2024-02

Best Practices in Policy and Procedure Management for Financial Services

PRESENTATION

Governance, Risk Management & Compliance Insight

Housekeeping Details

- Welcome to today's webinar!
- All attendees will be in listen only mode.
- We encourage you to ask questions via the Questions pane in your GoToWebinar control panel. We'll be answering as many questions as possible at the end of the presentation.
- A recording of today's session will be made available on mycomplianceoffice.com. We'll send you an email in the next few days with a link to view the recording.

Michael Rasmussen, The GRC Pundit and Analyst
GRC 20/20 Research, LLC

Michael Rasmussen is an internationally recognized pundit on governance, risk management, and compliance (GRC) – with specific expertise on the topics of enterprise GRC, GRC technology, corporate compliance, and policy management. With 30+ years of experience, Michael helps organizations improve GRC processes, design and implement GRC architecture, and select technologies that are effective, efficient, and agile. He is a sought-after keynote speaker, author, and advisor and is noted as the "Father of GRC" — being the first to define and model the GRC market in February 2002 while at Forrester.

Culture: Confusing Policy Communications

Inevitability of Failure: Too Many Documents & Manual Processes

Drivers in Policy Management

Policies in Context of GRC

GOVERNANCE

Policies define the organization's governance structure, culture, and behavior to reliably achieve objectives. Without good policy as a guide, corporate culture and control morphs, changes, and takes unintended paths.

RISK MANAGEMENT

Policies address uncertainty – there would not be a policy if there was not a risk of exposure to uncertainty. Policies are risk documents that establish risk responsibility, communication, appetites, tolerance, boundaries, controls, and risk ownership.

POLICY MANAGEMENT

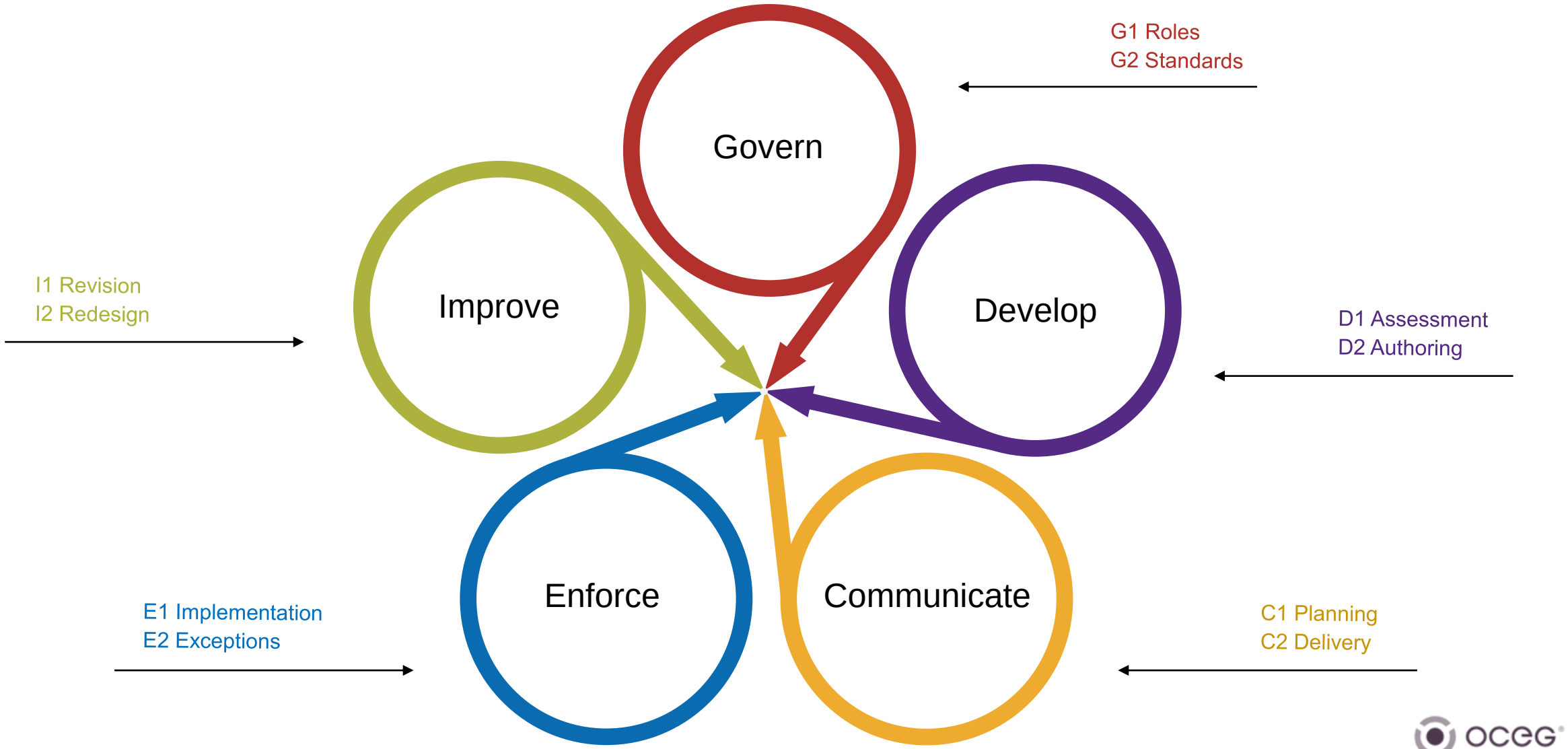
When fully integrated into the GRC ecosystem, policy management benefits from timely notification about changes throughout the organization that may demand policy issuance or revision. The organization benefits from standardization of policy development, distribution, enforcement, and review. This enables better selection of other internal controls, accurate reporting, and more efficient use of resources.

