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) Policy by Design – Creating an effective Policy Management Framework

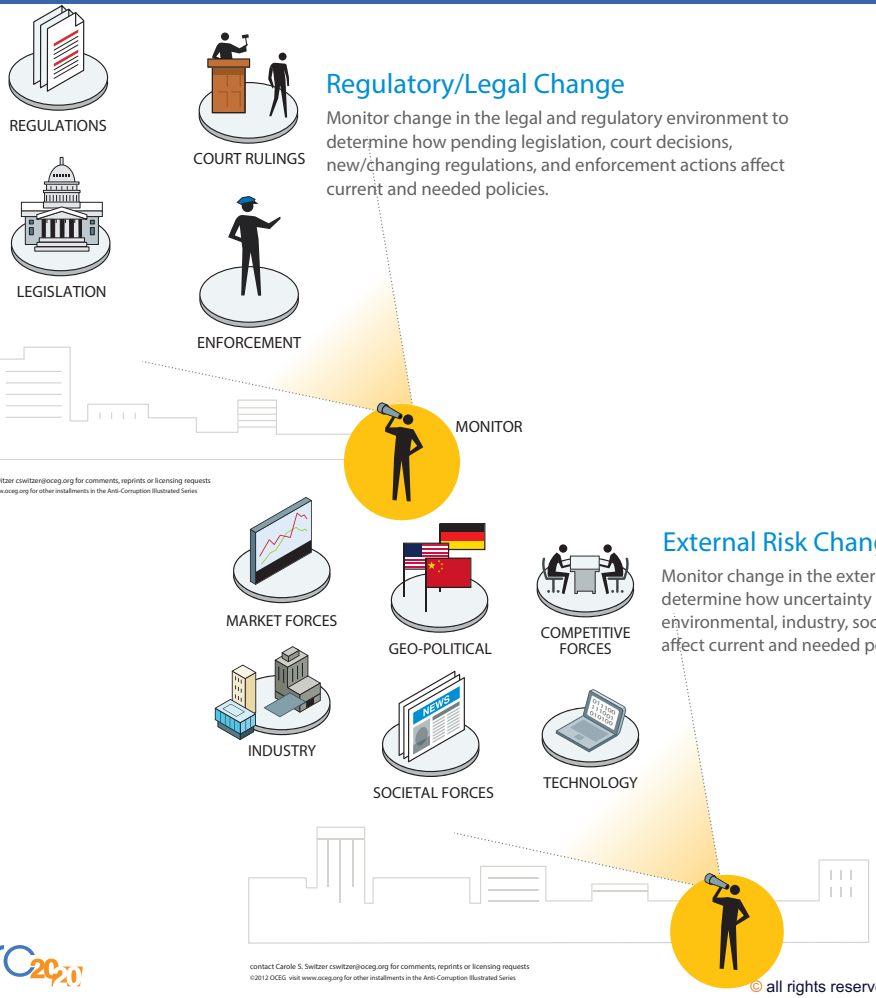
2) Mapping Regulation to Policy, Processes & Controls

Workshop Activity

PART 1

Policy by Design – Creating an effective Policy Management Framework

Change is the Greatest Challenge Impacting Policy Management



Regulatory/Legal Change

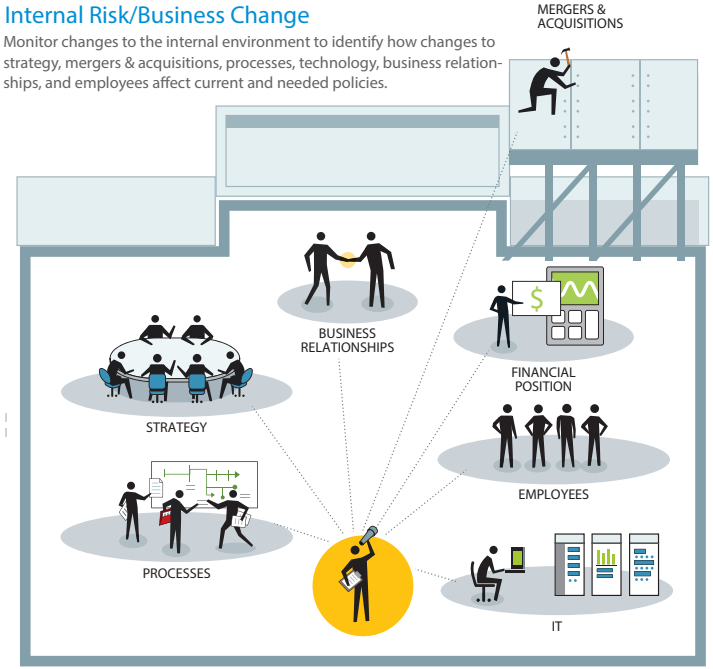
Monitor change in the legal and regulatory environment to determine how pending legislation, court decisions, new/changing regulations, and enforcement actions affect current and needed policies.

External Risk Change

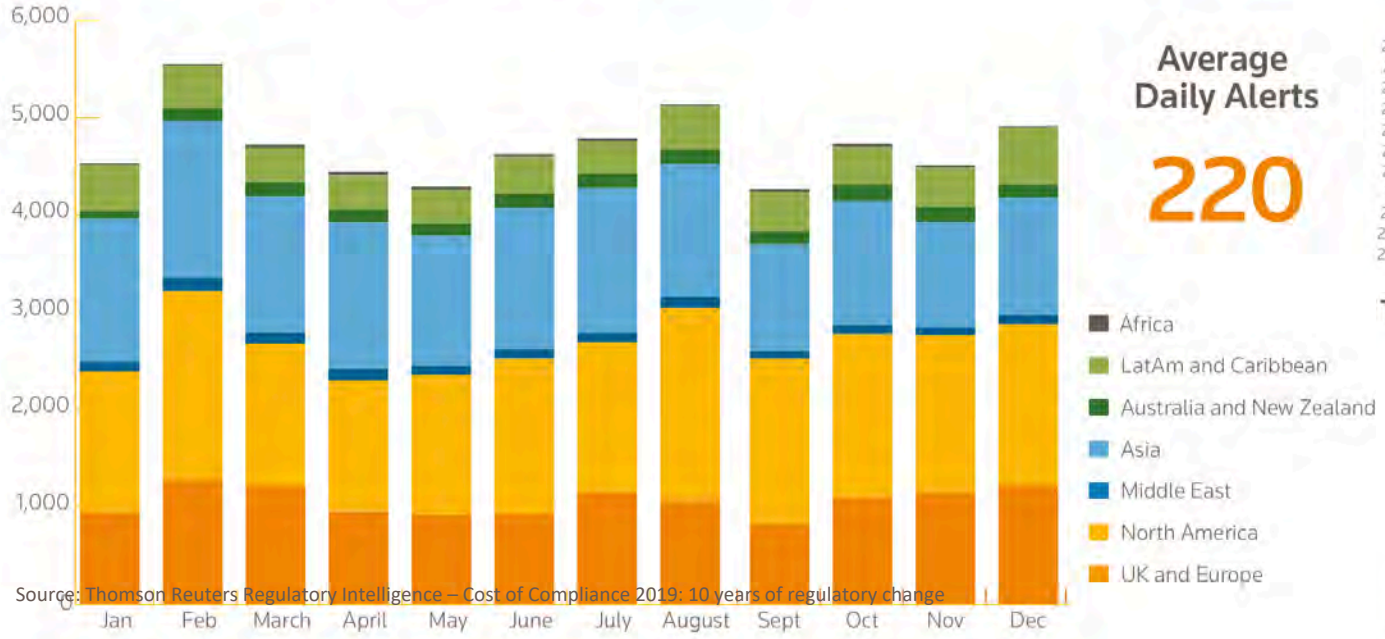
Monitor change in the external risk environment to determine how uncertainty in economic, geo-political, environmental, industry, societal, and market forces affect current and needed policies.

Internal Risk/Business Change

Monitor changes to the internal environment to identify how changes to strategy, mergers & acquisitions, processes, technology, business relationships, and employees affect current and needed policies.



Regulatory Activity in Financial Services 2008 to 2018

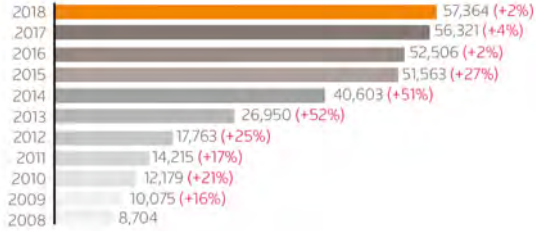


Source: Thomson Reuters Regulatory Intelligence – Cost of Compliance 2019: 10 years of regulatory change

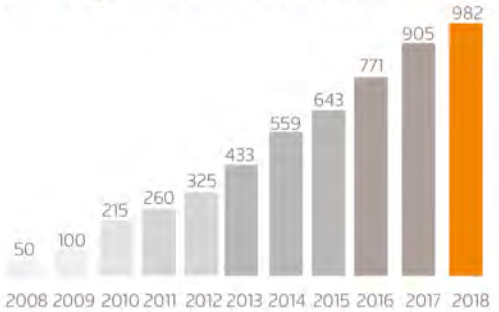
Average Daily Alerts

220

Total Yearly Alerts



Total Organisations Monitored



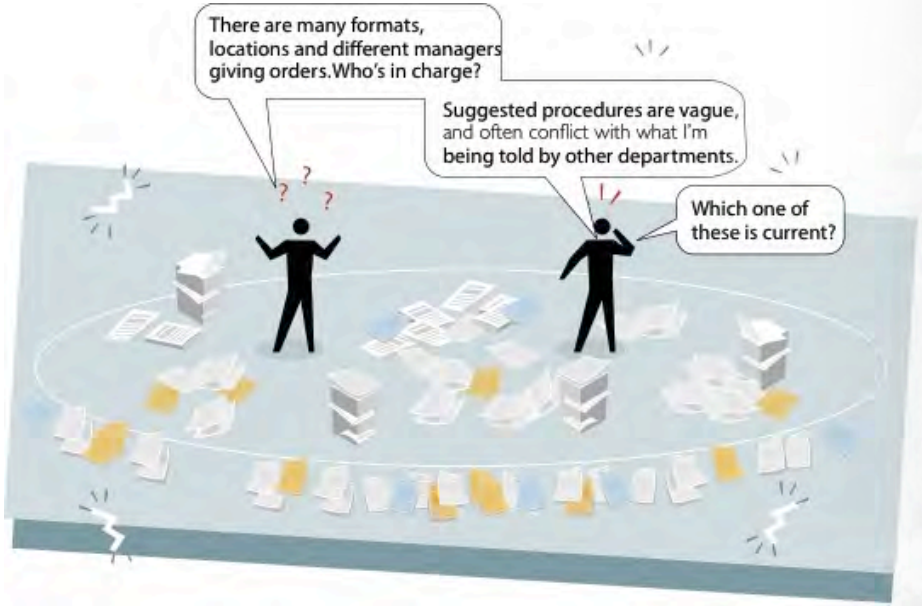
Compliance in Transition: From Old Ways to New Ways

ACCOUNTABILITY VS RESPONSIBILITY

(a subtle but very powerful difference)

Battling the Hydra of Ineffective Policy Management

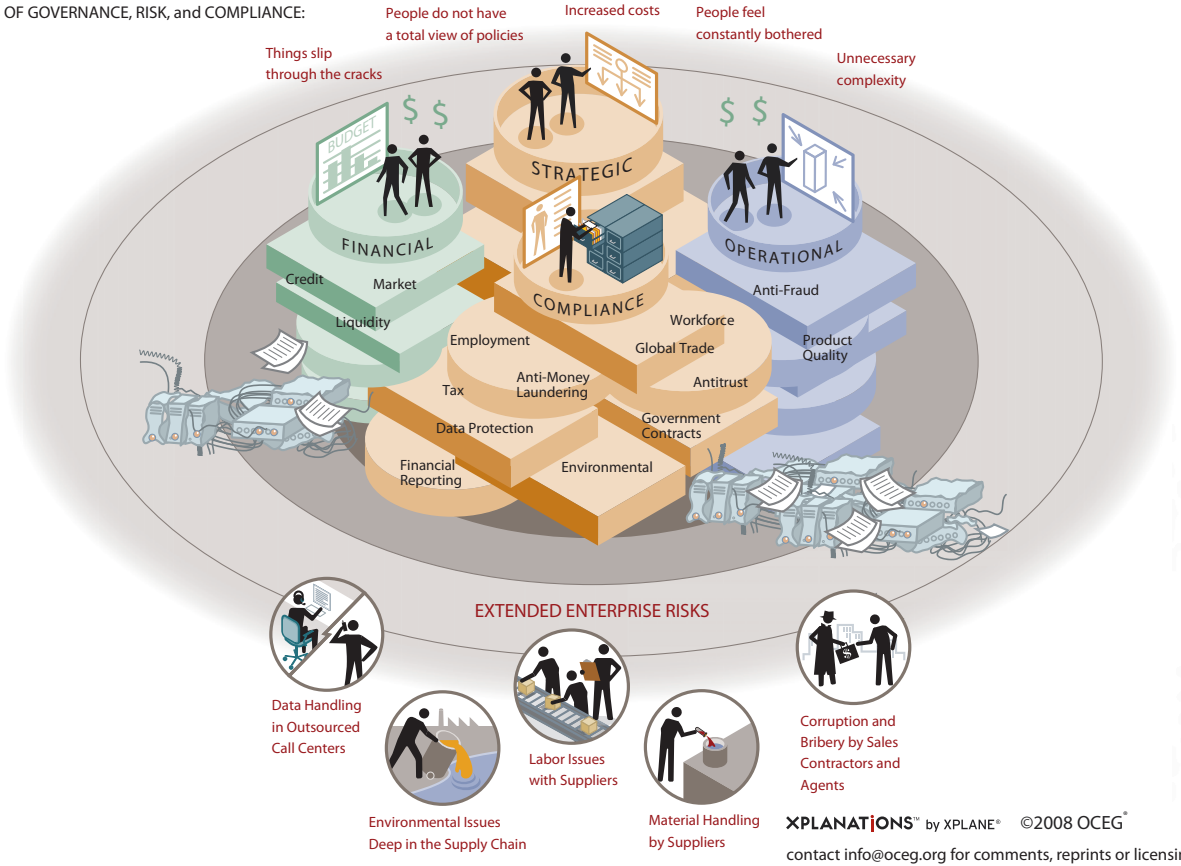
… Confusing Policy Management User Experience



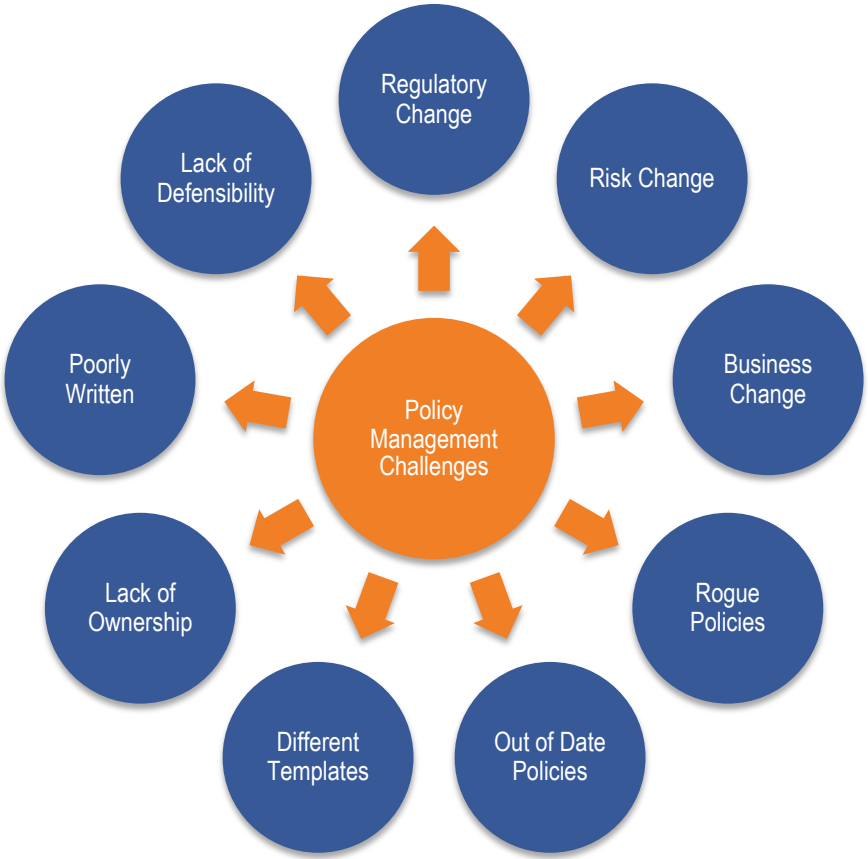
Policy Discovery & Inventory: Do You Know Where Your Policies Are?

