, procedure, guideline, and issue reporting needs at the location.
- ✓ Regulatory change. Robust integration of regulatory change and intelligence content and feeds, with capabilities to map 'chapter and verse' of a policy to 'chapter and verse' of a regulation.
- ✓ Redlining and advanced editing. Full editing and word processing capabilities within the policy management solution
- ✓ Process modeling. Process modeling capabilities to visualize business processes and identify policy control points on processes.

Deliver a Unified Company Policy Portal in the Format Needed



THE POLICY PORTAL

The policy portal is the interactive hub of policies and related resources. It provides policy users with timely awareness and understanding of what is expected. A well designed policy portal is:

- **INTUITIVE** It is easy to use and provides an attractive experience for employees to learn and interact within.
- **ADAPTIVE** It adapts to changes in the business, regulatory environment, and employee context to provide up to date relevant information when and where it is needed.
- **PERSONAL** It allows employees to customize and organize what is relevant to them, provide feedback to management and share things they find useful with other employees.
- **ACCESSIBLE** It is optimized for mobile and tablet, and also viewable via laptop and workspace interfaces so it is always there when needed.

excerpt from OCEG GRC Illustrated Series, use by permission only. ©2014 OCEG.org

An Engaging User Experience for Policy Management



UNIFIED

- The portal is a one stop shop for policies, training, reporting and guidance
- Policies are connected to related procedures, training, definitions and help links
- Changes in policy needs, updates and flags for attention are automated based on detected changes in role, requirements and activities

RELEVANT

- Policies are organized and presented based on employee role, activities, location and business unit and changes are automated
- The most critical "need to know" policies are easy to find
- Users customize personal libraries and can track their own policy related tasks, gaining merit badges for completion

INTERACTIVE

- Understanding is increased through embedded media, games and scenario enactments
- Pop-ups or links provide access to definitions & resources
- Alerts, notices and reminders are automated