COMPLIANCE

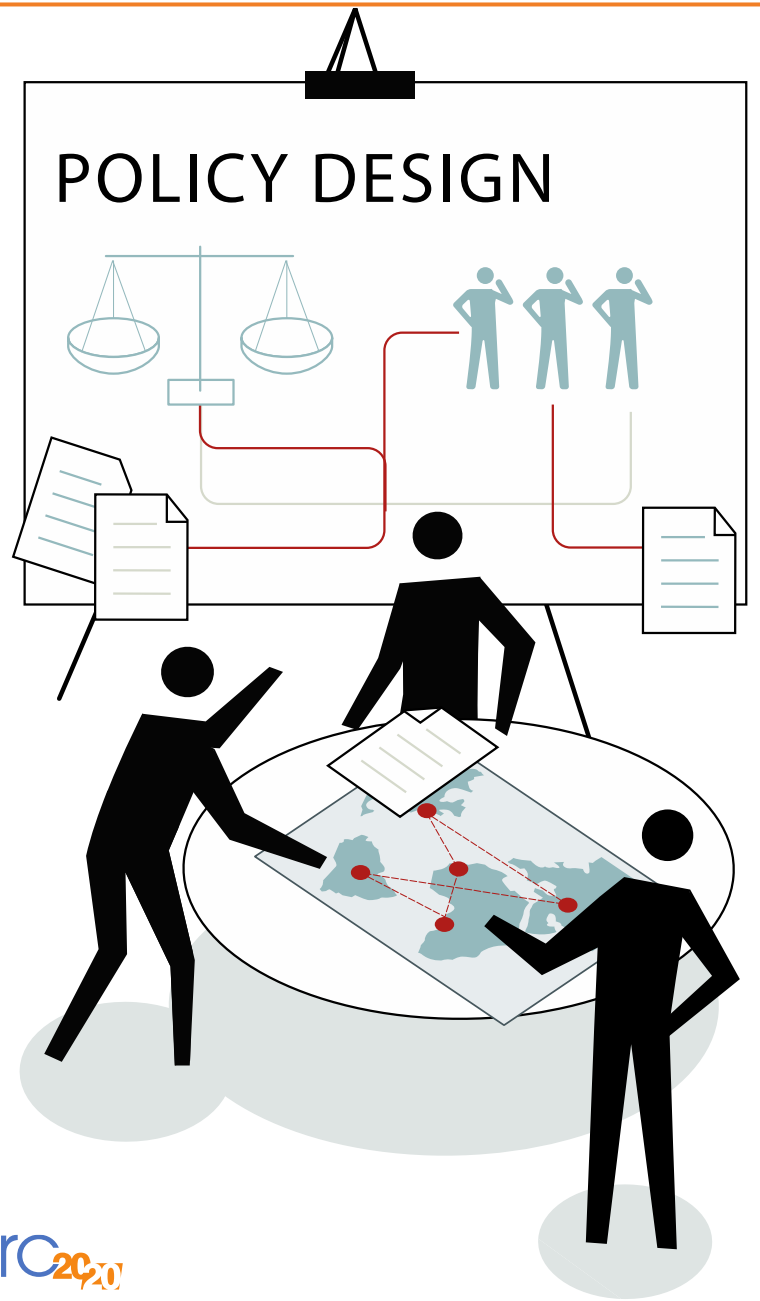
Policies that are understood and followed develop a culture of compliance and integrity. Policies establish how an organization meets its obligations and commitments and how it will stay within legal, regulatory, and contractual boundaries.

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

Policy Management Lifecycle



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:

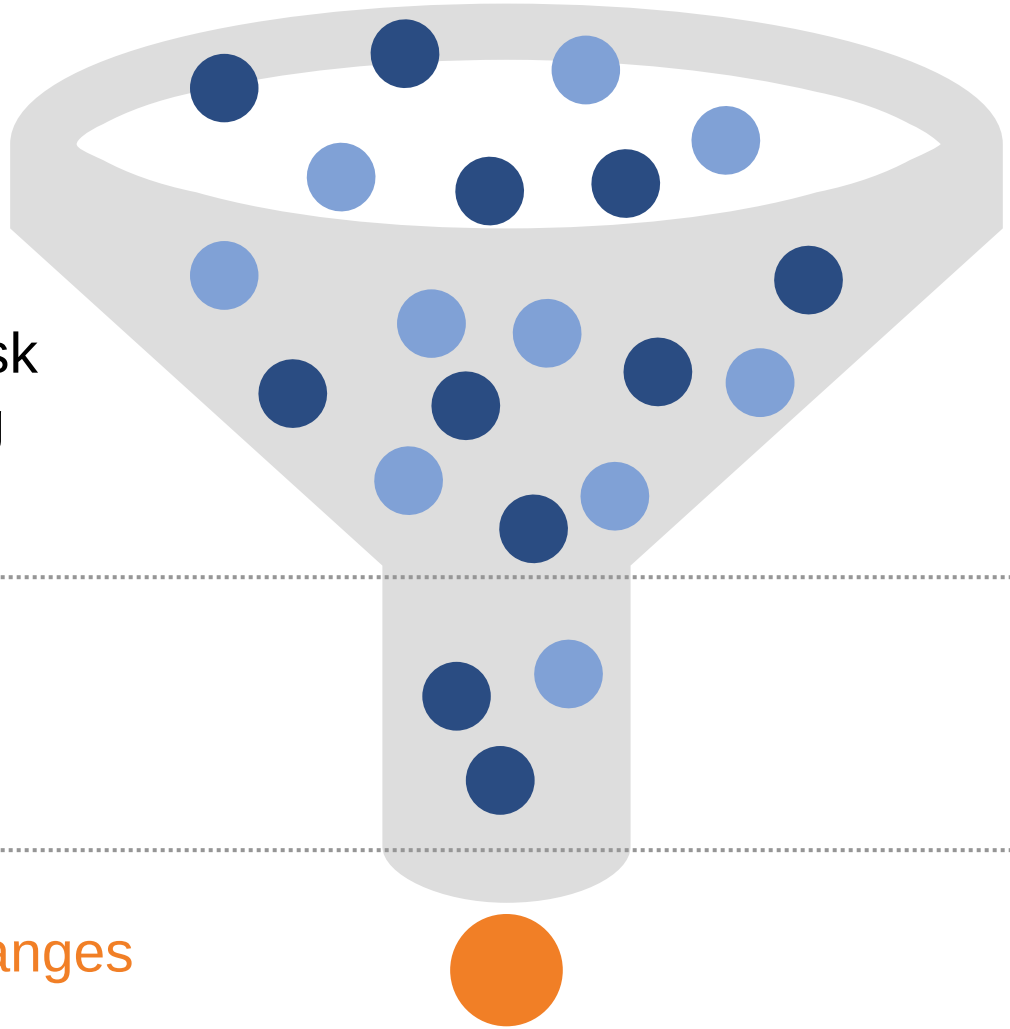
- ✓ Identify policies required by law and regulation and map each policy to the legal requirements it addresses, which may be more than one
- ✓ Determine what additional policies are desired
- ✓ Determine which types of policies must apply to vendors or partners and in what circumstances
- ✓ Determine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

Filtering Changes to Identify Policy Changes

1 Understand organization, regulatory, and risk change impacting policies

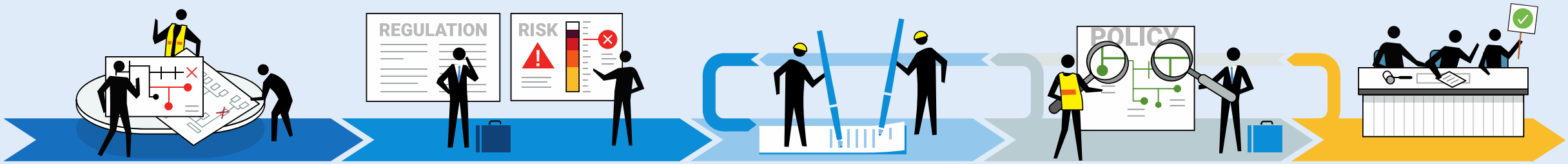
2 Determine synergies

3 Identify policy changes



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

KEY STEPS TO A COLLABORATIVE PROCESS



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 approvals and sign off.