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:



Drivers in Policy Management



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

GRC is the integrated collection of capabilities that enable an organization to:

G) reliably achieve objectives

R) while addressing uncertainty and

C) acting with integrity.

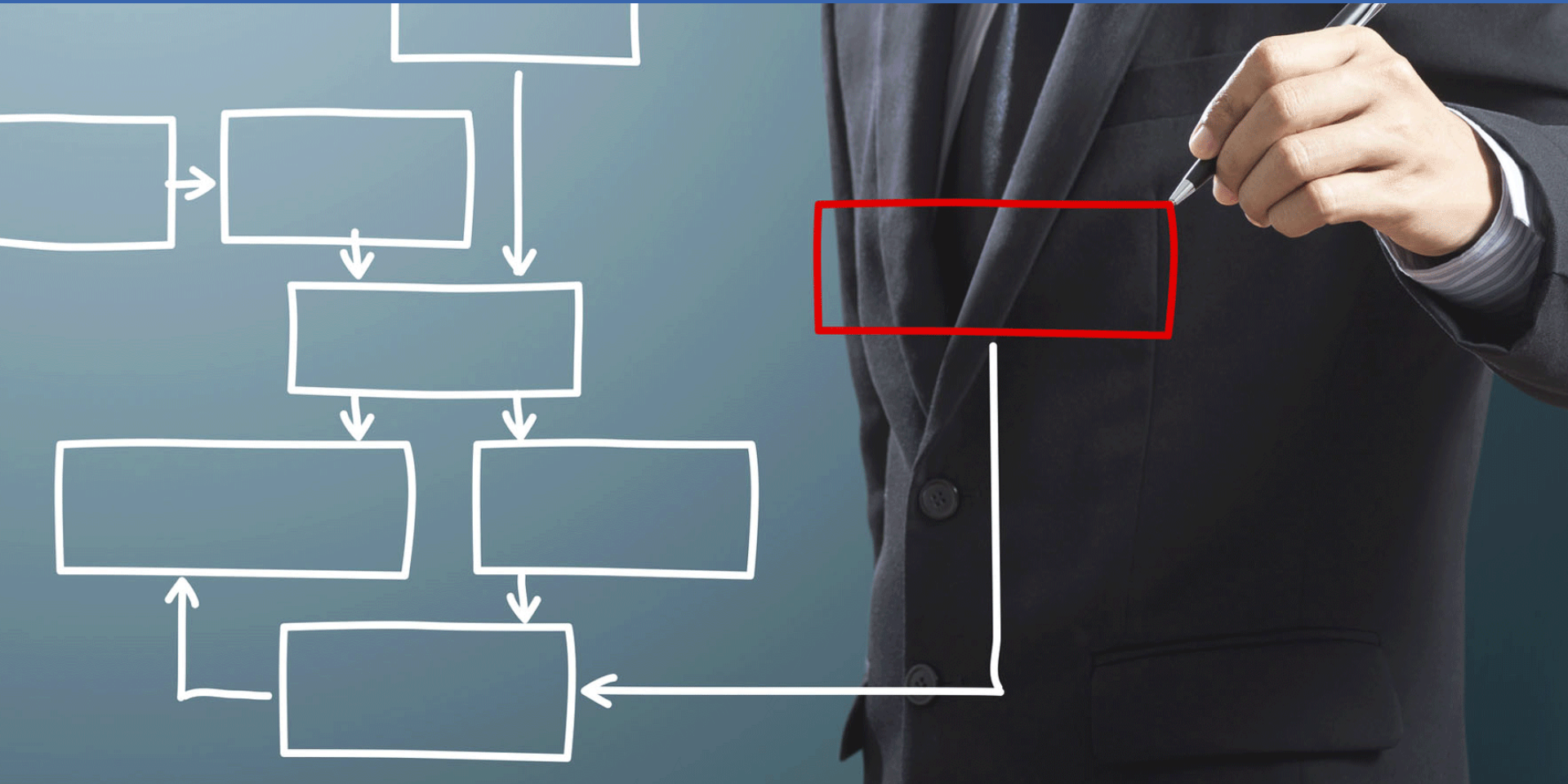
SOURCE: OCEG GRC Capability Model

Integrity: the Core of What Compliance is About

Policy Assurance: Do the frontlines understand policies?

Policy Assurance: Is the organization collaborating on policies?

Policy Assurance: How are policies understood in context of operations?



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

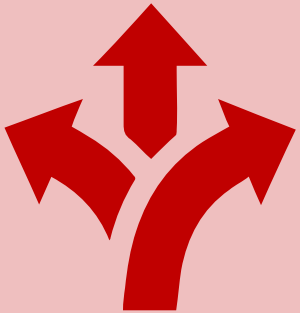
Mobility: Policy Communication Done & Delivered Anywhere at Anytime

What if we could design 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

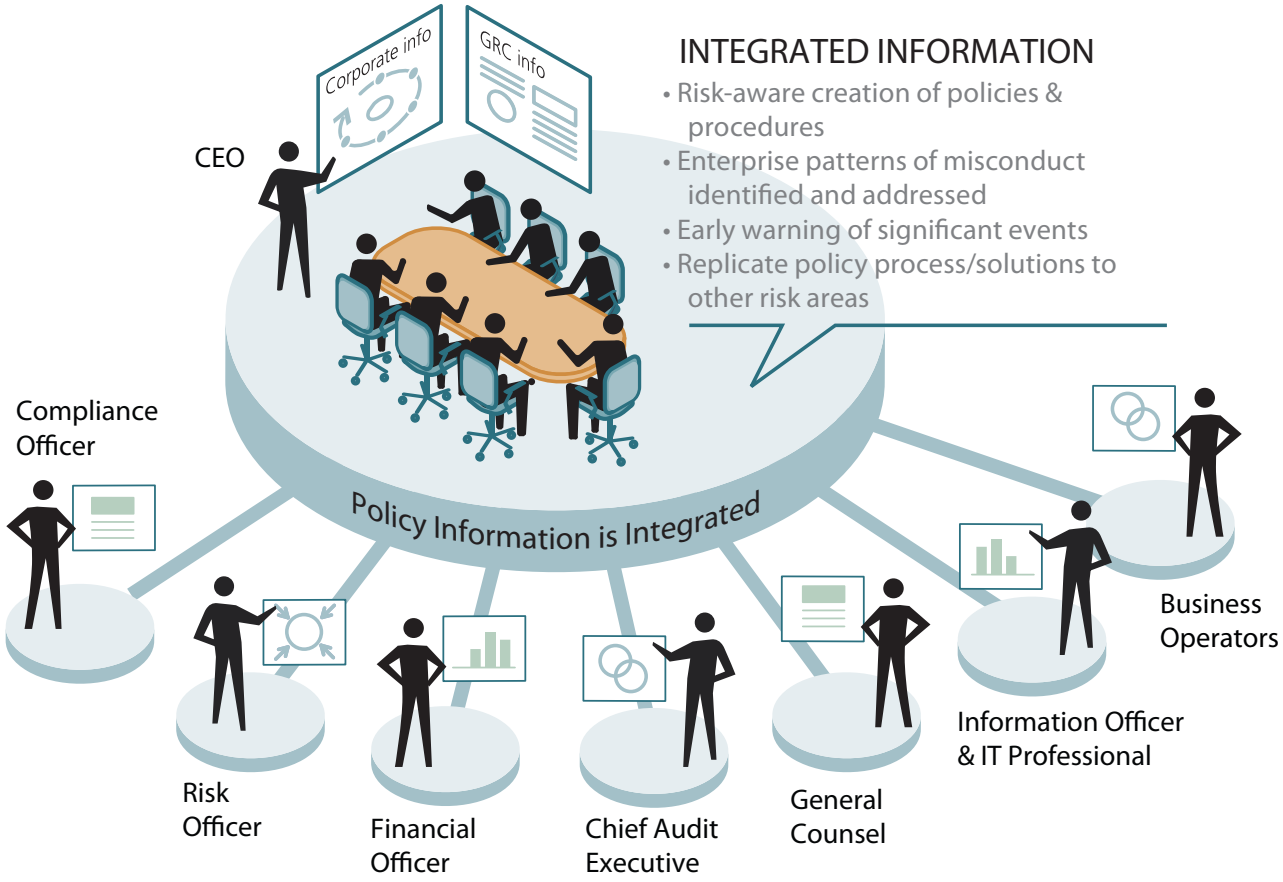
- An integrated approach that balances policy management centralization with distributed participation and collaboration

Policy Management Maturity Improvement: a Top Down Approach

- Policy Management Strategy
- Policy Management Process
- Policy Management Information
- Policy Management Technology

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 responseversus 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

Mission Statement

STATEMENT

Accountability

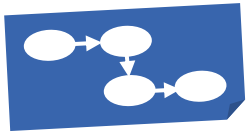
REPORTING

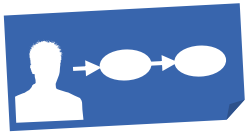
Roles Groups Involved

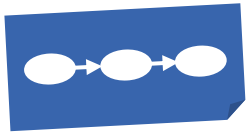
PERSONAS

Policy Management Lifecycle & Responsibilities

PROJECTS







Resources

METAPOLICY

STYLE GUIDE

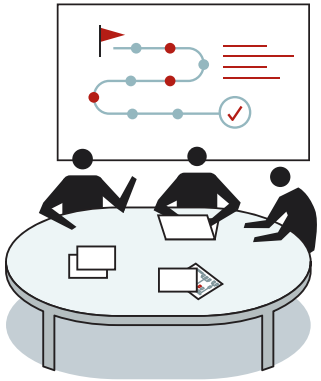
TEMPLATES

FORMS

Roles in Policy Management

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 manaqer; 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.

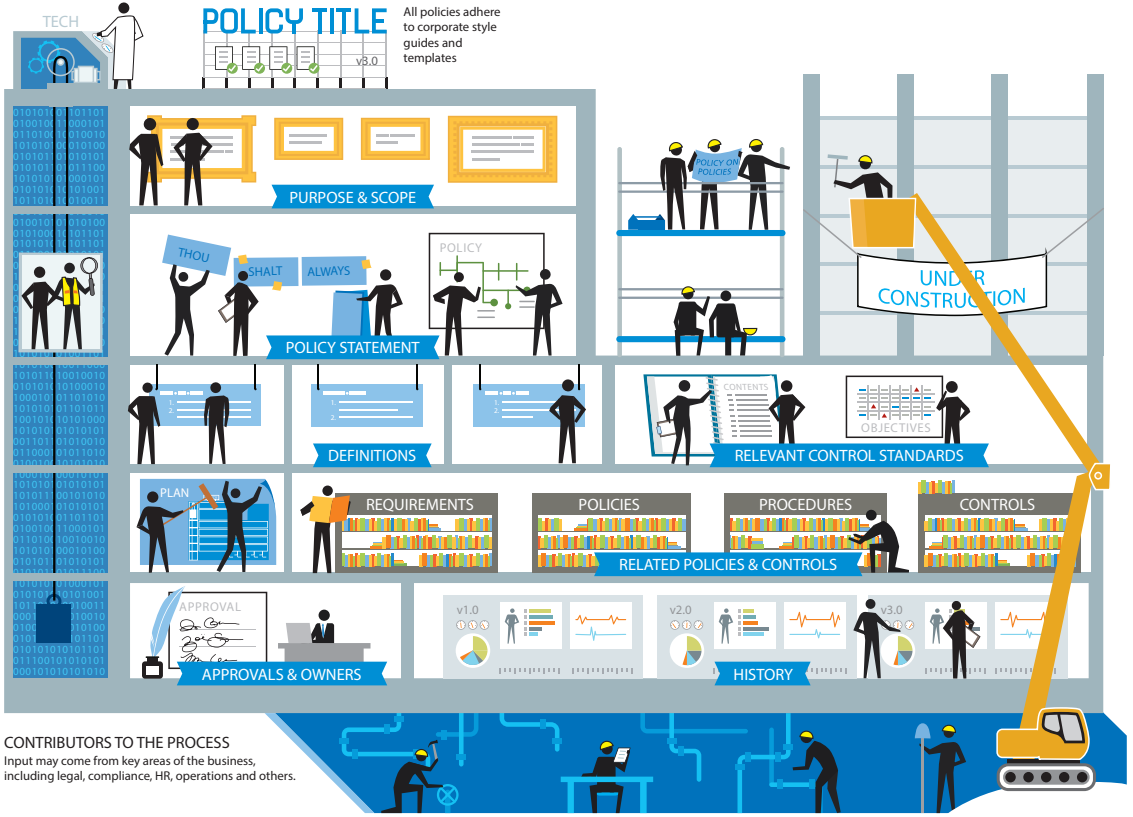
POLICY AUTHOR

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.