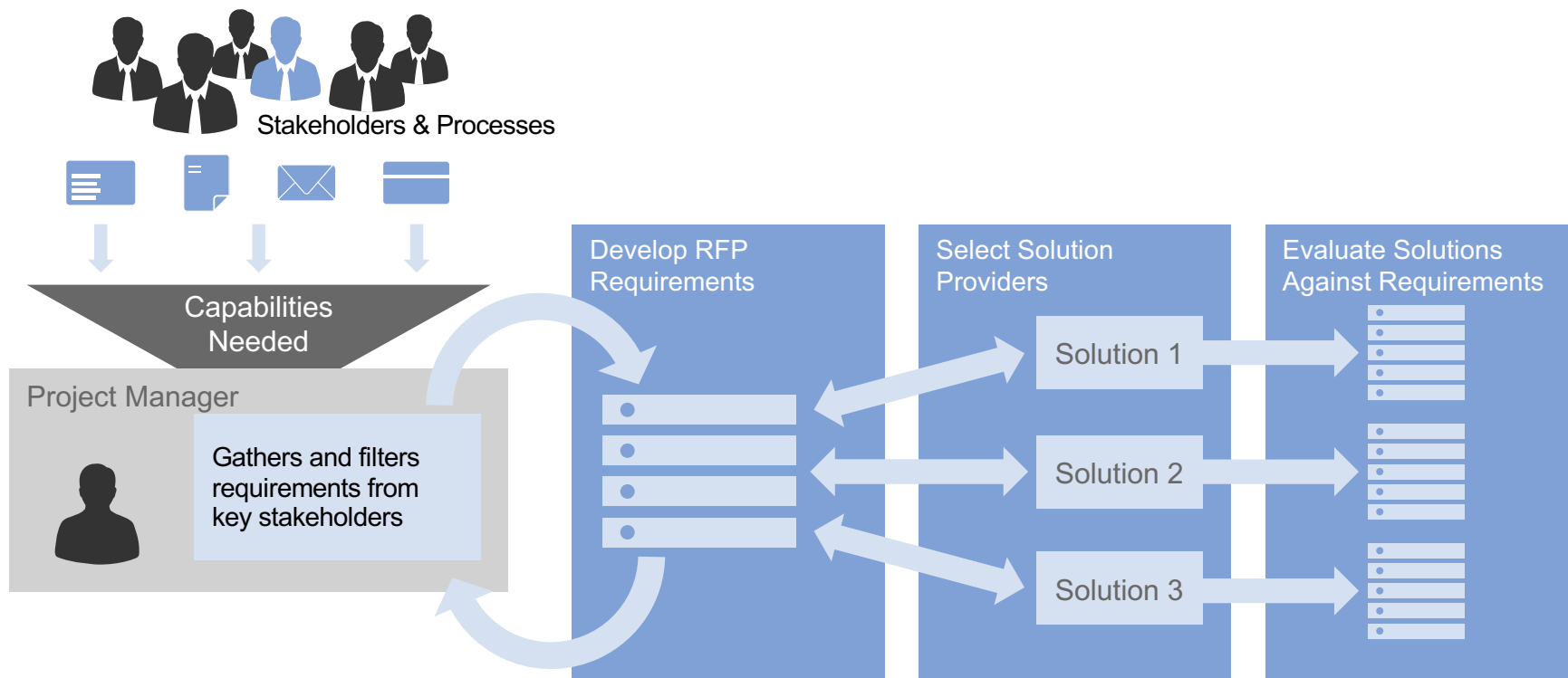
SOCIAL, YET PERSONAL

- Employees can share policies and provide feedback to managers
- Questions are answered by a variety of methods
- Employee avatar is linked to badges and progress in policy tasks

excerpt from OCEG GRC Illustrated Series, use by permission only. ©2014 OCEG.org

The interactive policy experience is only relevant if the policies themselves remain relevant. Organizations need to have a policy management lifecycle to develop and maintain policies in the midst of changing business, risk, and regulatory environments.

Policy Management Platform Selection Process



NOTE: these are just a selection of some common elements from GRC 20/20's RFP template containing over 250 requirements for Policy Management Platforms

Mature Policy Management Capabilities Achieve the Following 10 Objectives. . .