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

Build a Compliance & Ethics Engagement 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

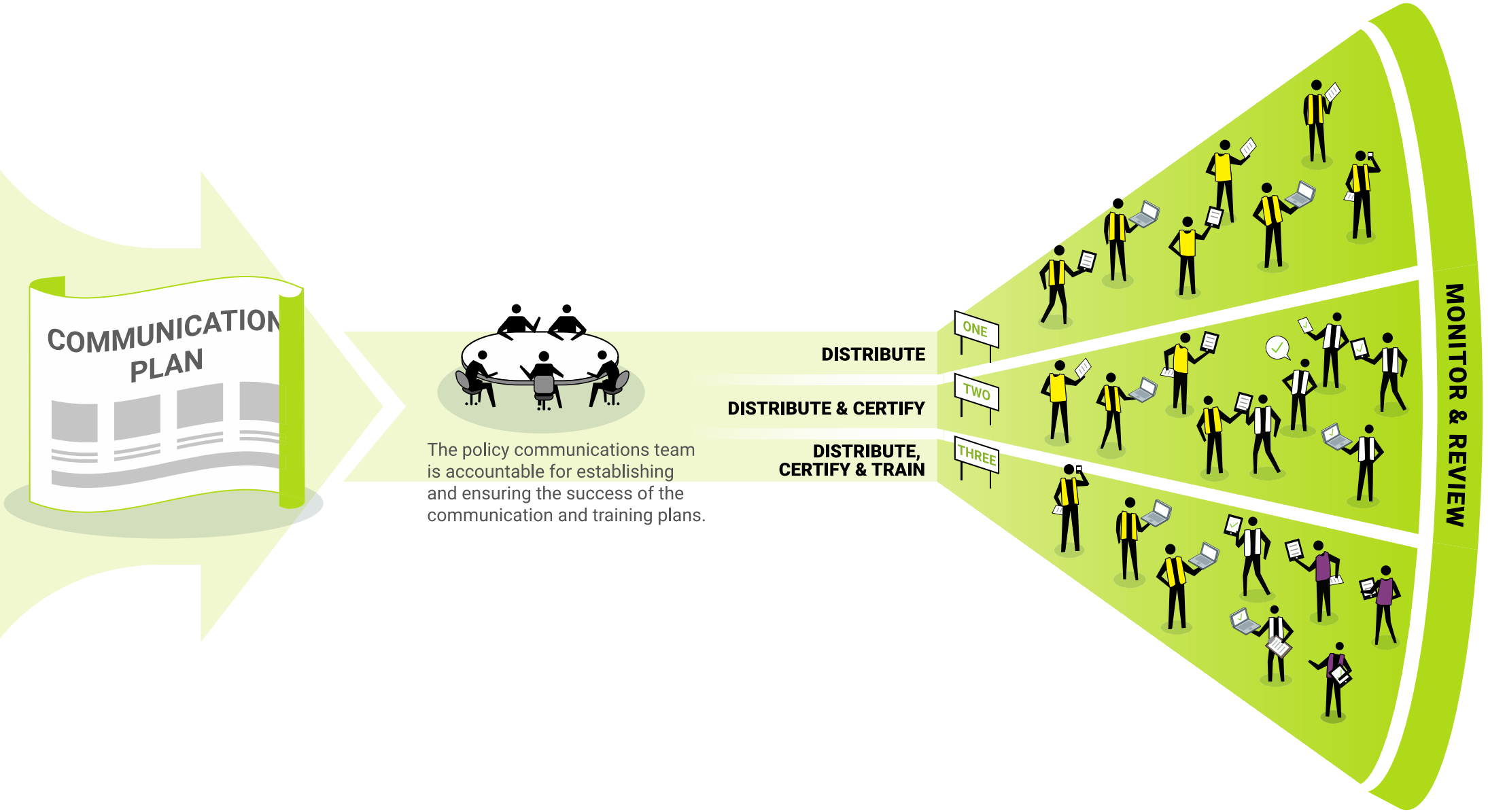
MEASUREMENT
Decide on metrics that will constitute 'success' for each phase of the communication process.

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.

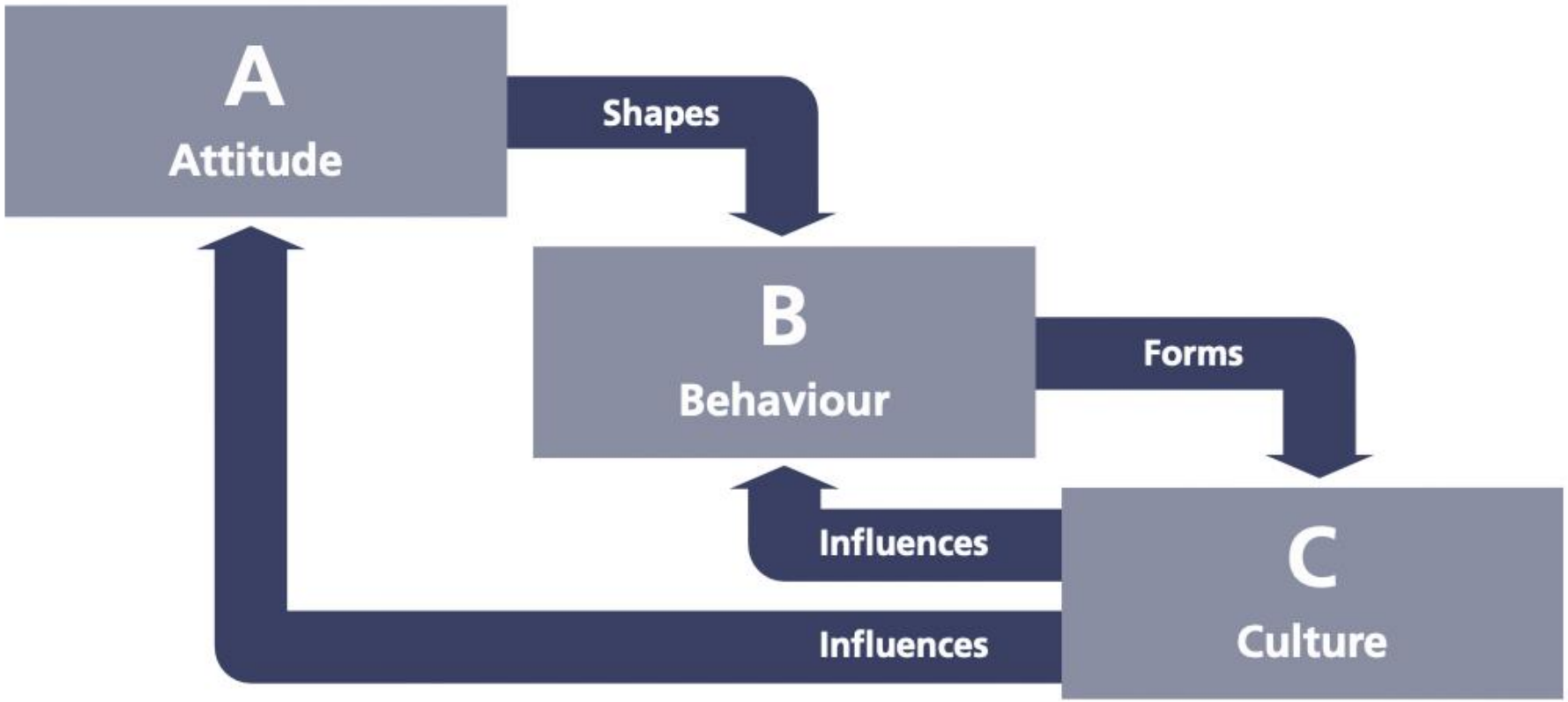
©OCEG, Contact support@oceg.org for comments, reprints or licensing
© GRC 20/20 Research, LLC • www.GRC2020.com