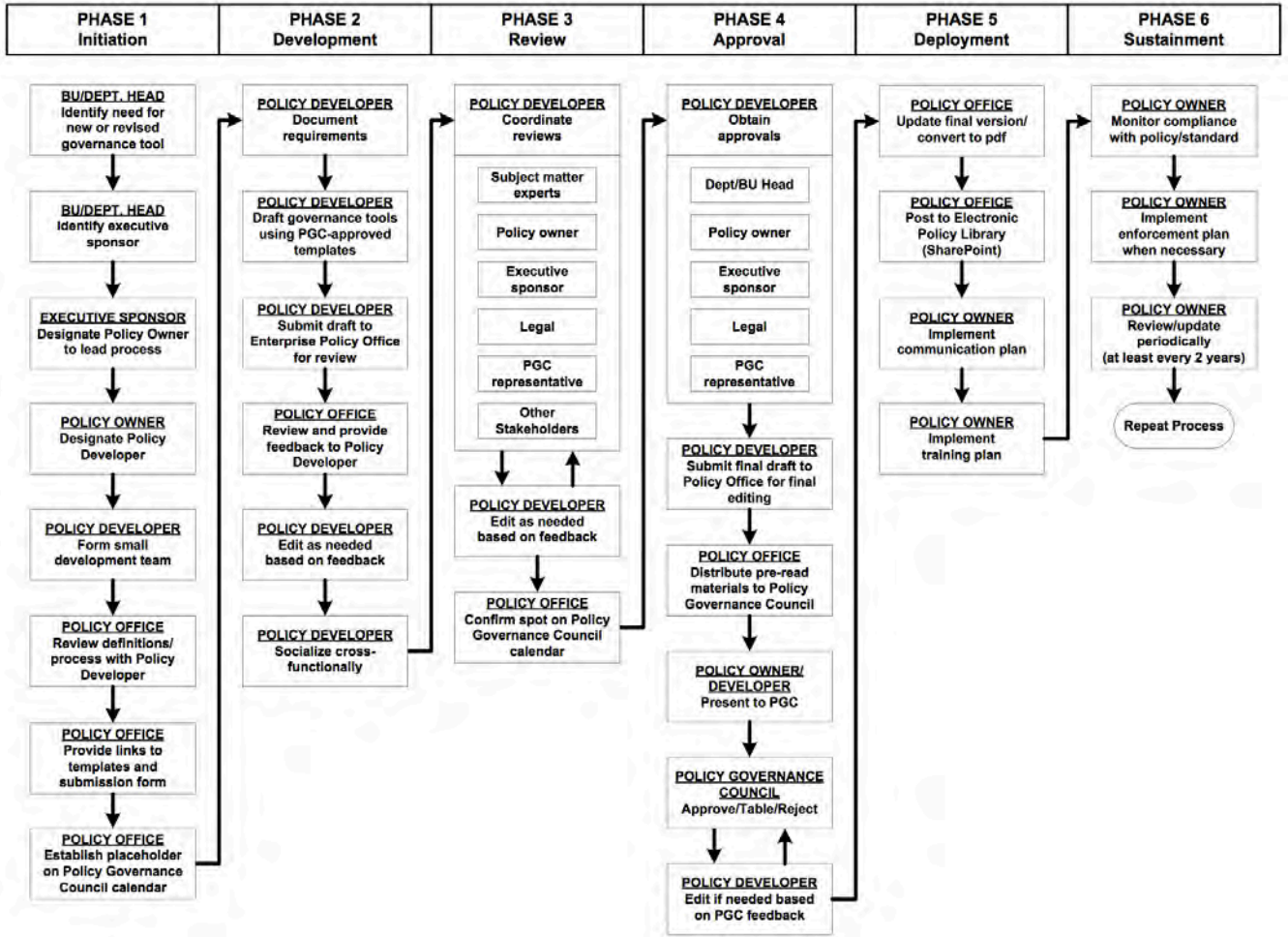
MetaPolicy: The Policy on Writing Policies

Start with a MetaPolicy that has support from Executive Management

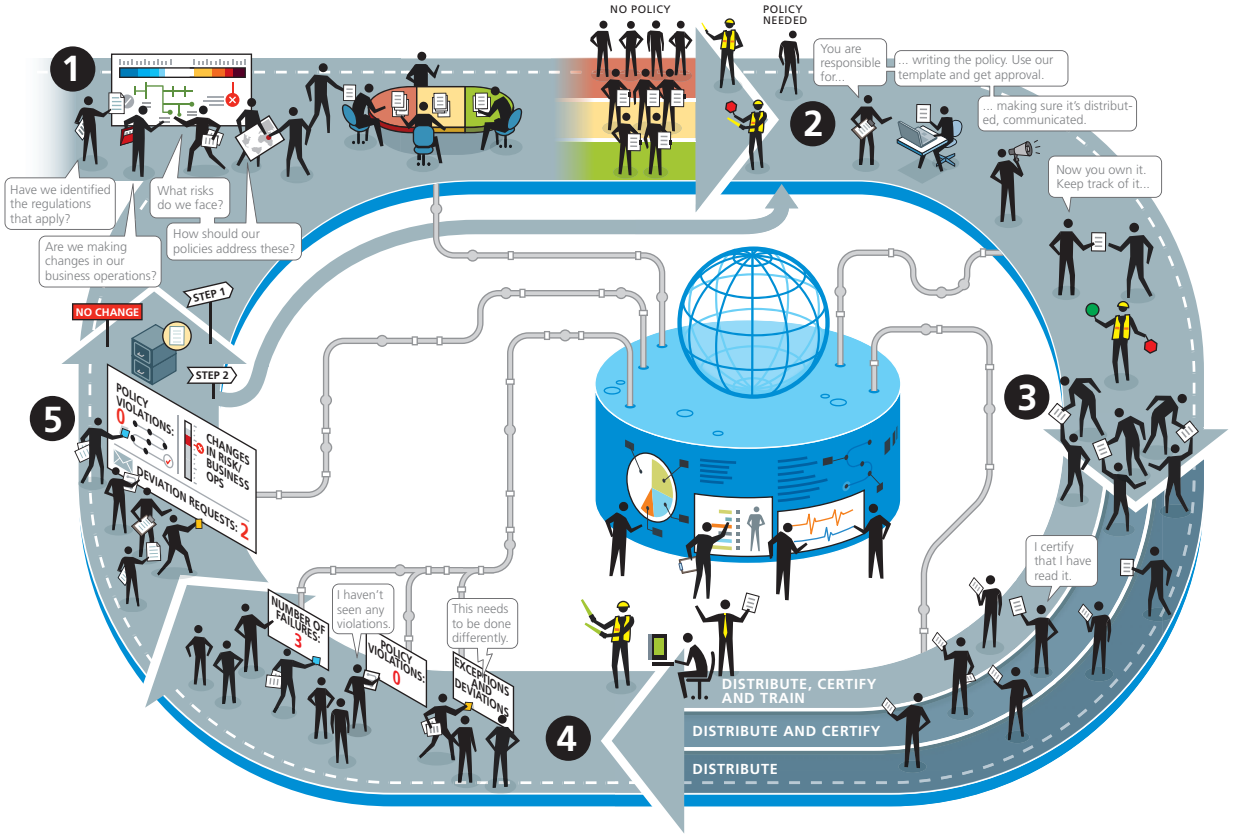
- Brings integrity and value to policy management
- Provides accountability to policy management processes that are often scattered across the organization
- Enables policy management to work in harmony across organization functions delivering efficiency, effectiveness, and agility
- Well-governed and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



MetaPolicy Process Example 1: Policy Development Process



GRC 20/20's Effective Policy Management Lifecycle



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

When to Write a Policy

DANGER
Don't let your policy house fall into disrepair.

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?

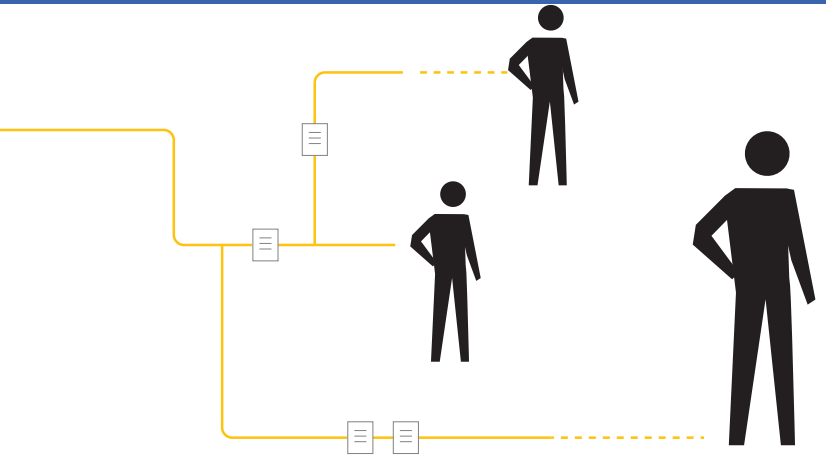
How did we handle this without a policy?

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) 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

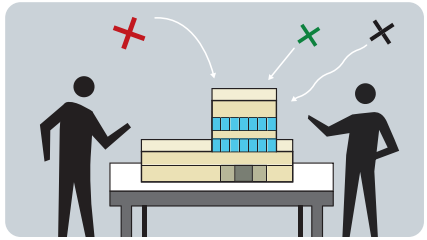
2 BUSINESS ANALYSIS

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

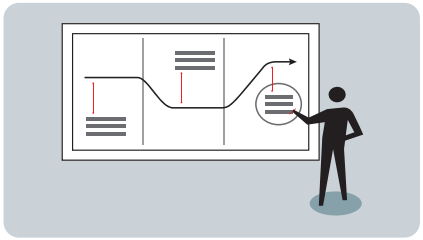
This analysis includes multiple parts that focus on risk, company history and overall industry practices.

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

ANALYZE RISKS



UNDERSTAND HISTORY



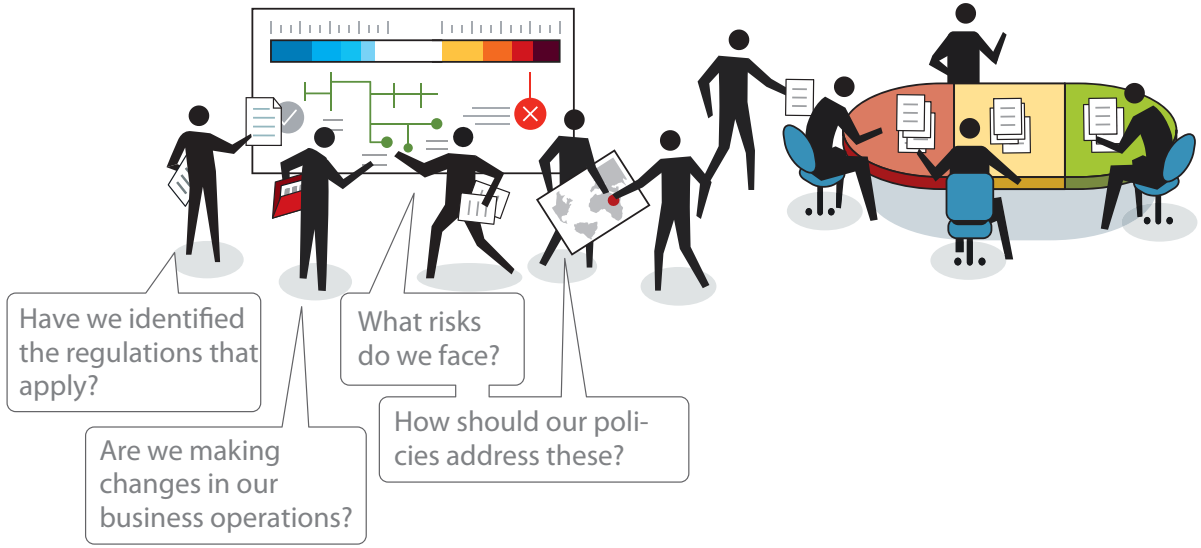
REVIEW EXISTING POLICIES

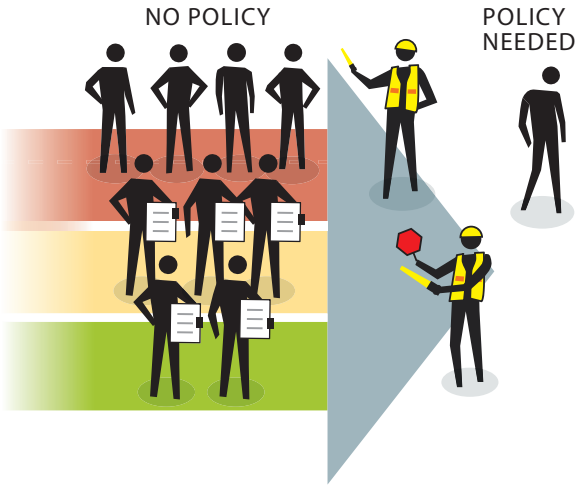
3 DETERMINE ACTION

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.

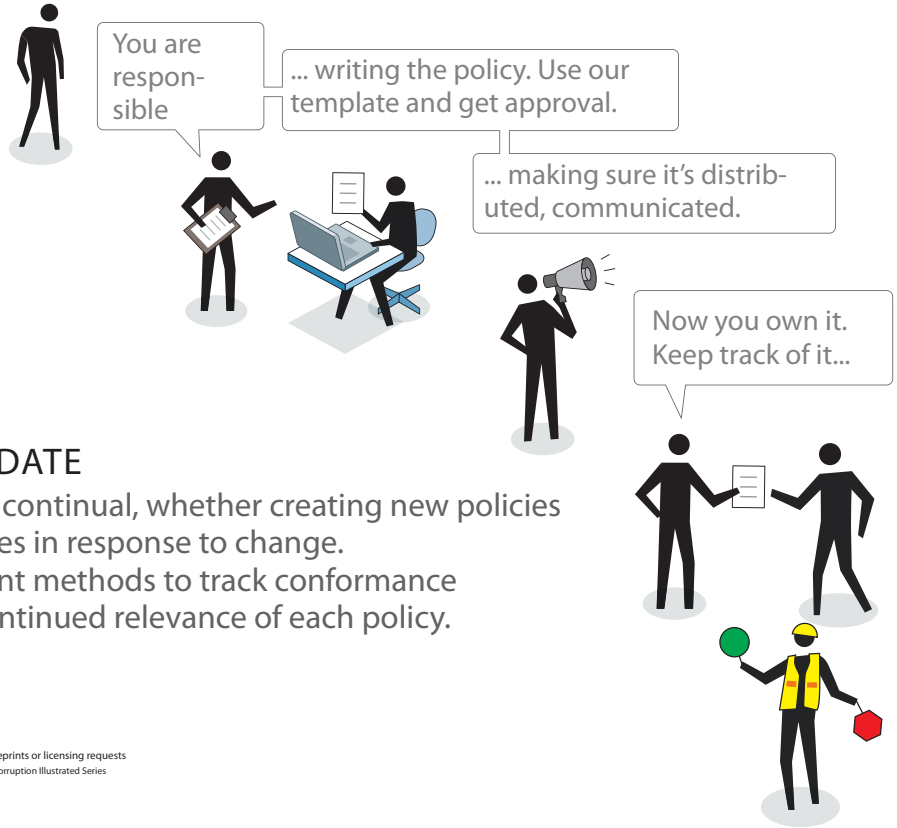
Determine Policies that Need to be Changed

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.