1

Reliably Achieve Business Objectives

2

Mitigate Risk & Uncertainty

3

Define Organizational Culture

4

Increase Stakeholder Confidence

5

Prepare & Protect the Organization

6

Prevent, Detect, and Reduce Adversity and Weaknesses

7

Motivate & Inspire Desired Conduct

8

Consistent Processes & Behavior

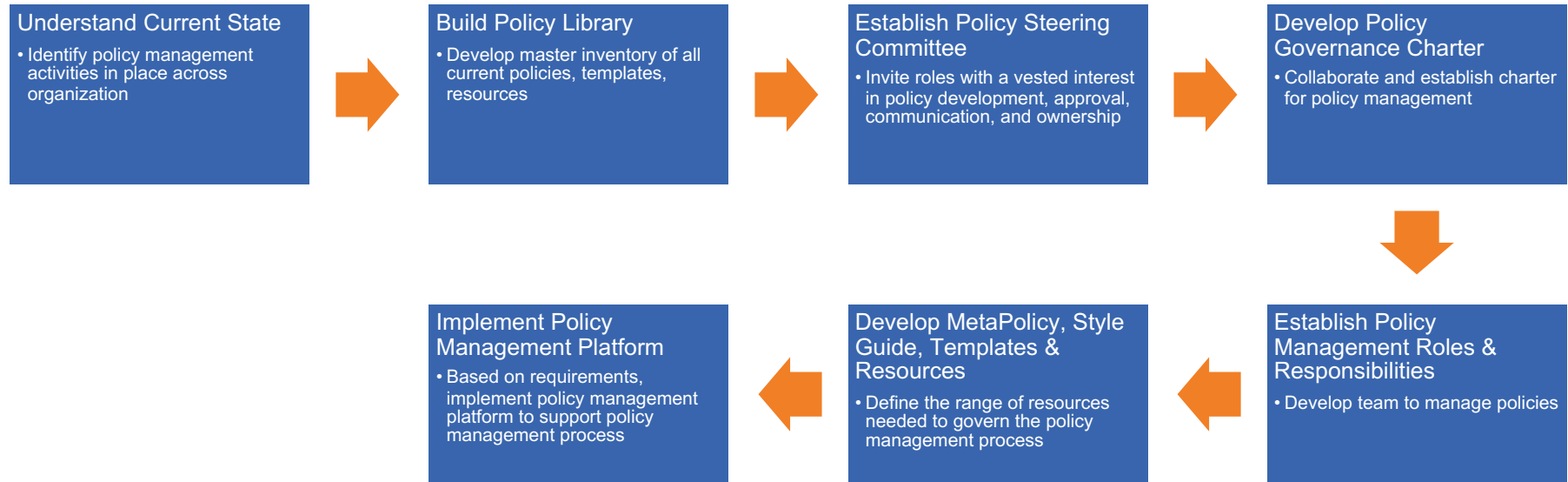
9

Improve Responsiveness & Efficiency

10

Optimize Economic Return & Value

Steps to Building an Enterprise Policy Management Program



Careful Planning is the Key to Success to Policy Management



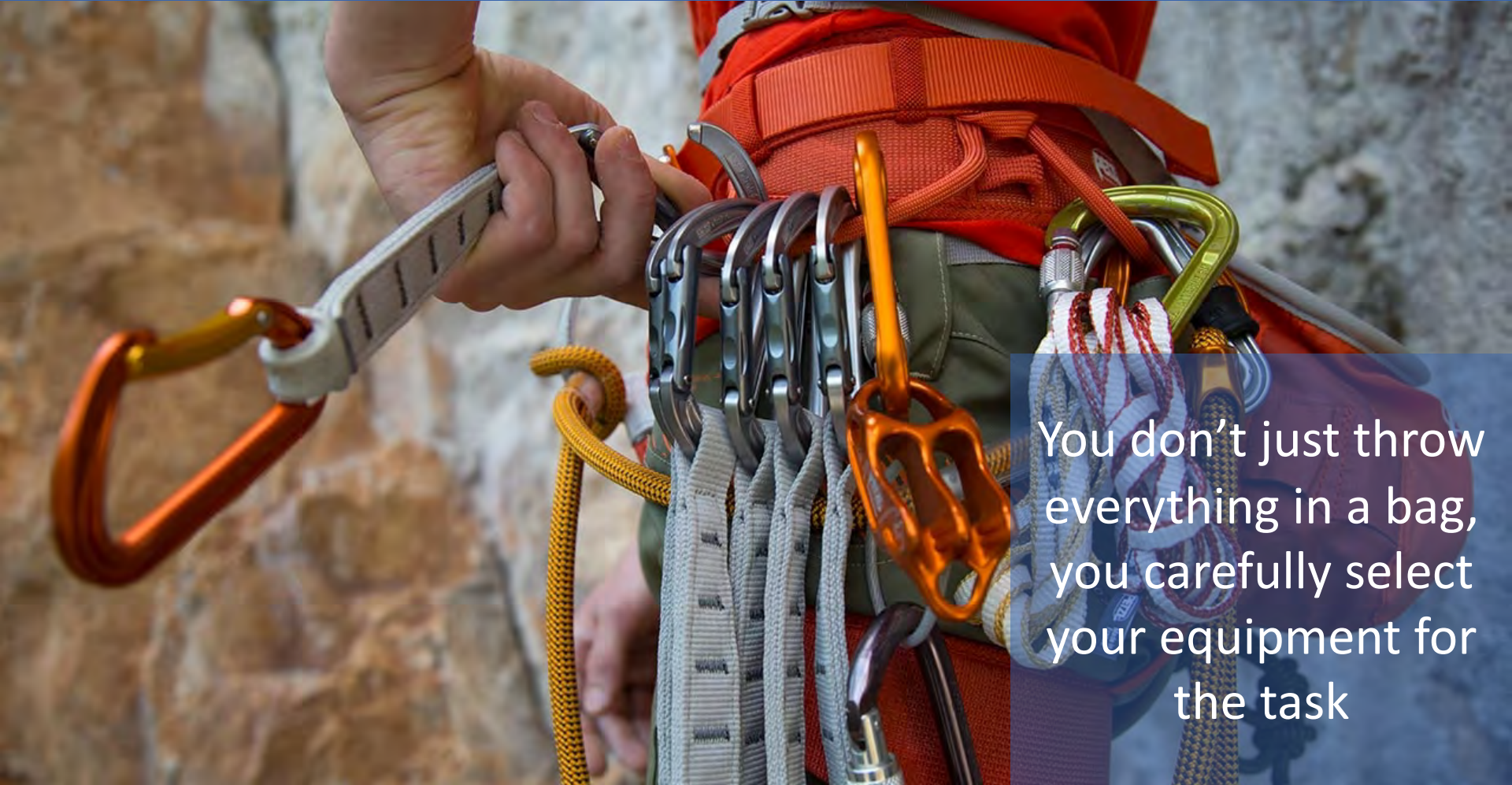
It is critical to plan
your policy
management
journey by laying
out the route
ahead of time