Implement a Compliance & Ethics Engagement Plan



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

Compliance & Ethics Culture: A-B-C Model

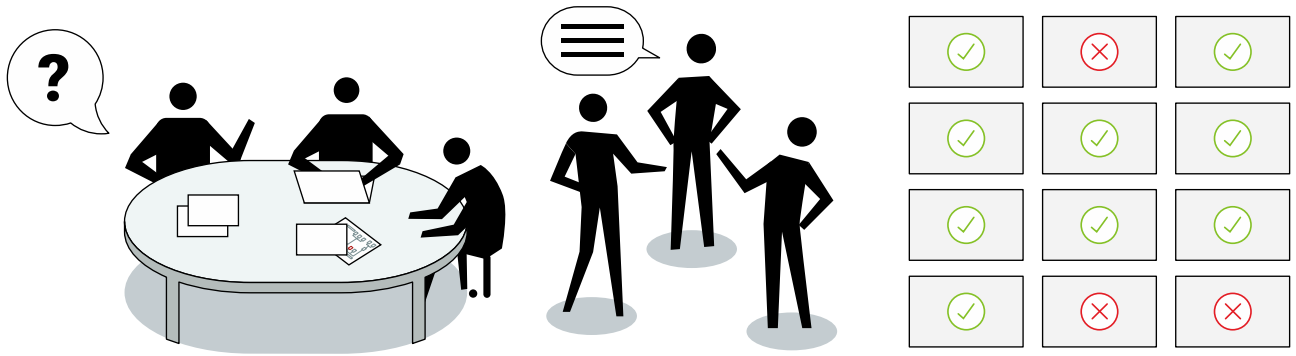


Source: The Institute of Risk Management; ***Risk Culture: Resources for Practitioners***

The Human Firewall: Well Written & Maintained Policies

The Human Firewall: Compliance Understanding & Engagement

It is Critical to Document and Manage Policy Exceptions and Exemptions

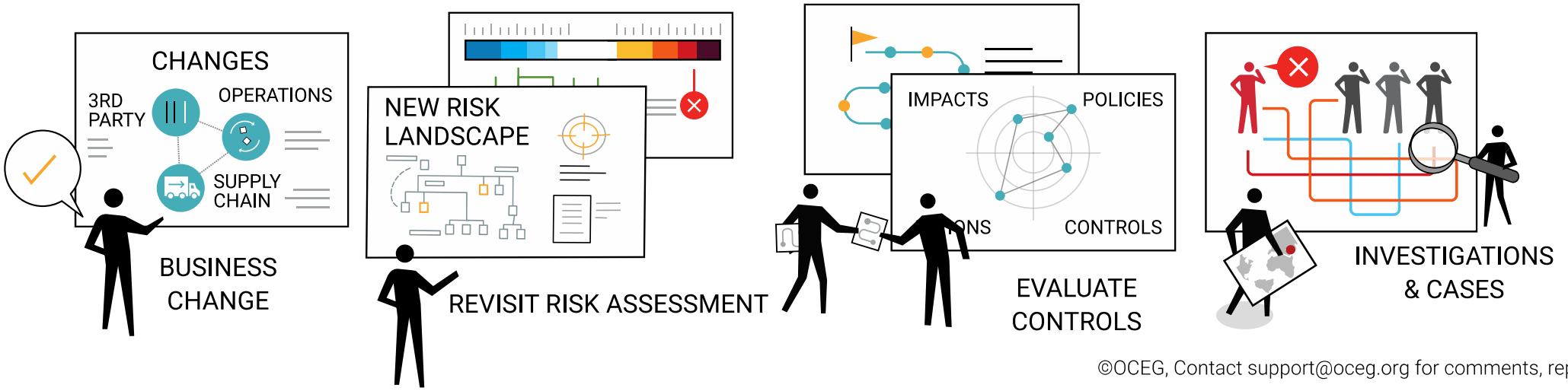


- Policy enforcement is not always possible. Exceptions happen when the organization cannot comply with a policy or when the policy is subjective or requires excessive clarification.
- Organizations need processes to authorize, track, monitor and review exceptions.
- Those who authorize exceptions must have authority. Limits should be set so exceptions are regularly reviewed and not granted for extended/unreasonable time periods.
- Exceptions must be documented and available to auditors and regulators upon request. Organizations that demonstrate exception management are 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.

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

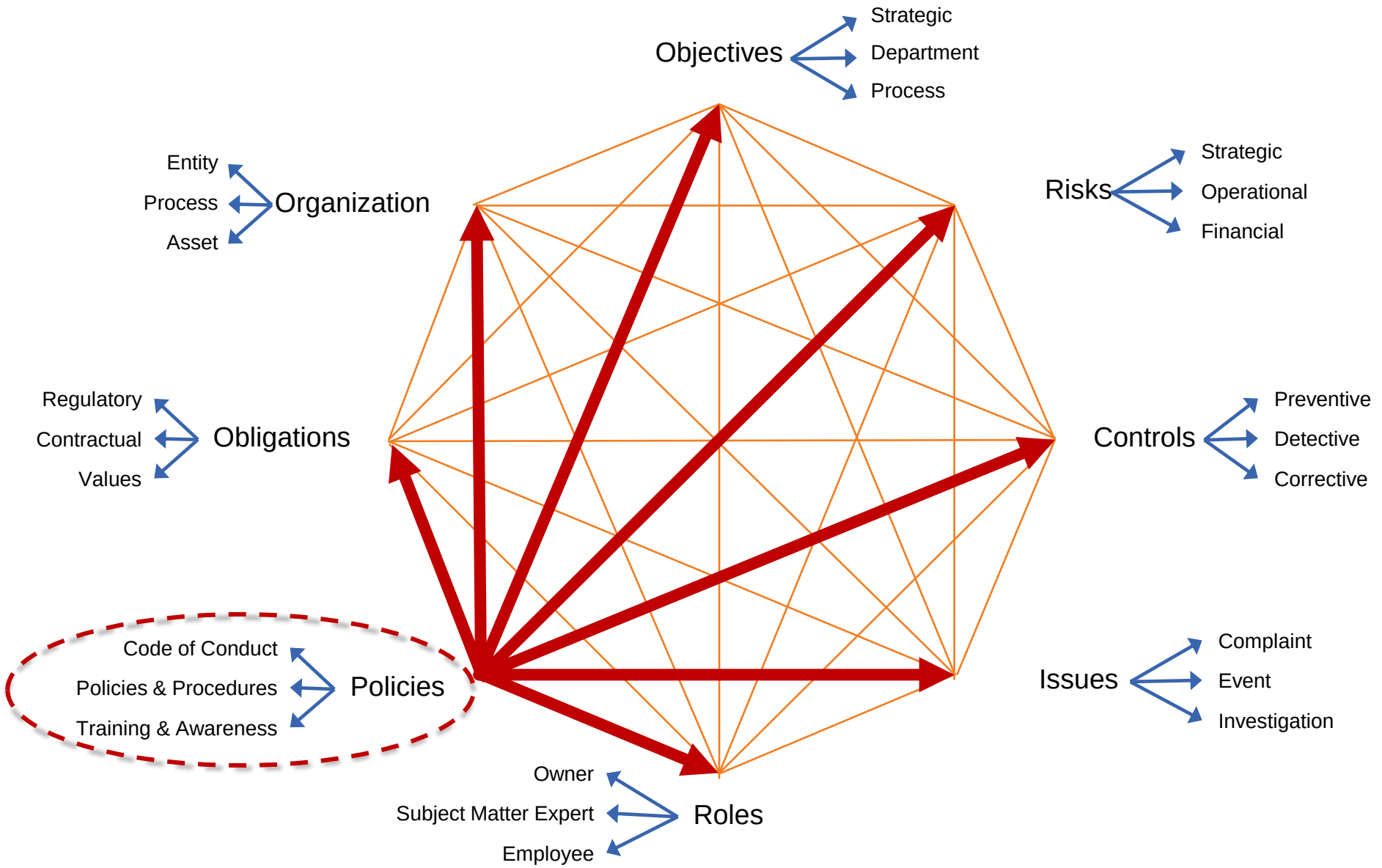
Implement a Periodic Review Cycle to Maintain Policies