Assign Policy Development Responsibilities

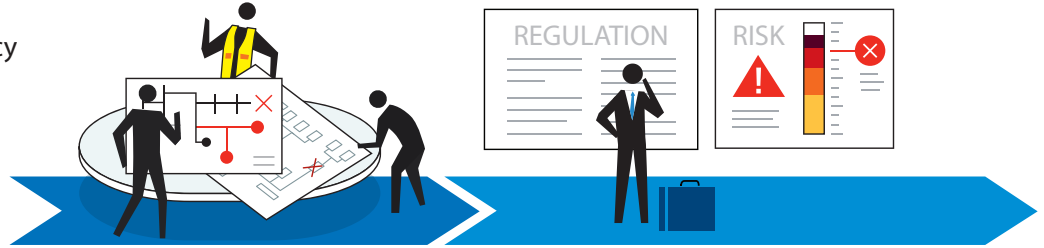


DEVELOP AND UPDATE

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.

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

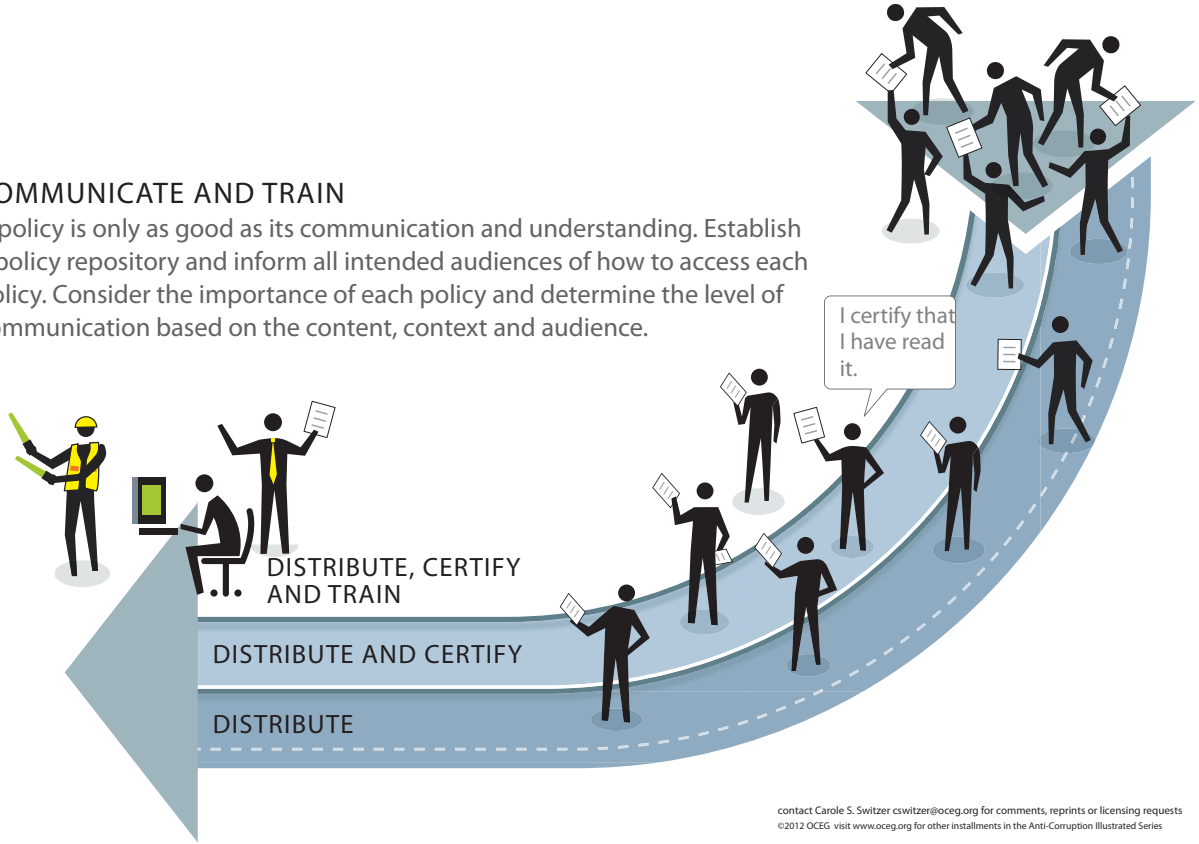
Identification of major implementation considerations and questions to aid the Policy Owner and Implementation Team in crafting strategies to deal with them, e.g.:

- Stakeholder Considerations
- Risk Management Considerations
- Communication Considerations

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.



Policy Pull and Policy Push Mechanisms

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

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

Elements of a Policy Communication Plan

COMMUNICATION 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 and training program to be accessible, understandable and actionable by all groups regardless of education level, geography, culture, language, ethnic group or disability status.

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

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

INTERNAL 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.

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.

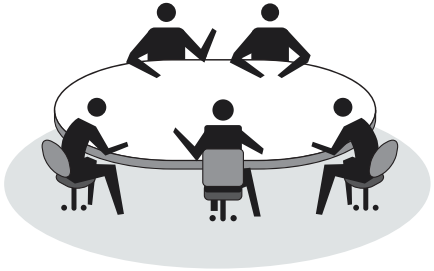
Medium Relevance

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

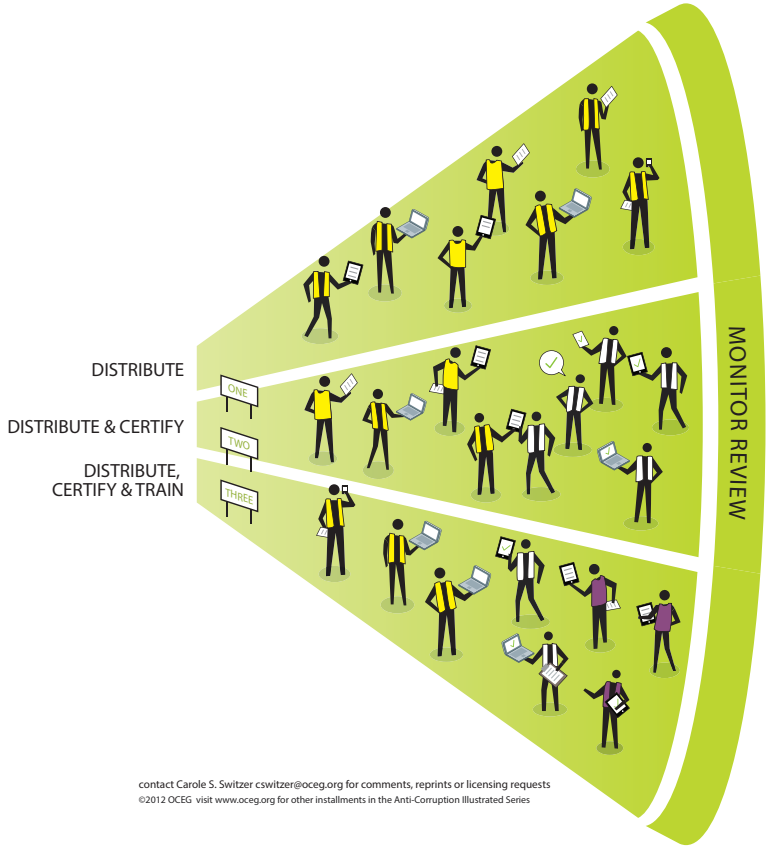
No Relevance

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

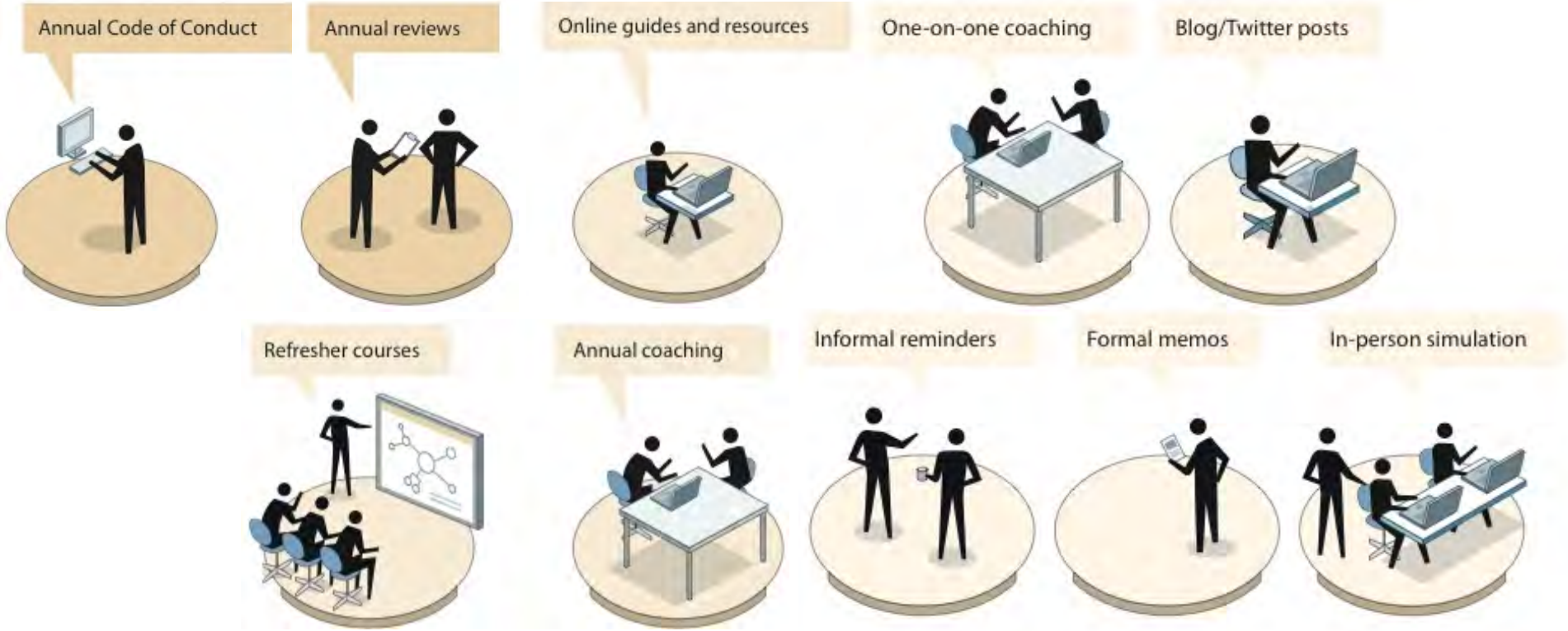
Policy Team Approves Plan & Initiates Communication



The communication team for a policy is established to ensure that the appropriate commitment of resources and strategy are in place to successfully communicate and train individuals on the policy and its requirements.



Methods to Communicate a Policy & Increase Awareness



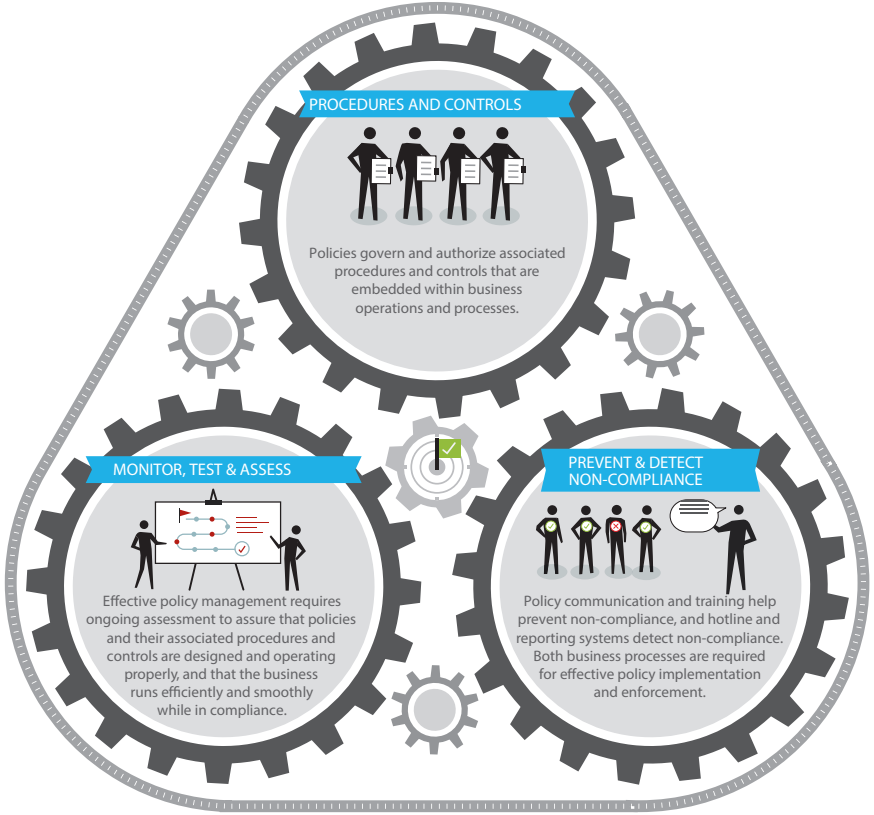
1 Determine Need | 2 Develop & Approve | 3 Communicate & Train | 4 Monitor & Enforce | 5 Measure & Maintain

Implement, Monitor & Enforce Policies

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

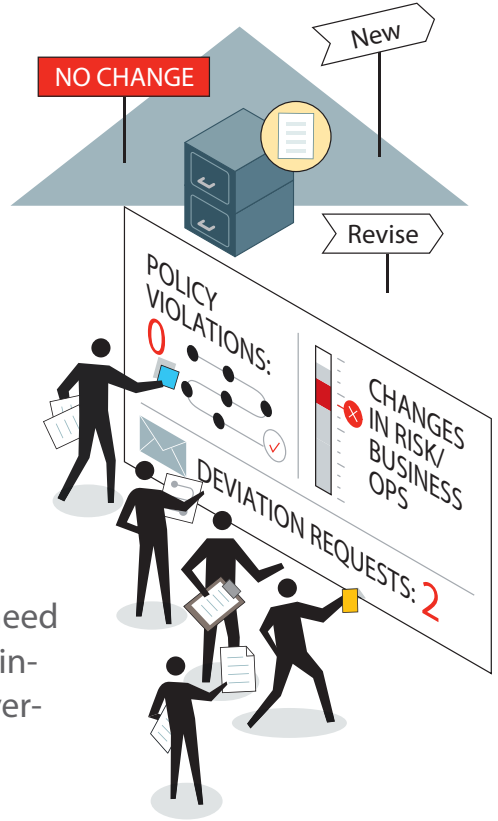


It is Critical to Document and Manage Policy Exceptions and Exemptions

- 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, Re-Evaluate & Maintain Policies



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.