Conditioning is Critical, Make Sure Your Team and Systems are Ready



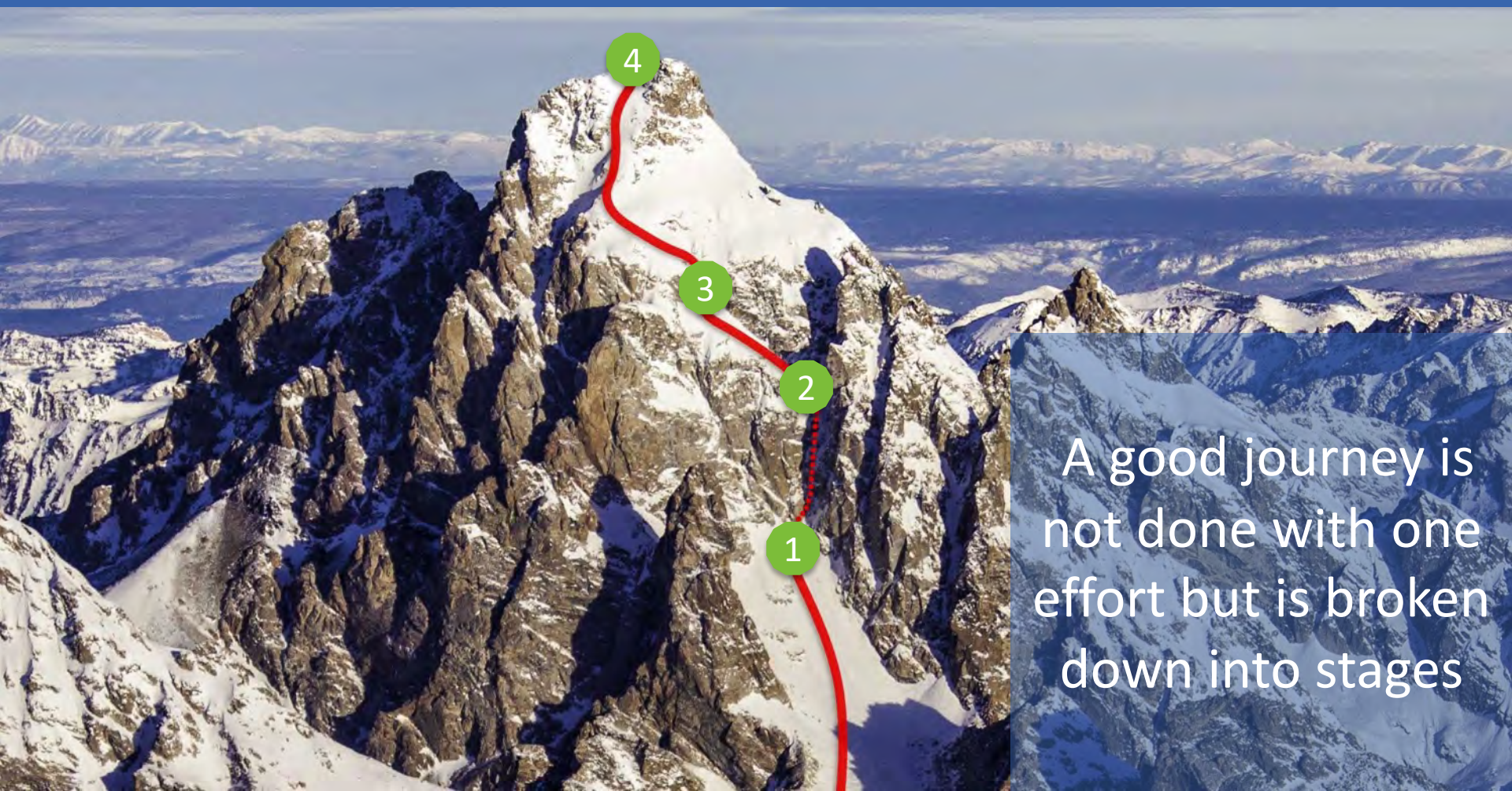
Is your organization prepared for the policy management journey?