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.



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

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.

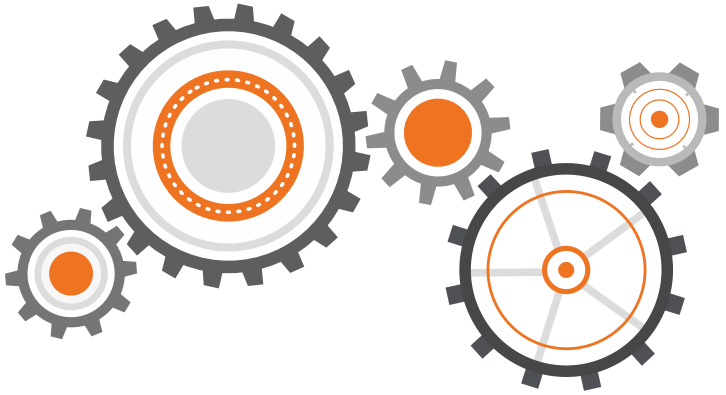
reduced costs

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

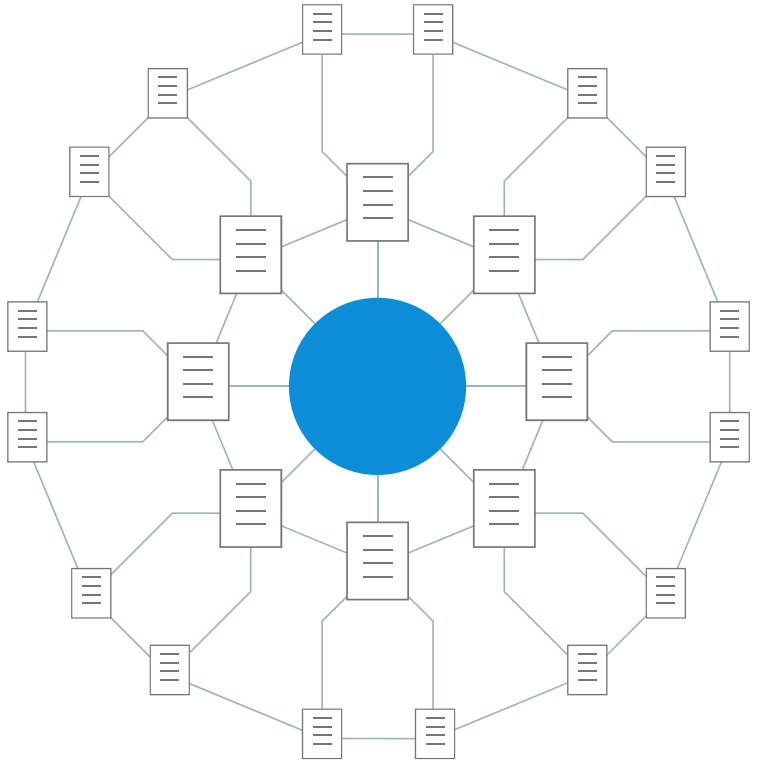
How Technology Enables Policy Management

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, procedures, obligations and related objectives
- Provide a robust system of record for access, certification and 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 for defensible audit trails
- Maintain accountable workflow
- Deliver comprehensive reporting

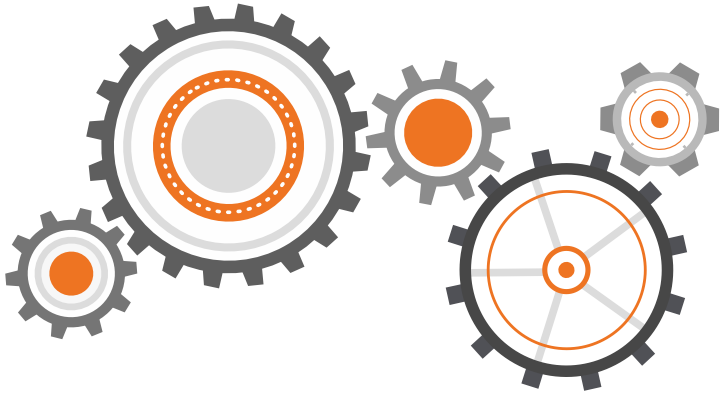


©OCEG, Contact support@oceg.org for comments, reprints or licensing

Leverage Technology for Policy & Compliance Management

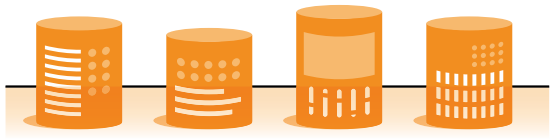
TECHNOLOGY

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.



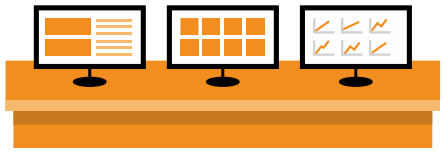
REPOSITORY

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



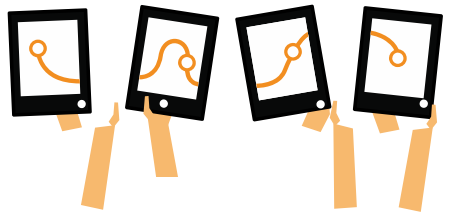
CONSISTENCY

Technology creates a consistent environment to conduct assessments, track issues of non-compliance, and take corrective actions. Technology allows an organization to easily and efficiently manage hundreds to thousands of policies especially during audits and assessments.



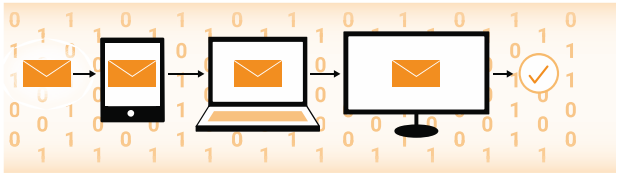
ACCOUNTABILITY

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.