Measure the Design as Well as Operational Effectiveness of Policies

Design Effectiveness

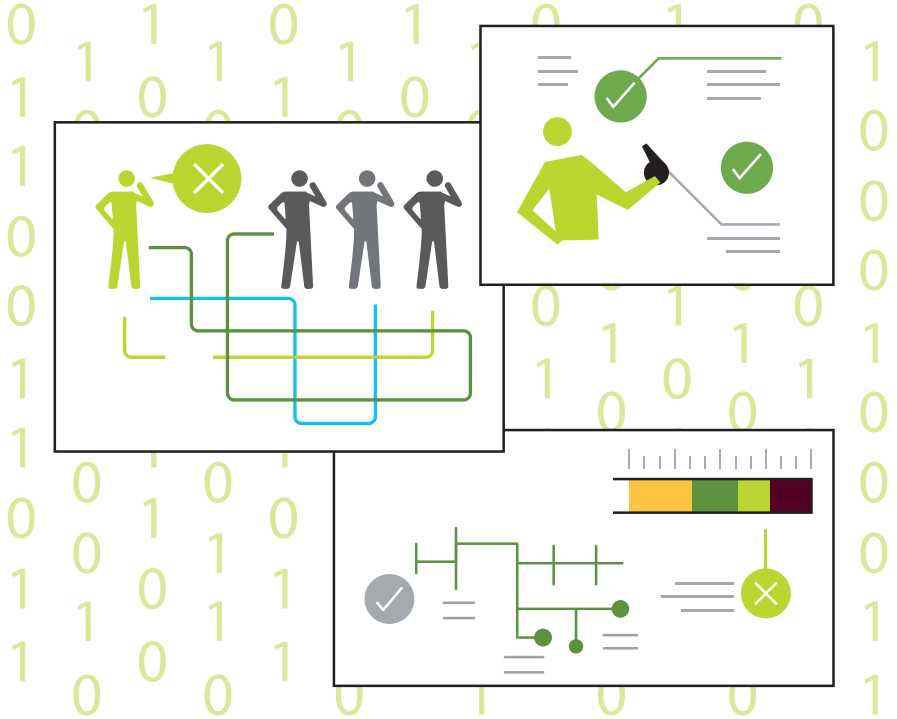
- An organization begins with understanding if the policy system is effectively designed.
- To determine this, an organization documents policies and processes.
- Ultimately, the organization must judge if all of these policies, processes, and the system as a whole are designed such that it will satisfy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



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?

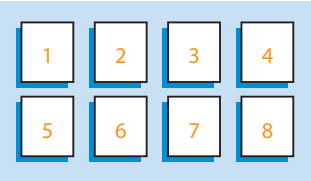
TRAINING
Have employees successfully completed required training programs related to this policy?

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?

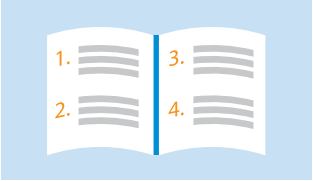
1 Determine Need | 2 Develop & Approve | 3 Communicate & Train | 4 Monitor & Enforce | 5 Measure & Maintain

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



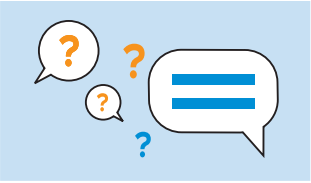
VERSION (DATE, TIME)

The organization needs to have an auditable record of the versions and communication activities around policies to have an effective compliance program.



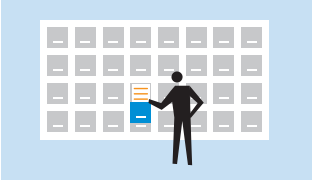
TESTING

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



QUESTIONS

It is necessary that individuals have a way to get questions answered about policies that remain after training and communication.



ACCESSING PAST RECORDS

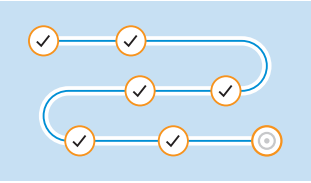
To defend itself and validate an effective compliance/policy program the organization should be able to have a complete history of policy communication and training from the past.

EXCEPTIONS

Exceptions to the policy, and training/ communication plan, are to be documented, approved, and periodically evaluated.

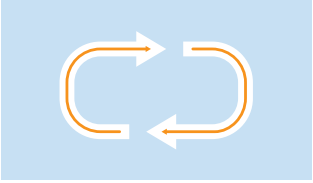
DEFENSIBILITY

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



TRACKING

The organization should have a complete record of all training and communications of policies so they can show what, when, where, why, and how communication took place.

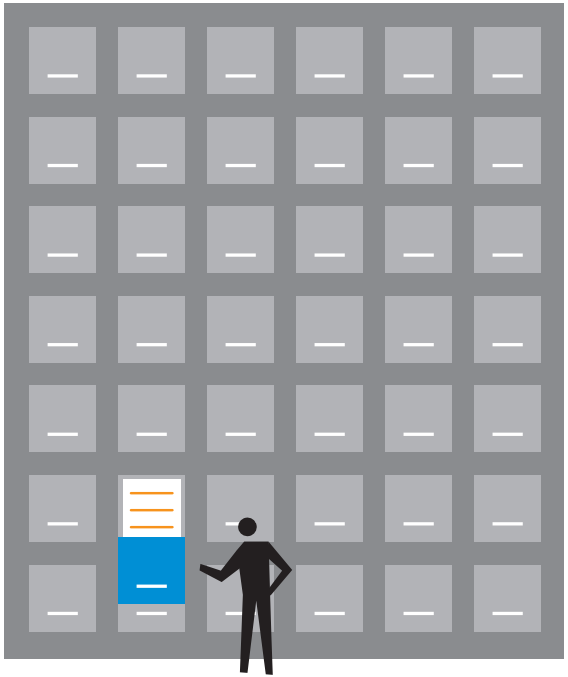


REPEATABLE CYCLE

Policy communication and training are not a one time effort. To guide behavior and defend the organization requires consitent communication and training and learning from the results of previous efforts.

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.



Implement a Periodic Review Cycle to Maintain Policies

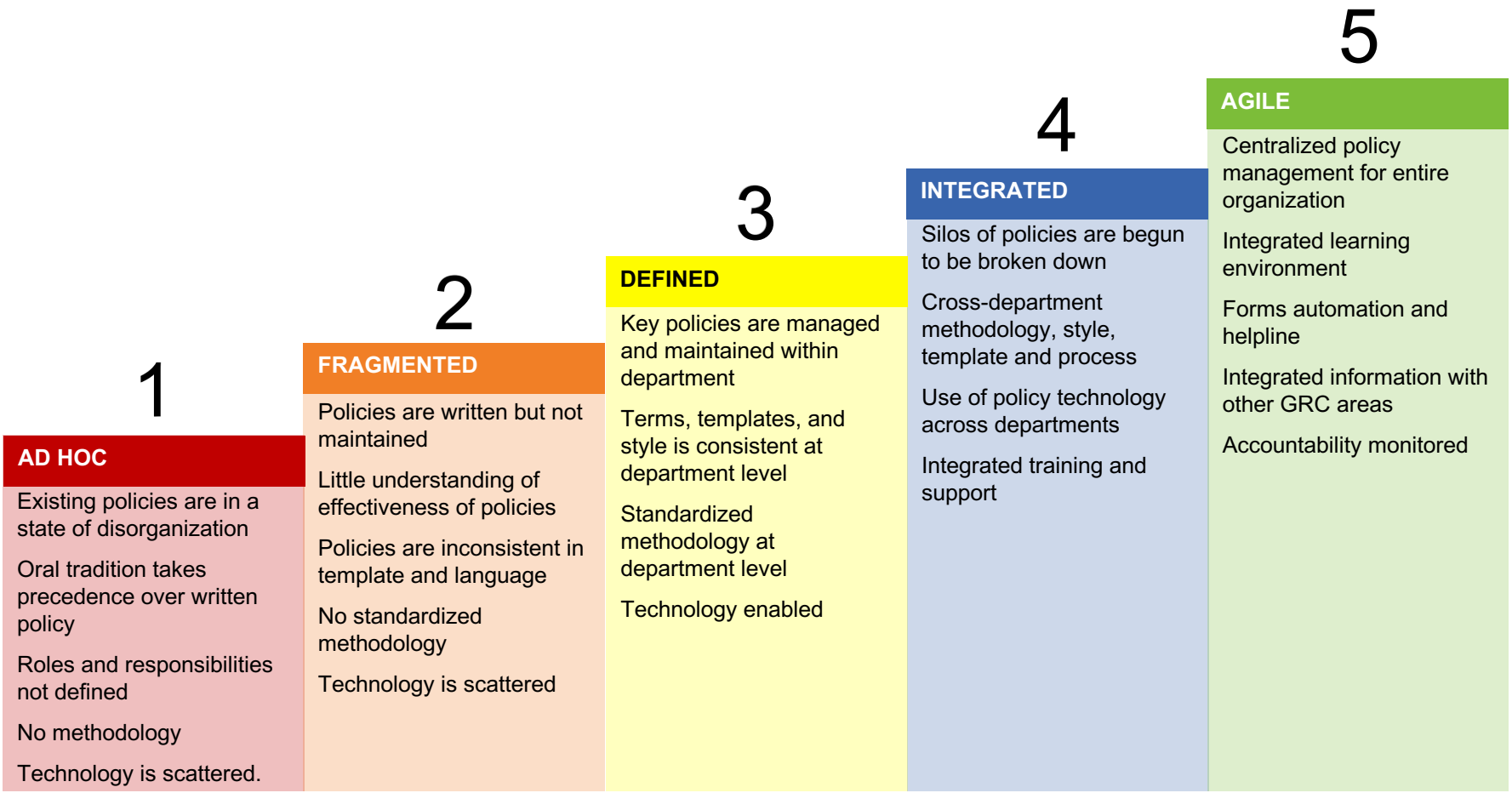
Frequent changes to policies should not be necessary in a healthy policy environment. Active diligence through regular review cycles will ensure policies remain appropriate and aligned to organizational needs and help minimize unnecessary exposure and liability. Policies found to be out of date should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

GRC 20/20‘S Policy Management Maturity Model



Workshop Activity

PART 2

Mapping Regulation to Policy, Processes & Controls

> *Realize that everything connects to everything else.*
>
> Leonardo da Vinci

The Chaos of Compliance Interconnectedness

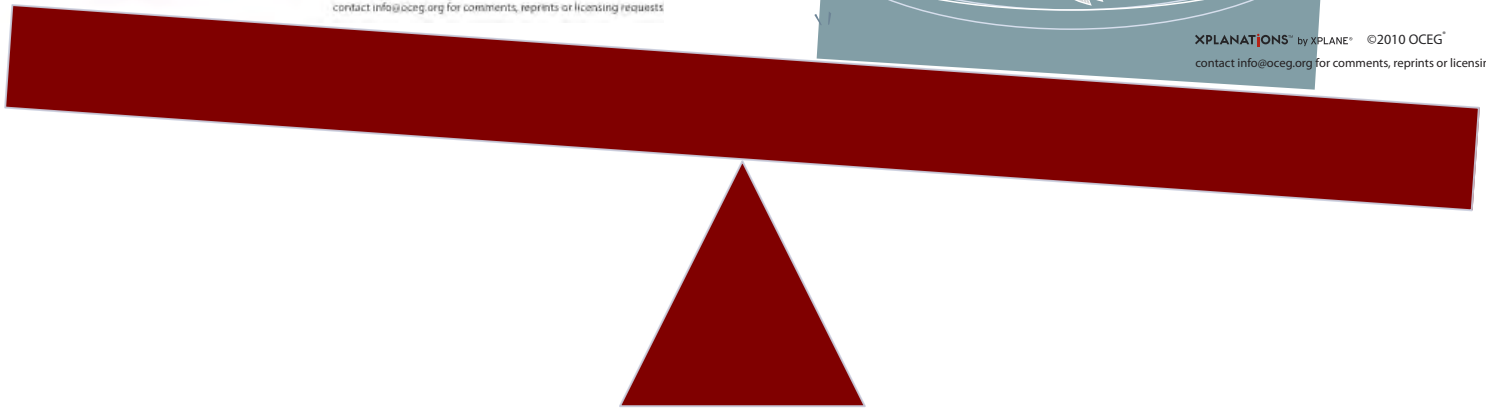
> *Realize that everything connects to everything else.*
>
> Leonardo da Vinci

Regulatory Change Pressures on Organizations

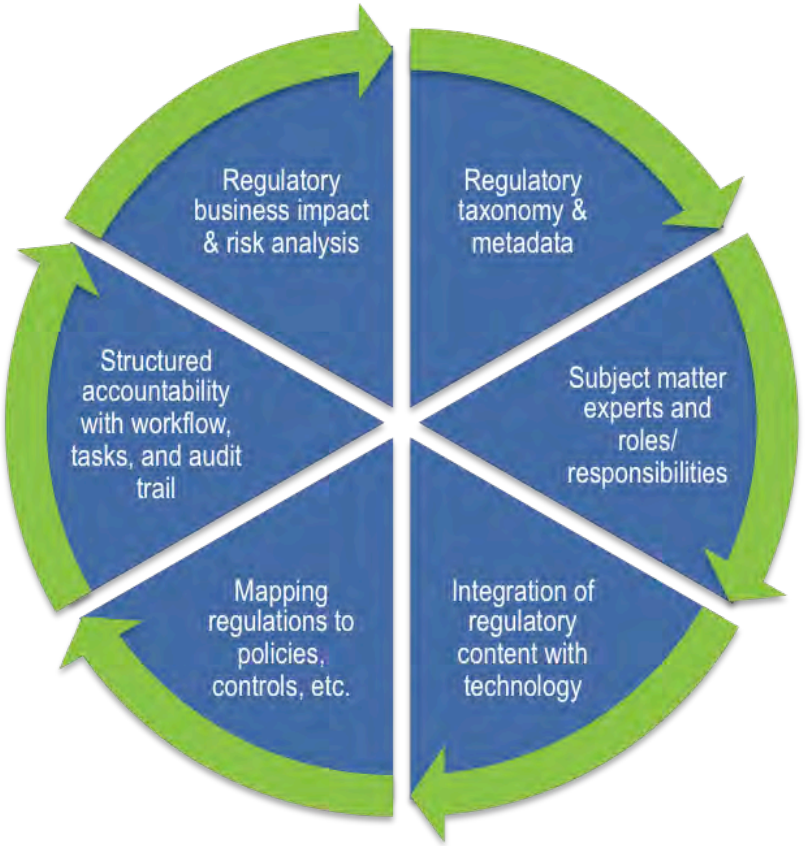
Balancing the Right Amount of Policy

NO GUIDANCE OR SUPPORT
(UNDER-CONTROL)