Select the Right Equipment for the Policy Management Journey



You don't just throw everything in a bag, you carefully select your equipment for the task

Tackle Your Policy Management Strategy in Stages



A good journey is not done with one effort but is broken down into stages

Preparing for the Next Journey



Once complete it is not over, you begin preparing for the next project

Building a Business Case for Policy Management

THE CONCEPT

Develop a conceptual model outlining:

- The purpose for stronger policy management
- How it will deliver value to the organization
- The audience that you need to persuade

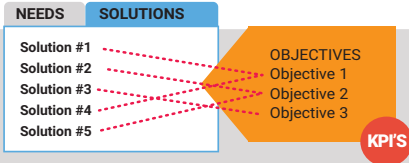
1 PURPOSE

Define a high-level purpose for your business case that encompasses the business need for policy management and the solution that you plan to explore.



2 VALUE

Connect to the business strategy by drawing direct lines from business objectives to policy management and outline the way this should be measured.



3 STAKEHOLDERS

Understand the external and internal stakeholders affected by policy management and how roles, responsibilities and relationships might change.



4 AUDIENCE

Intimately understand who will decide if and how policy management will move forward; and why they should care.



5 BIG IDEA

Sketch out a conceptual model for what policy management might look like; and begin the process of vocally socializing the concept with the audience.



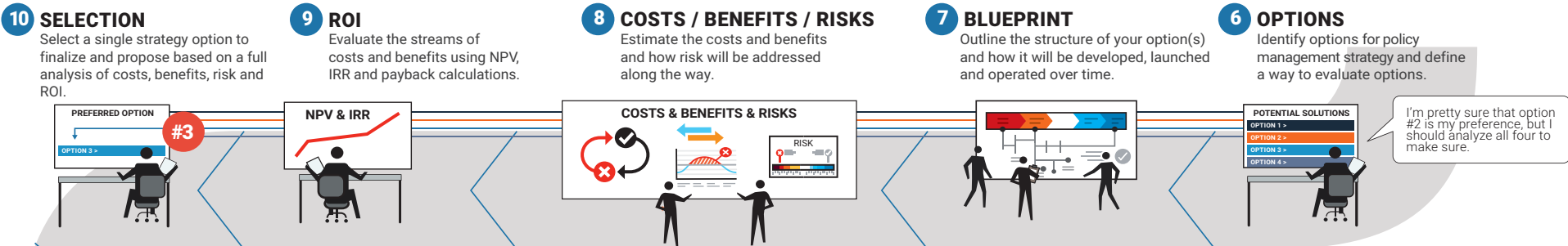
©OCEG, Contact support@oceg.org for comments, reprints or licensing

Building a Business Case for Policy Management

THE ANALYSIS

Develop an analytical model that:

- Identifies and blueprints multiple options,
- Evaluates costs, benefits, risk and ROI
- Selects a single course of action to propose for policy management



©OCEG, Contact support@oceg.org for comments, reprints or licensing

Building a Business Case for Policy Management

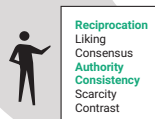
THE PITCH

Develop a pitch that persuades your audience using:

- Narrative and visual design
- Physical presence
- Scientific (and ethical) techniques of persuasion

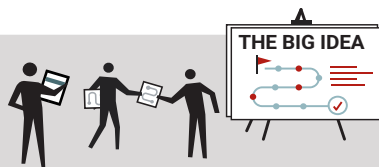
11 PERSUASION

Use ethical and scientifically proven principles of persuasion to convince your audience.