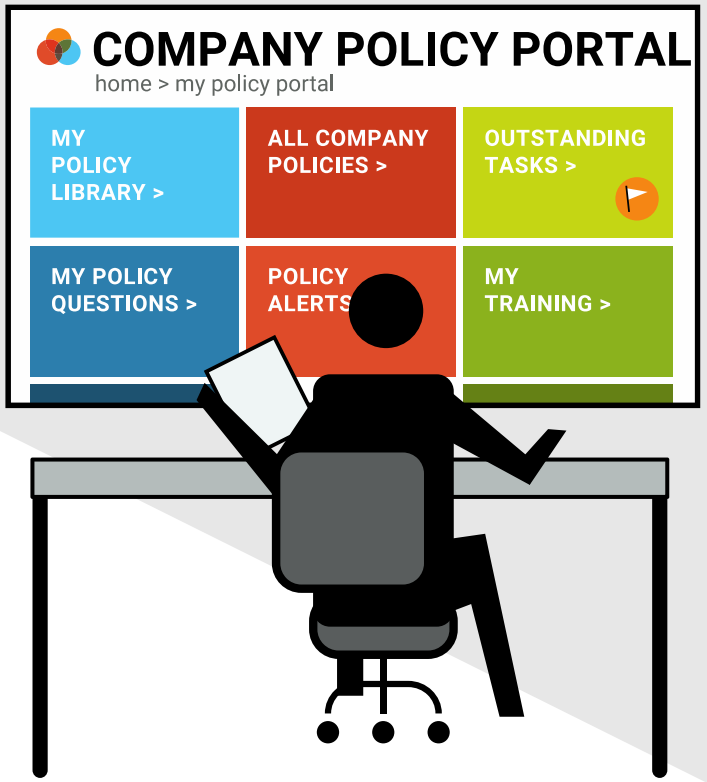
AUTOMATION

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.



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

Deliver a Unified Company Portal on Policies & Training



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 engaging experience for employees to learn and interact with policies.
- **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.

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

An Engaging User Experience for Compliance & Ethics Management

KEEPING POLICIES RELEVANT

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

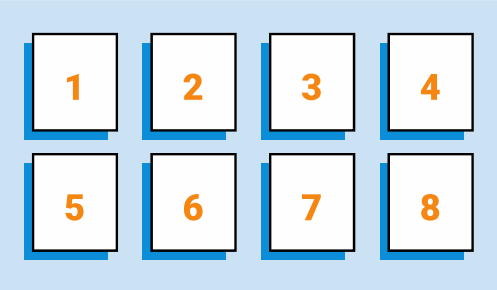
SOCIAL

- 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

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

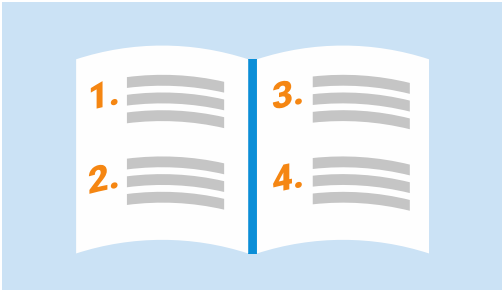
©OCEG, Contact support@oceg.org for comments, reprints or licensing

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



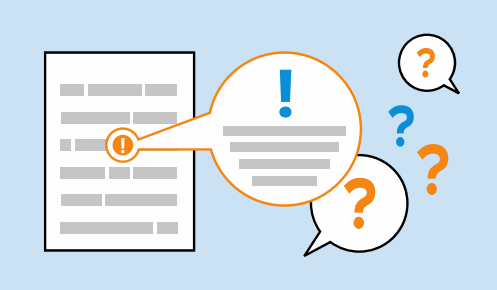
VERSION (DATE, TIME)

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.



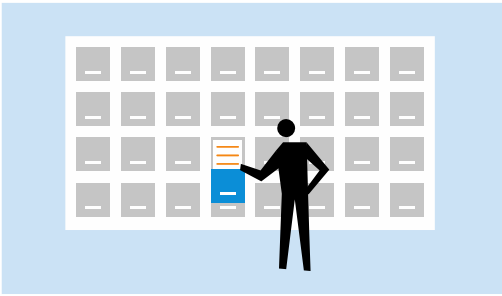
TESTING UNDERSTANDING

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



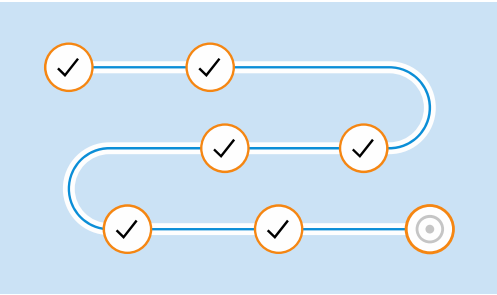
QUESTIONS & EXCEPTIONS

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.



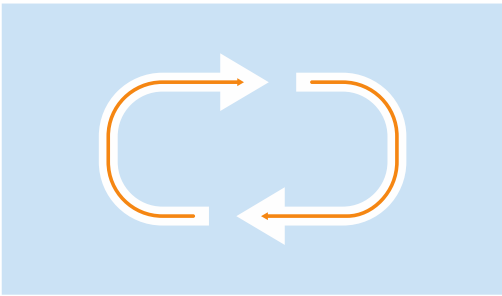
ACCESSING PAST RECORDS

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.