OVER-CONTROL



Developing a Framework to Manage Policies in Context of Regulatory Change

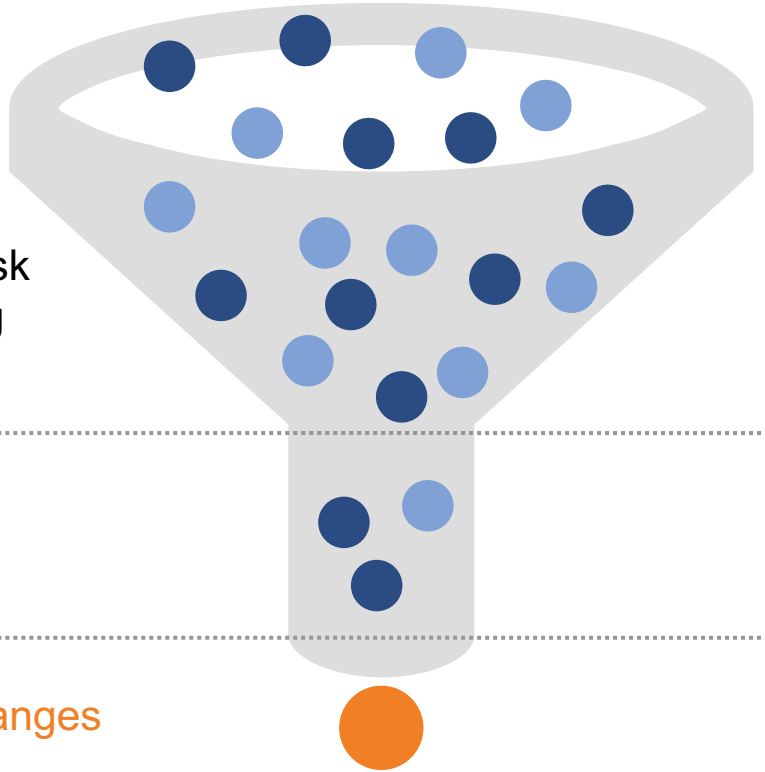


Filtering Changes to Identify Synergies and Change Needed

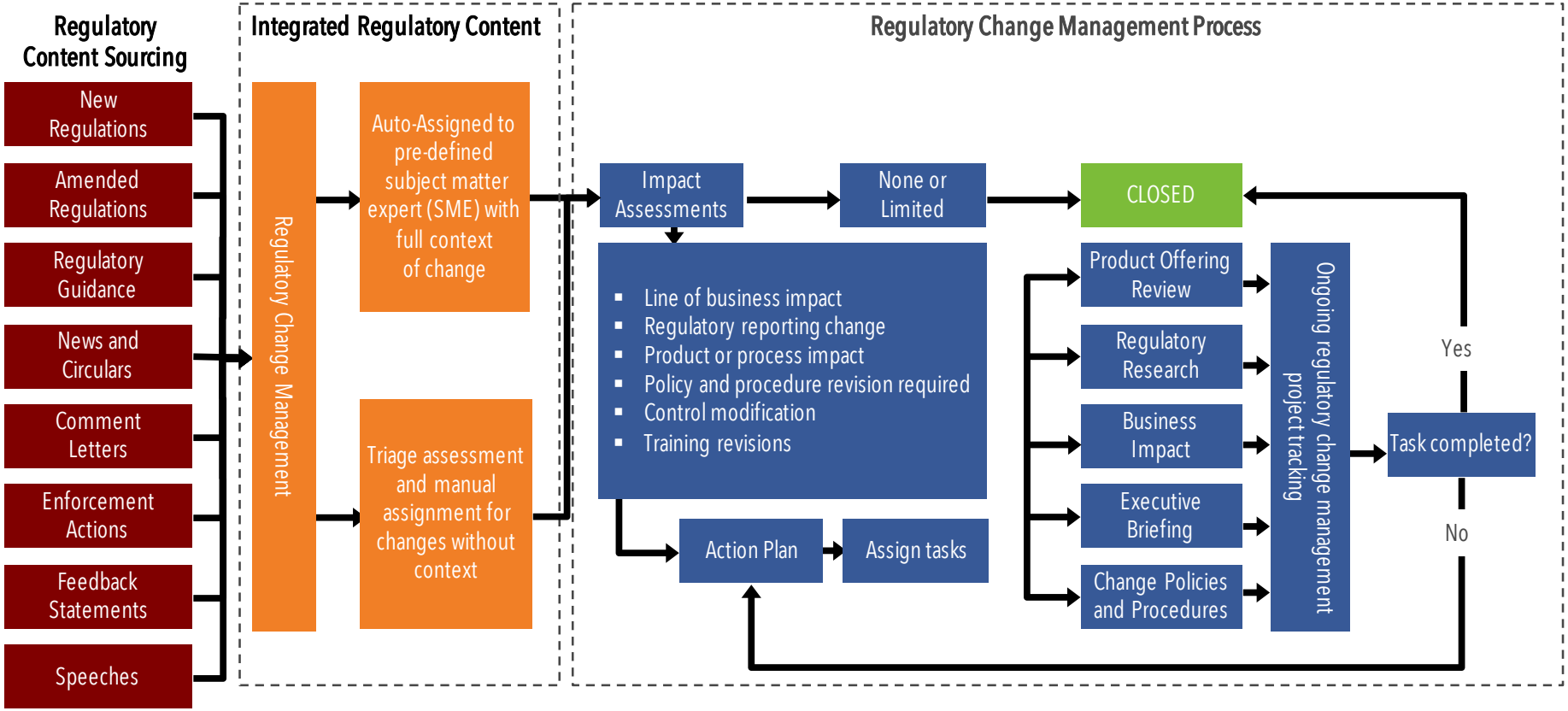
1 Understand organization, regulatory, and risk change impacting policies

2 Determine synergies

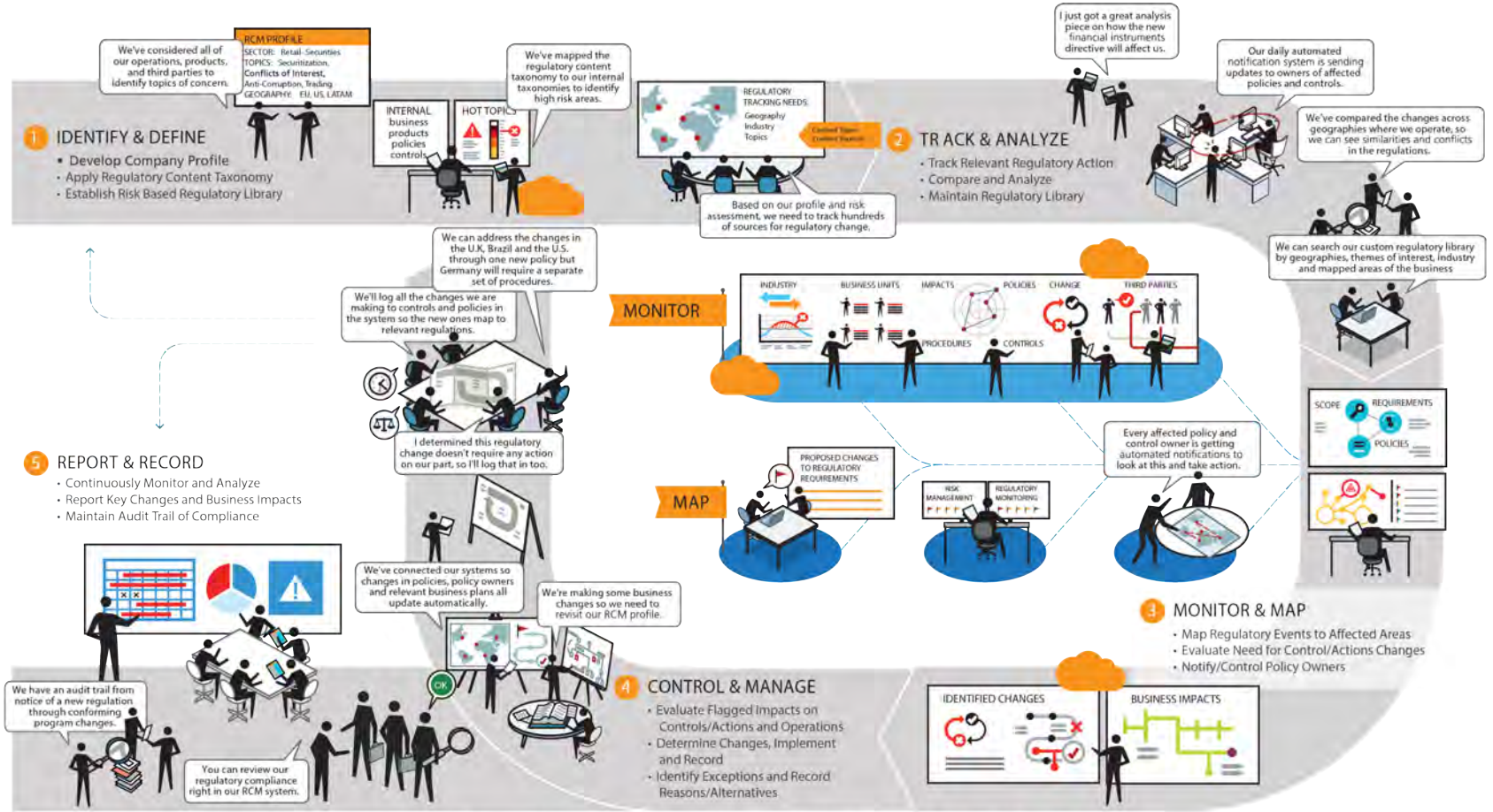
3 Identify policy changes



Regulatory Change Management Process



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

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.

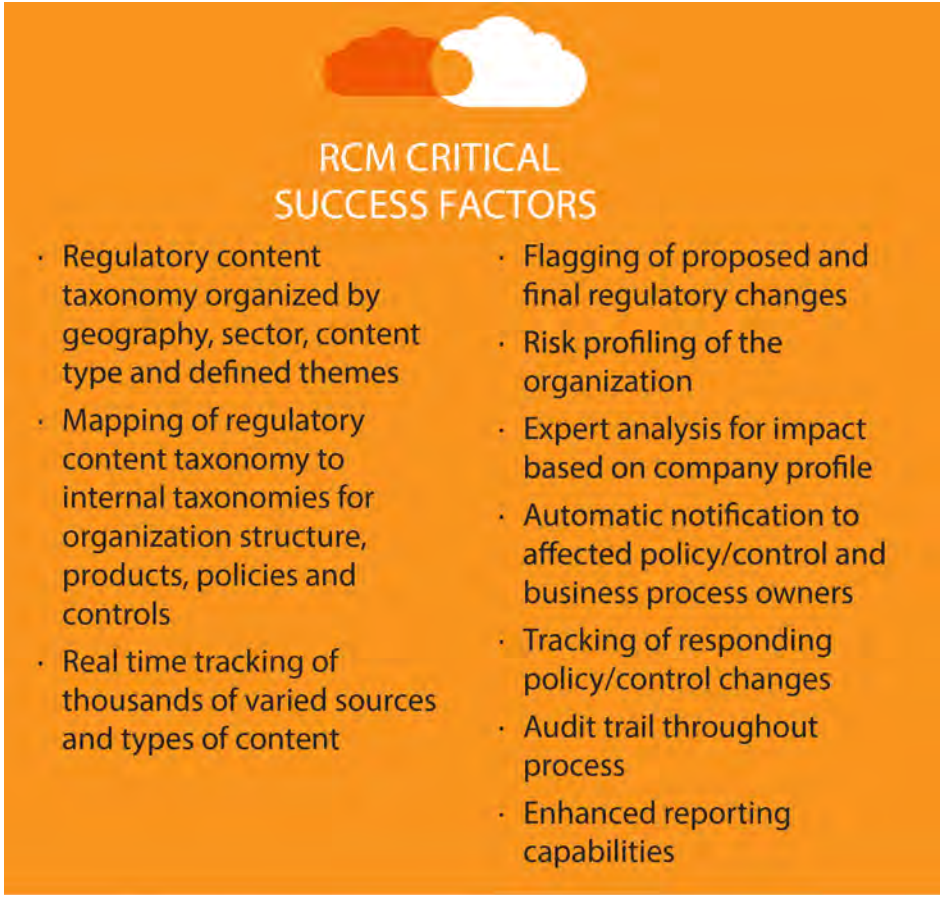
Trends

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.