12 NARRATIVE

Use effective storytelling to transform your message into a compelling and memorable narrative.



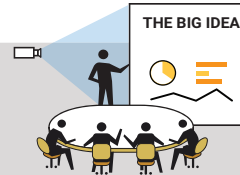
13 MEDIA

Use the principles of effective visual and audio design to communicate your business case.



14 PRESENTATION

Use in-person presentation and other interpersonal skills to present the business case to the audience.



15 FOLLOW-UP

Ensure that a final decision is made with ongoing follow-up and communication.



©OCEG, Contact support@oceg.org for comments, reprints or licensing

Building a Business Case for Policy Management

THE POLICY MANAGEMENT BUSINESS CASE OF VALUE

A change in policy management strategy requires a clear and compelling business case of value. This starts with understanding the current state in how policies are managed and defining the proposed future state. In contrasting these two states the organization builds a business case of value around the angles of *efficiency*, *effectiveness*, and *agility*.



EFFICIENCY

TIME

Estimate how many hours of employee time will be saved by streamlining and standardizing processes and/or changing technology.

MONEY

Estimate the amount of money saved by the proposed changes based on reduced employee hours in managing policies, legal fees and fines that may arise from noncompliance, and removal of redundant technologies.



EFFECTIVENESS

CONSISTENCY

Demonstrate examples of problems arising from lack of consistency and improvements resulting from the proposed change.

ACCOUNTABLE

Demonstrate how an improved system of record can assist in resolving issues, identifying needed control changes and proving efforts to stakeholders, regulators and enforcement authorities.



AGILITY

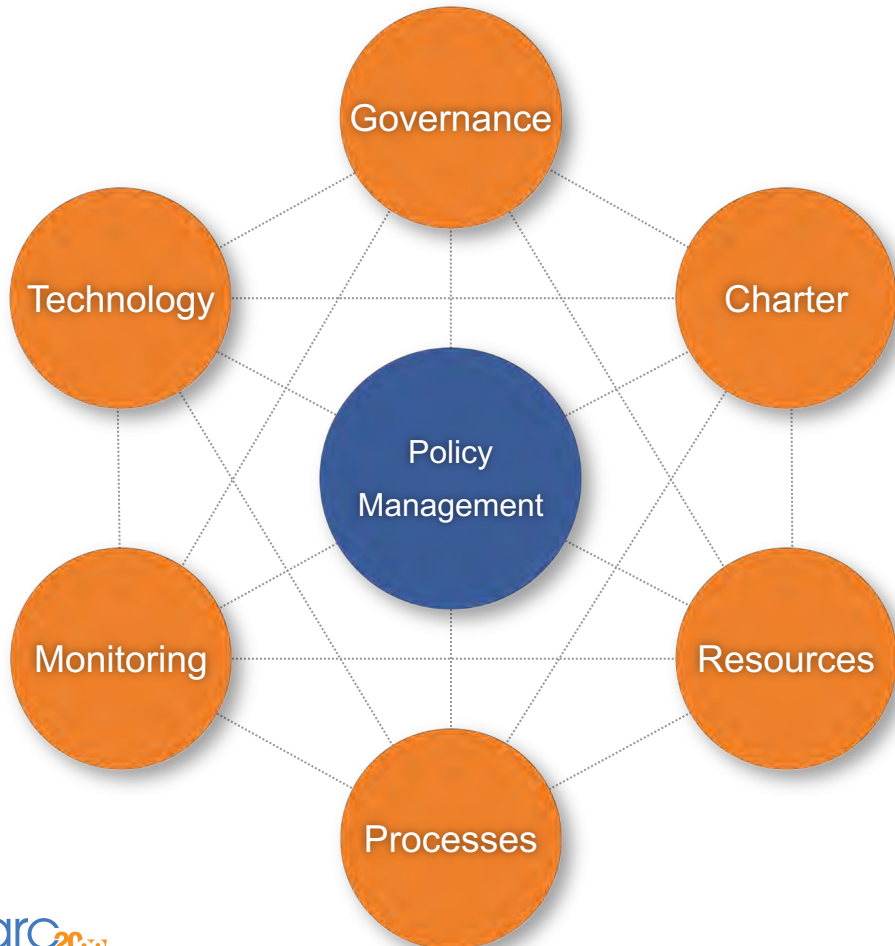
CHANGE

Show how there can be connection between procedures and systems for identifying regulatory, business and other changes and the proposed procedures and systems for policy management.