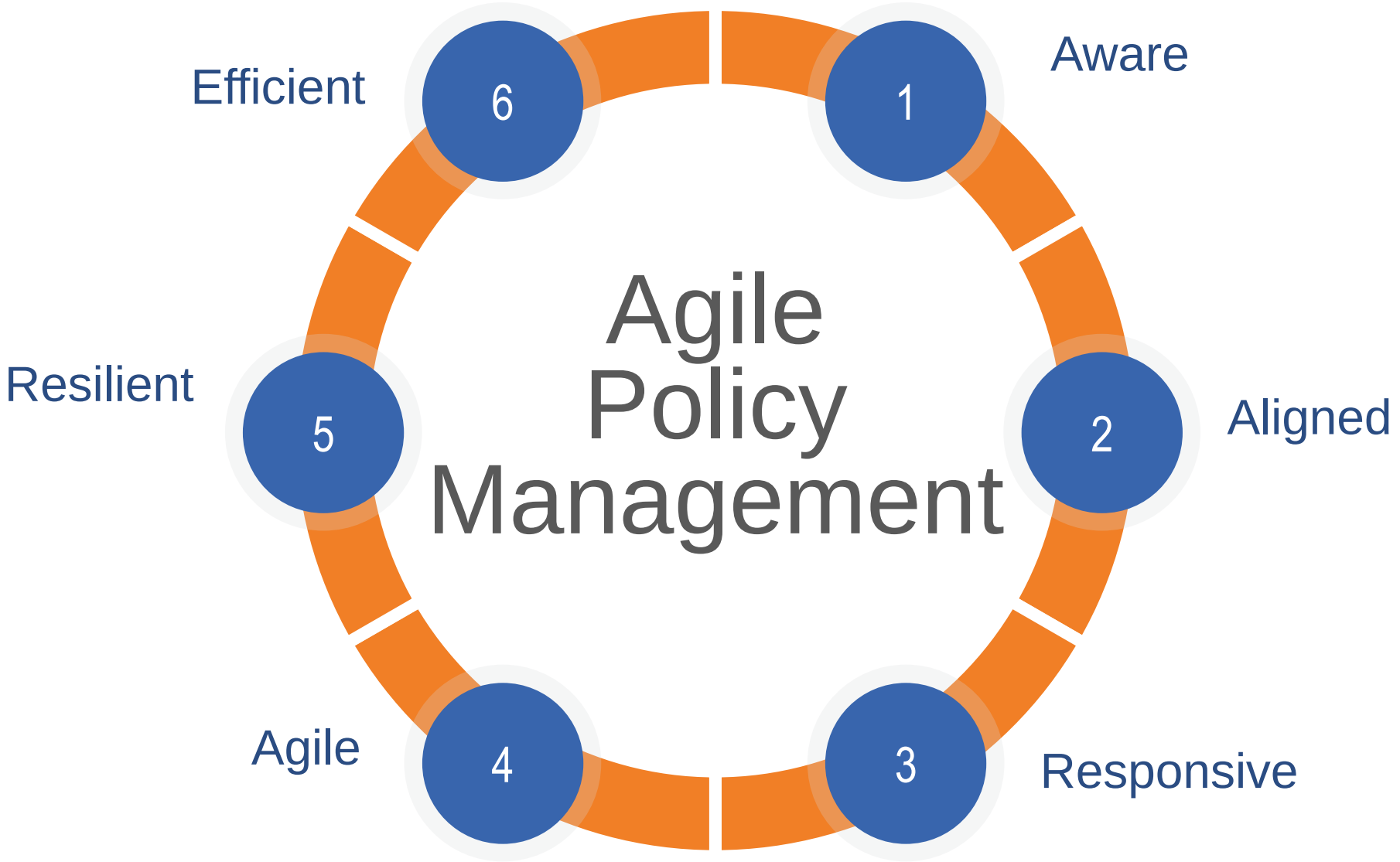


REPEATABLE CYCLE

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

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

Benefits of 360° Contextual Awareness of Policies



MCO KYO

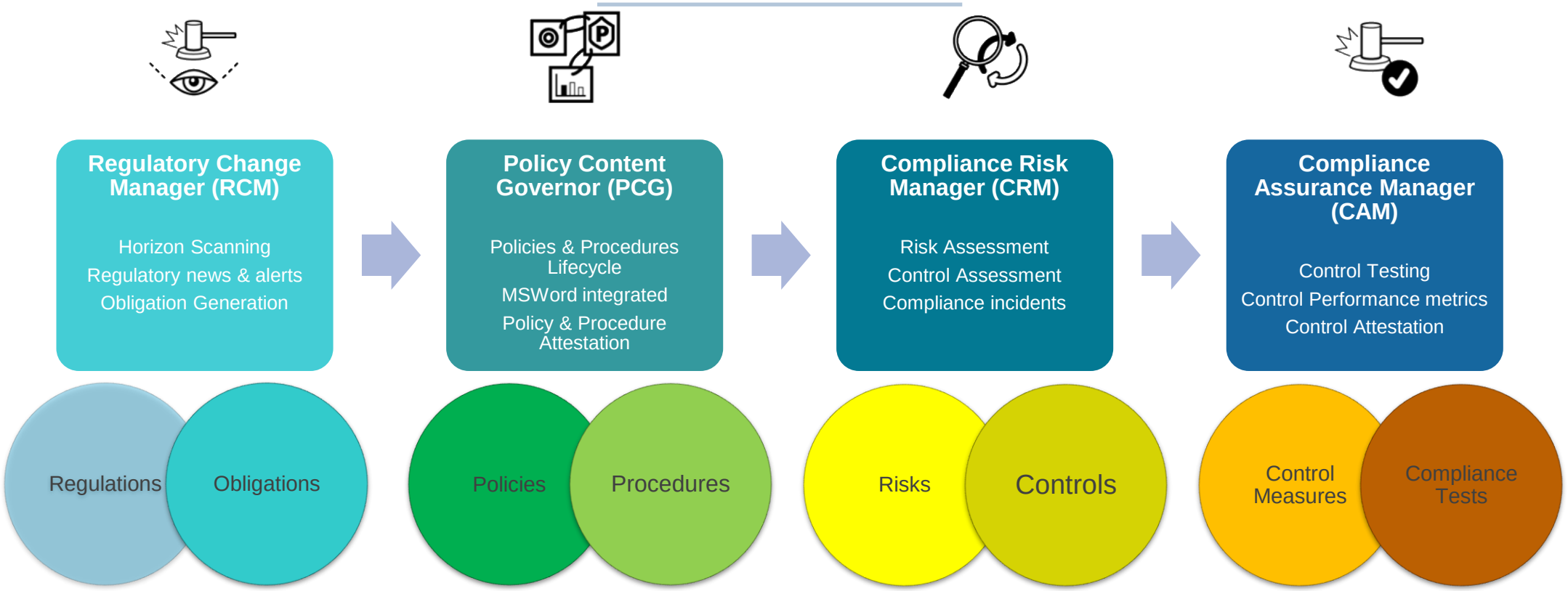
KYO is used by Chief Compliance Officers to support their entire compliance governance program through:

- Storage and management of libraries of regulations, obligations, policies, procedures, risks and controls
- Support for all the major compliance functions of regulatory change management, policy management, risk management and assurance
- Recording and tracking of all issues and actions
- Complete integrated reporting for compliance governance and oversight.

KYO helps our clients prove the firm’s compliance to both internal and external stakeholders

KYO is part of the integrated suite of compliance products from MCO

KYO



The KYO system is made up of four distinct products.