Regulatory Change Management Success Factors



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

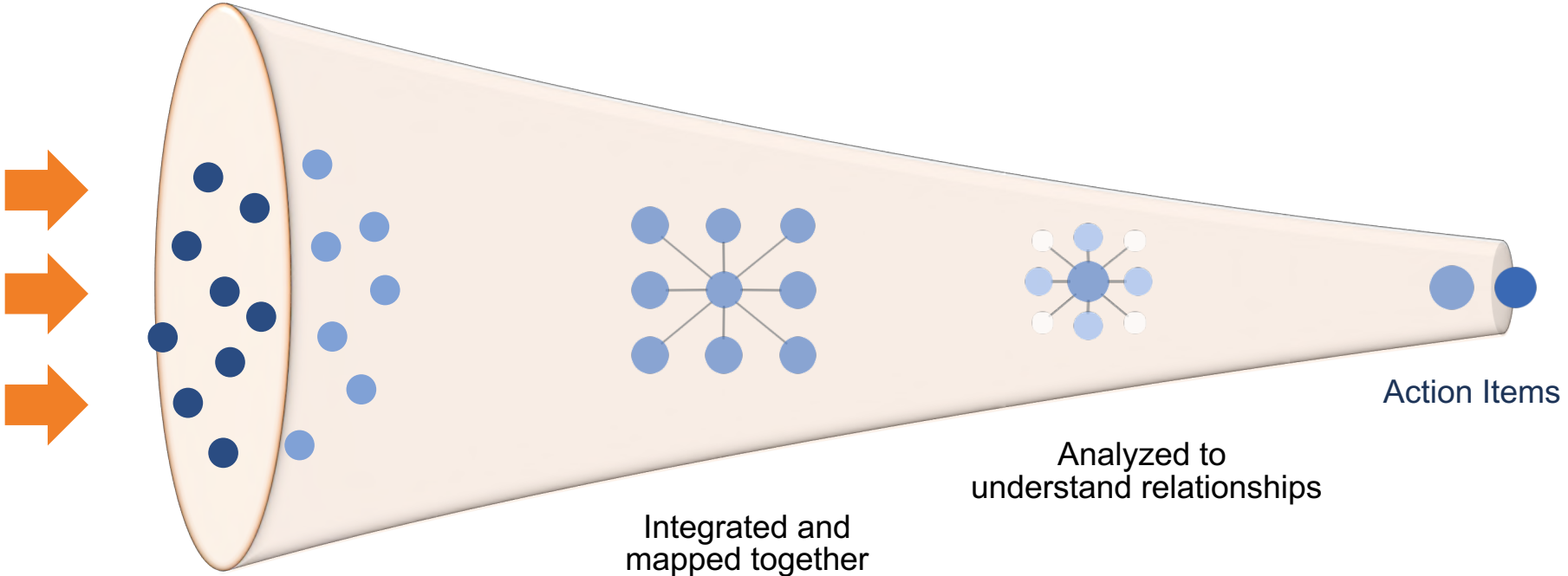
Leveraging a common system increases effectiveness while reducing costs

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

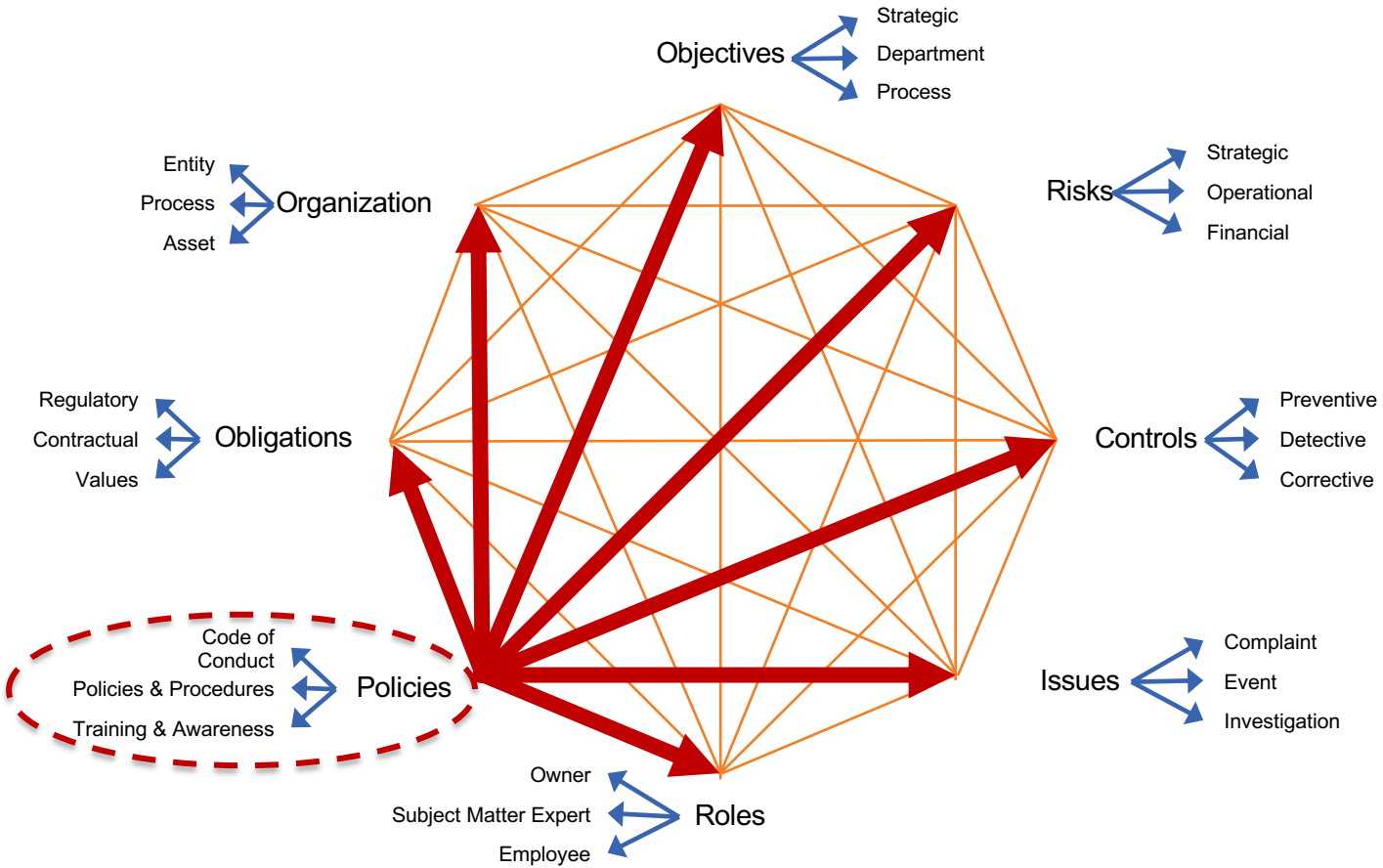
Information consistency makes it possible to examine trends across business units and analyze correlation with business performance

Better insight enables optimized allocation of capital to risks and requirements

360° Policy Contextual Intelligence



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.

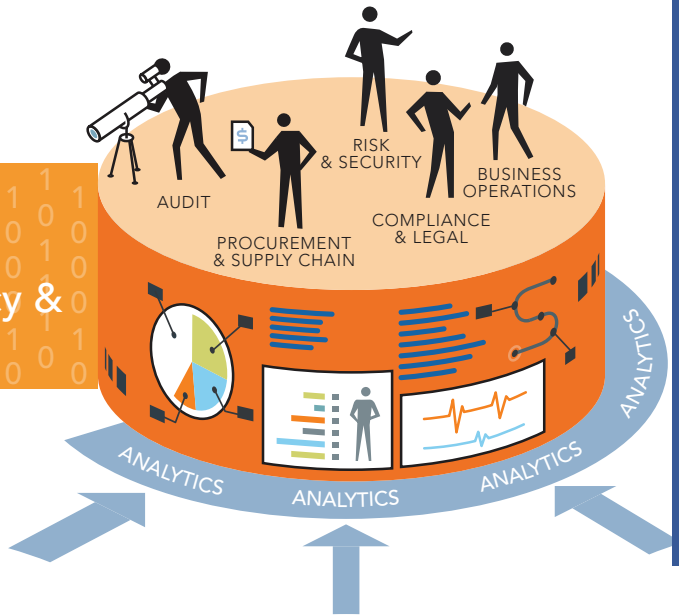
reduced costs

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

Technology Enables Efficient, Effective & Agile Policy & Training Management

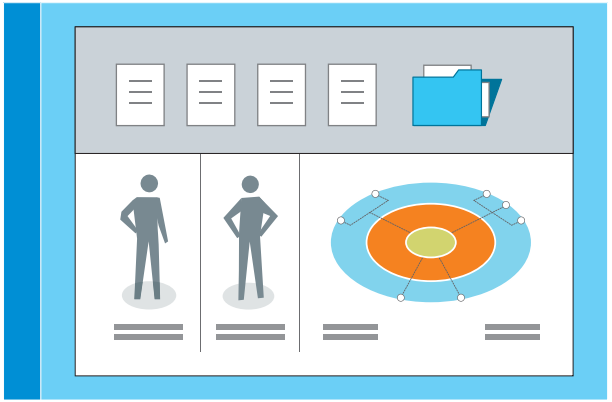
The bottom line: With today's complex business operations, global expansion, and the ever changing legal, regulatory and compliance environments, a well-defined policy management program is vital to enable an organization to effectively develop and maintain the wide gamut of policies it needs to govern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

Policy Management Technology Enables Management of Policy Processes

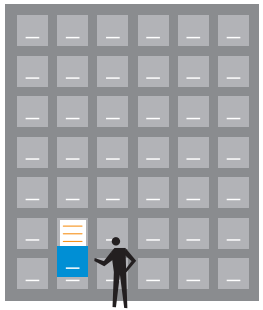


AUTOMATION AND TRACKING

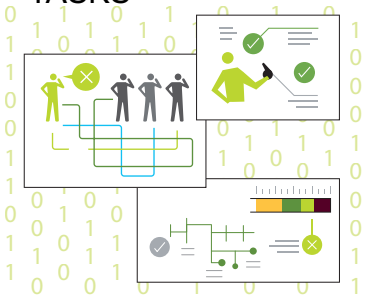
Technology enables the change tracking and monitoring process by integrating information and content sources with software that automates and tracks workflow, accountability, and analysis of changes or additions needed in policies.

MANAGEMENT REPORTING

AUDIT TRAIL



WORKFLOW & TASKS



COLLABORATION

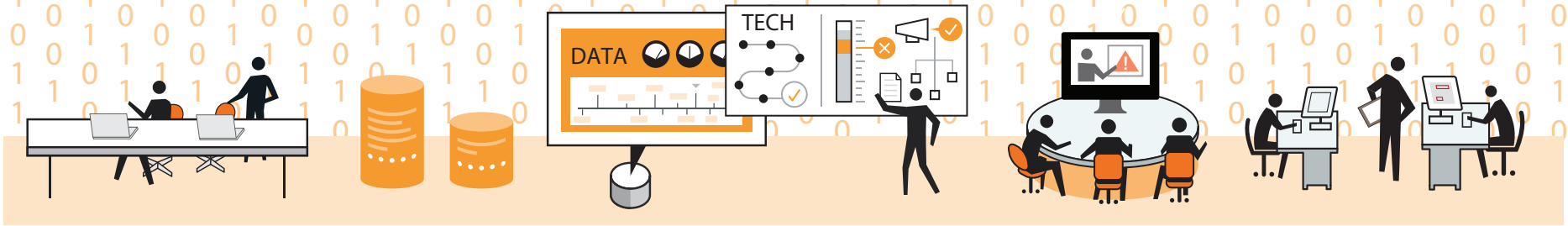
ENFORCEMENT

IFORCE
munication, policies aren't always fol-

Benefits of Technology

Technology is the backbone for the implementation of the policy, training and communications plan.

THE BENEFIT OF TECHNOLOGY



Integration

Policy communication and training technologies need to integrate into the larger business environment - such as with HR systems to gain access to employee lists to properly target and communicate policies.

Visibility

Policy communication and training technologies need to be user friendly and intuitive so that users of varying degrees of capabilities can use the system and understand the policy.

Global Reach

Policy communication and training technologies should have the proper capabilities to meet the language and geographic needs of the organization.

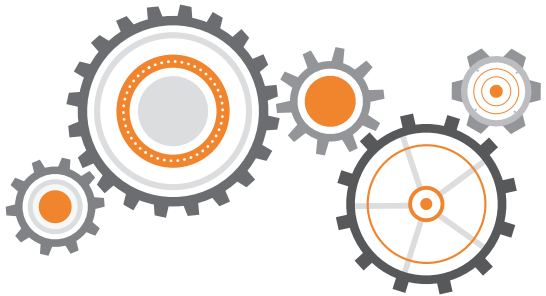
Availability

Policy communication and training technologies need to be accessible across the business and often business relationships so that anyone associated with the organization can easily access the policy and associated training.

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

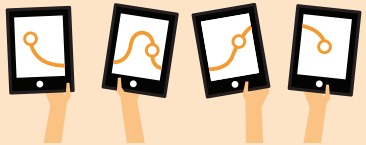
Technology enables policy implementation and enforcement by creating a repository of all policies, procedures, and controls that are cross-referenced with one another and not treated as isolated documents.

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.

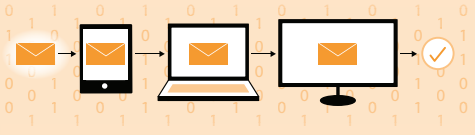
Accountability

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.



Automation

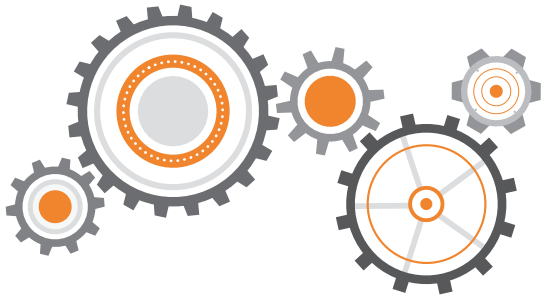
Technology enables the automation of workflows and tasks to complete audits and assessments related to policy compliance. No longer is the organization encumbered by unanswered or lost emails or documents that are out of sync.



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

Policy Management: Critical Capabilities

Solution Area Definition

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

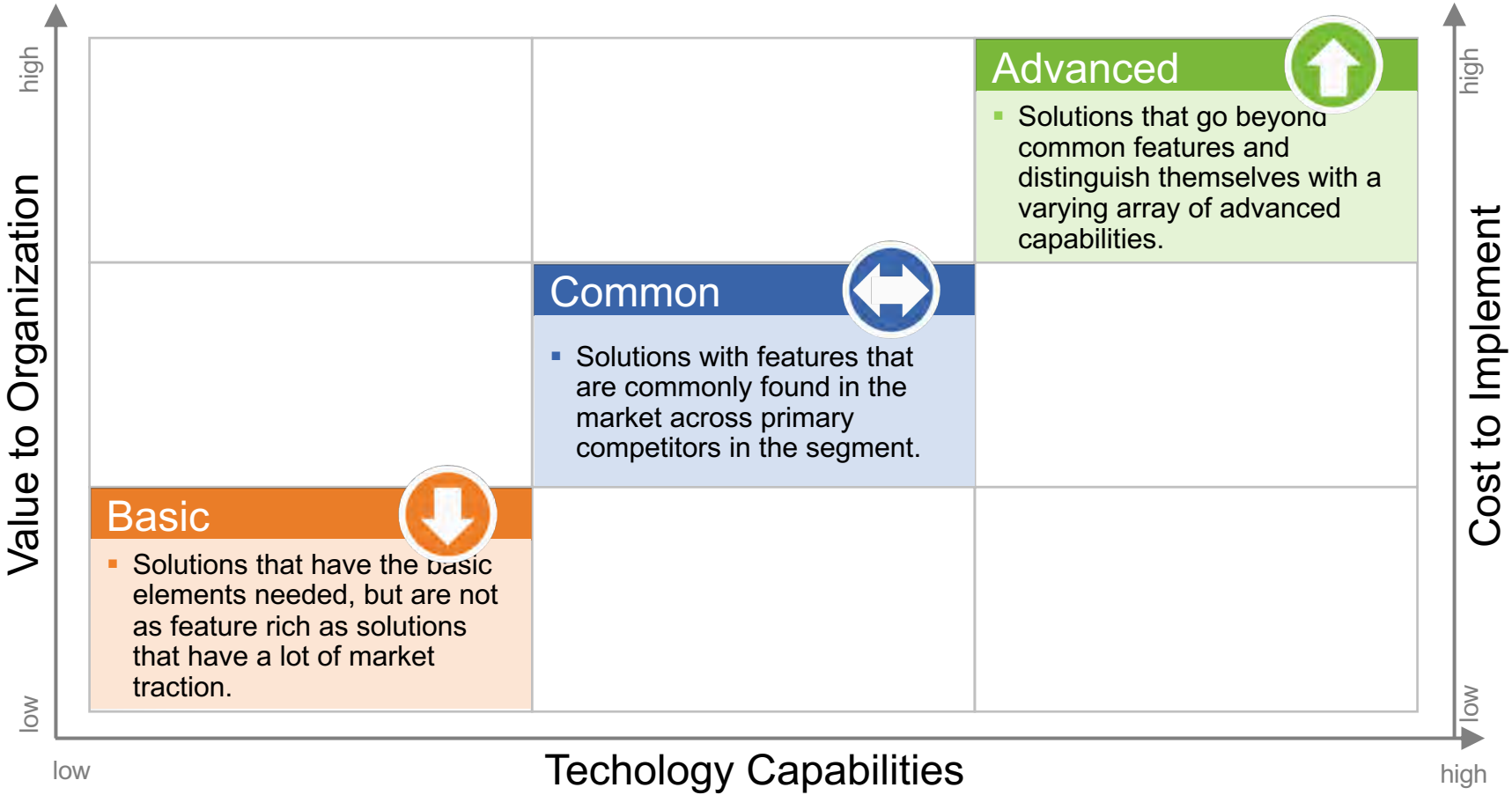
This enables organizations to manage:

- 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.