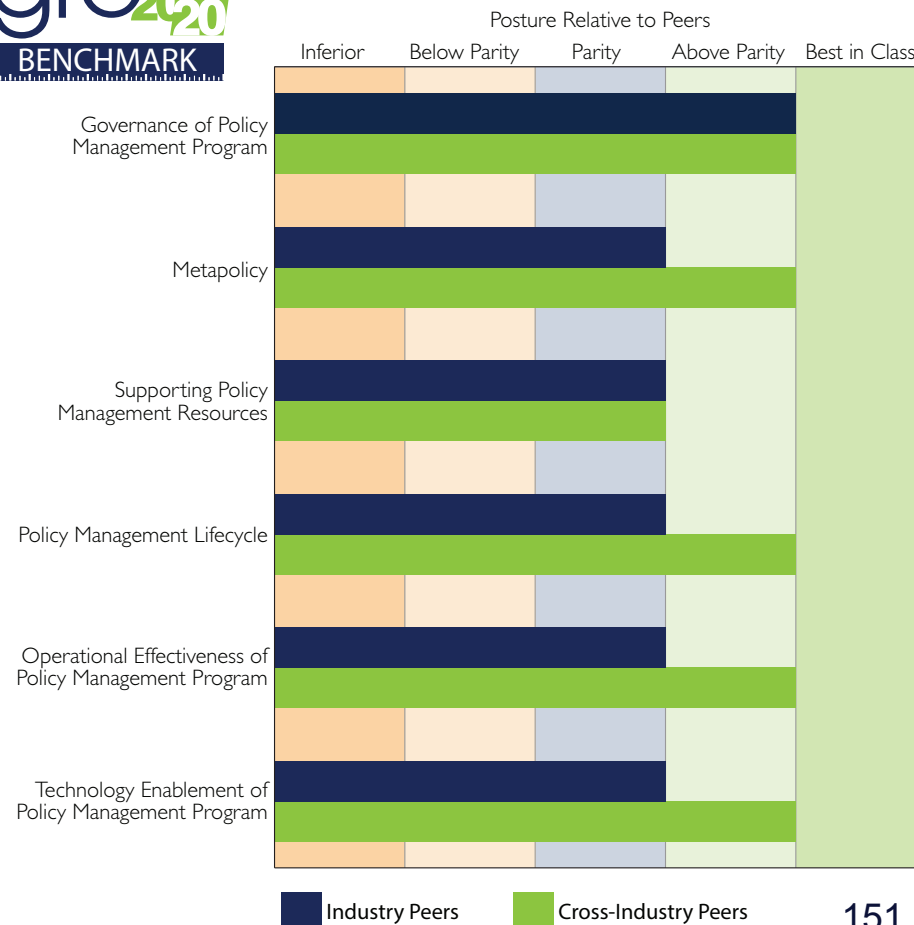
RESPONSIVE

Demonstrate how the identification and notification systems proposed will increase responsiveness and agility to address changes and ensure policy conformance.

GRC 20/20's Effective Policy Management Benchmark



EFFECTIVE POLICY MANAGEMENT





Workshop Activity

Our Agenda . . .

1) PART 1: Policy by Design

Why Policies Matter

2) PART 2: Policy Governance

Blueprint for Effective Policy Management

3) PART 3: Policy Management Lifecycle

Managing Policies from Creation to Dissolution

4) PART 4: Policy Management Architecture

Enabling Information & Technology Management of Policies



Questions?

Michael Rasmussen, J.D.
The GRC Pundit & OCEG Fellow
mkras@grc2020.com
+1.888.365.4560

Subscribe

GRC 20/20 Newsletter



LinkedIn: GRC 20/20



LinkedIn: Michael Rasmussen



Twitter: GRCPundit



Blog: GRC Pundit