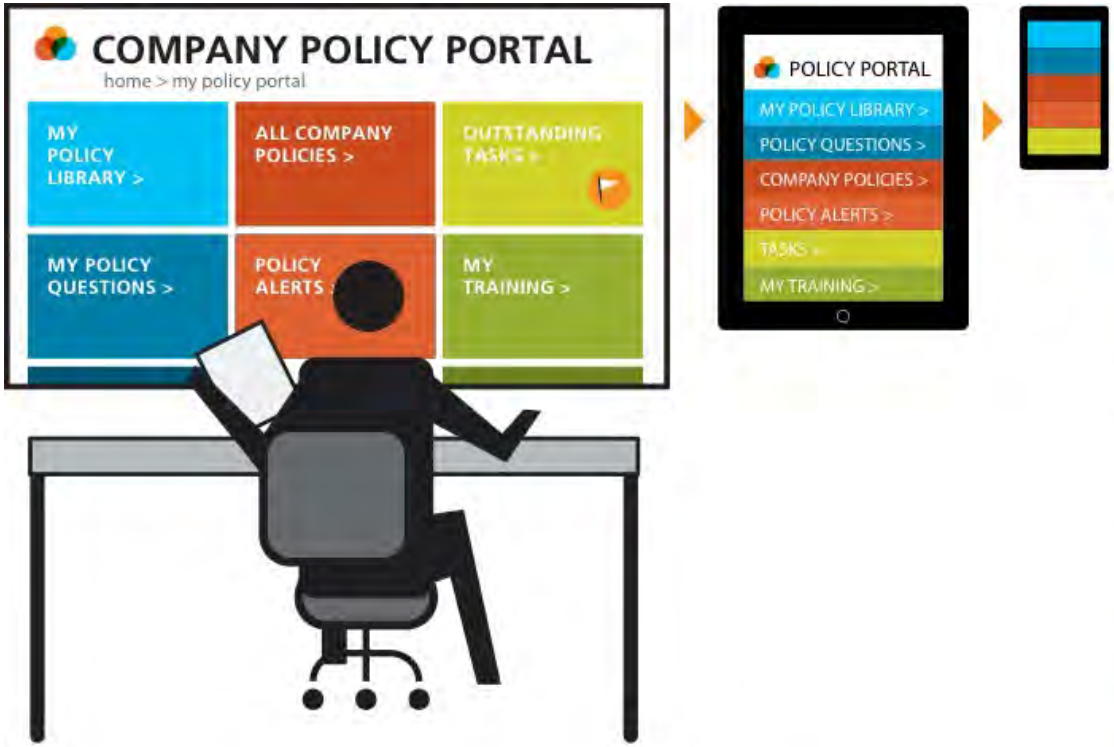
Critical Capabilities

- ❑ 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



Deliver a Unified Company Policy Portal in the Format Needed



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

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.

An Engaging User Experience for Policy Management

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.

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

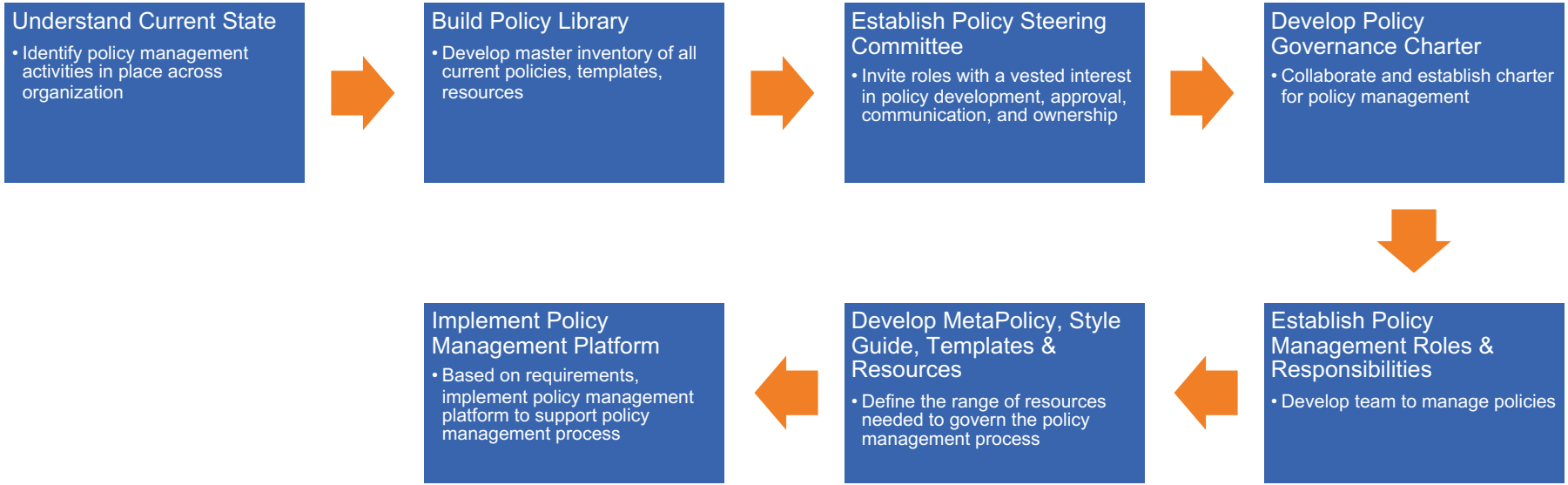
INTERACTIVE

- 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

Steps to Building an Enterprise Policy Management Program



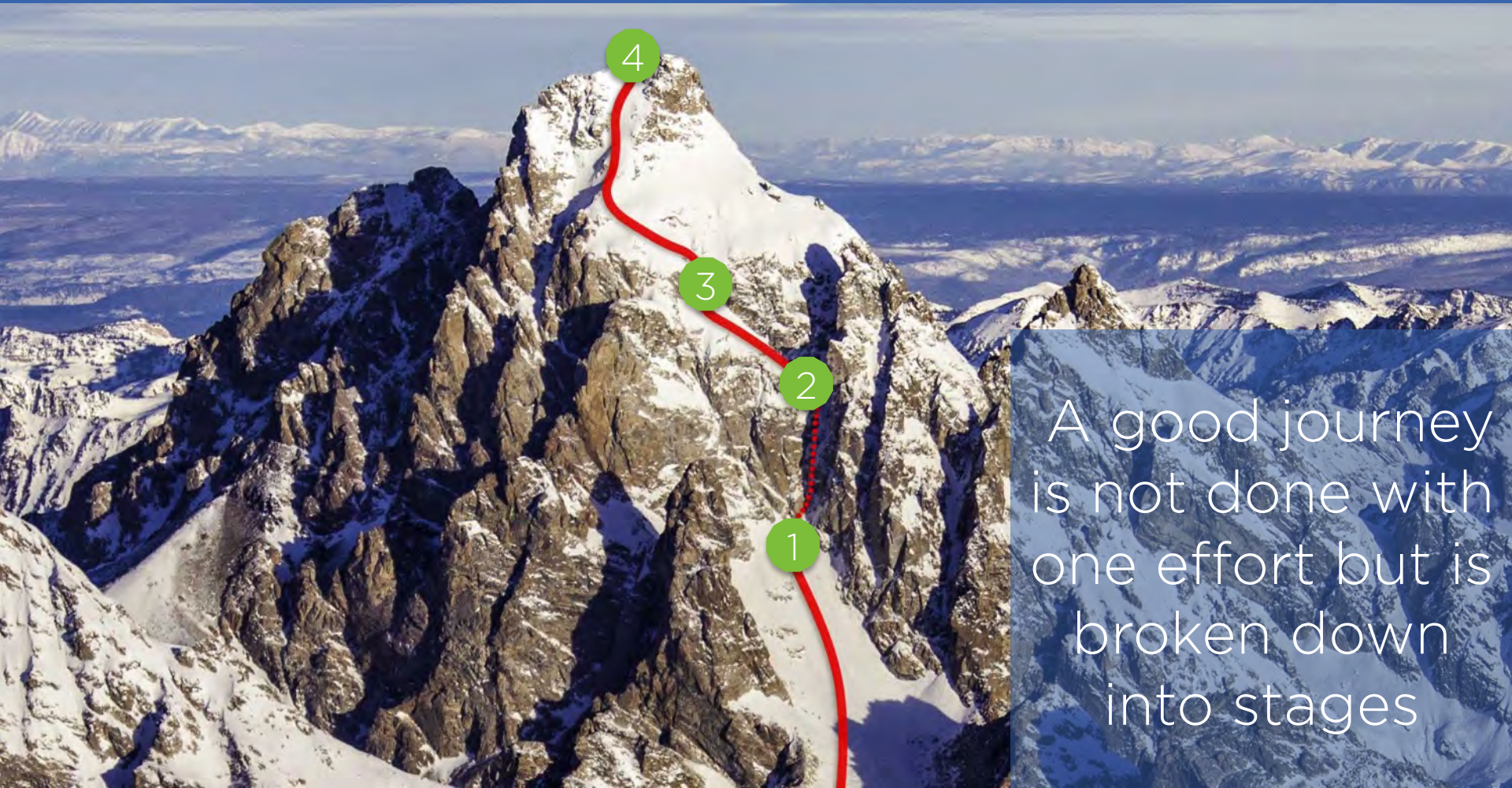
Careful Planning is the Key to Success to Policy Management

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

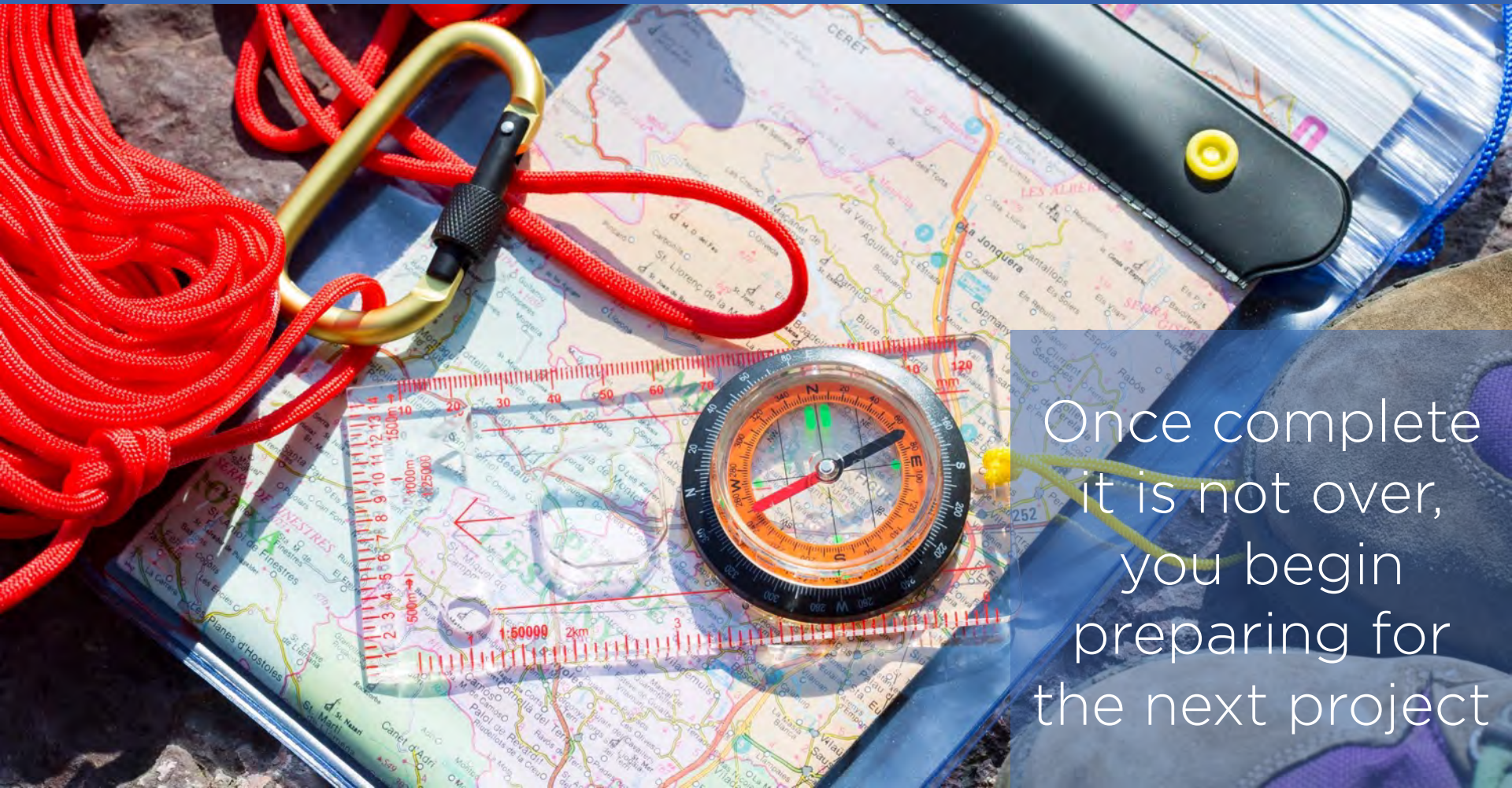
Conditioning is Critical, Make Sure Your Team and Systems are Ready

Select the Right Equipment for the Policy Management Journey

Tackle Your Policy Management Strategy in Stages



Preparing for the Next Journey



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

Workshop Activity

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