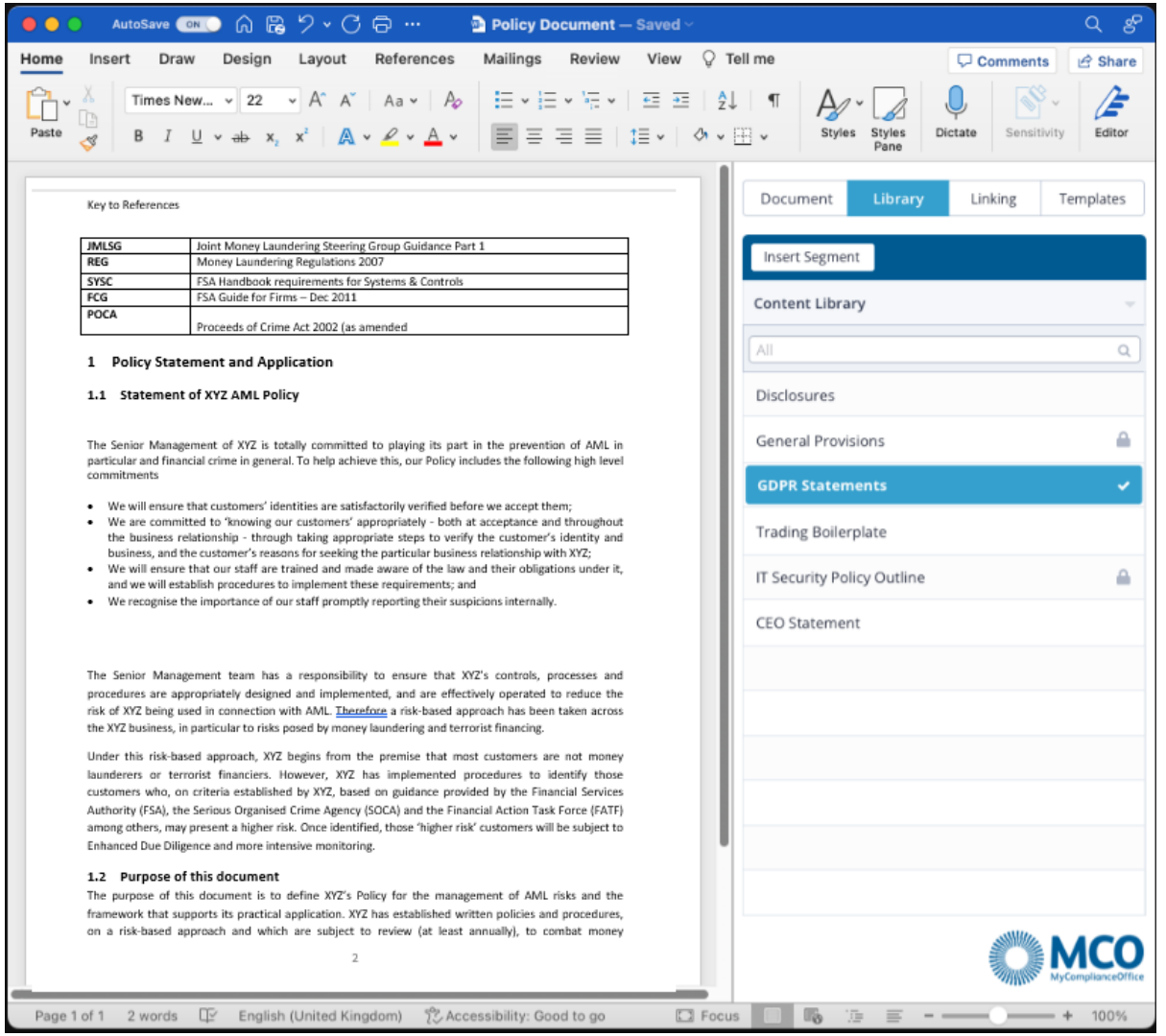
Clients can purchase one or more products safe in the knowledge that they have complete interoperability across the products and get the benefits of scale as they go on their compliance management journey.

MCO's "Policy Content Governor"

Product Features

Collaborative Editing with Word

- Real-time collaborative editing using online Word maximizes efficiency
- Add-In provides secured access to MCO entities and information that can be used and referenced by the policy
- Construct policies from templates and by including boilerplate content from client-administered library
- Pre-approved content can be included in policies and protected from changes by policy authors
- Policies are stored in secure MCO database

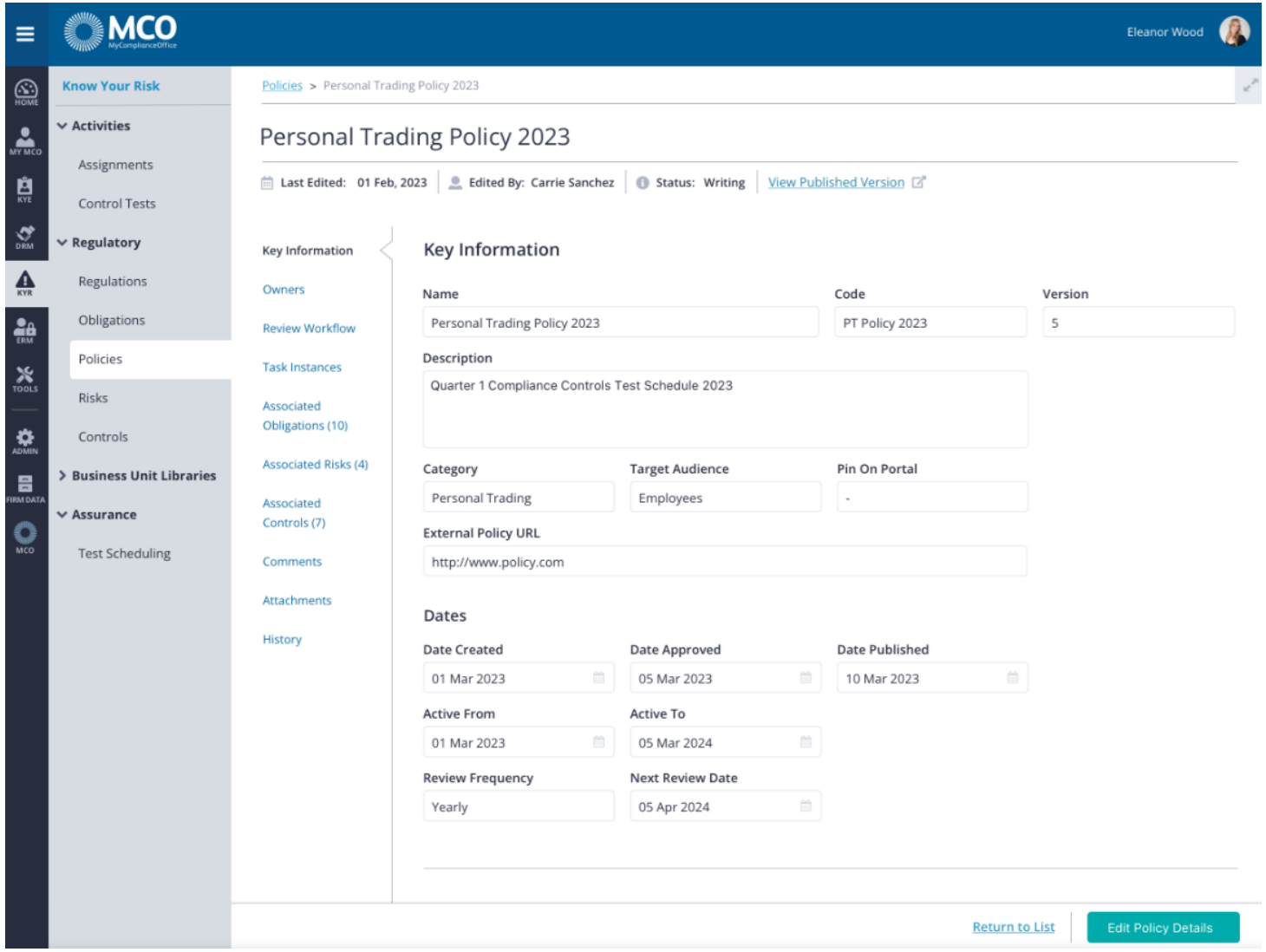


MCO's "Policy Content Governor"

Product Features

Policy Key Information

- Maintain all of a policy's key attributes to help categorize, keep them well organized and make them easier to find
- Assign Target Audiences to identify the specific groups of people for whom the policy is intended
- Configure review frequencies for policies which will trigger notifications to policy owners when the next scheduled review should take place
- The system will maintain key policy process dates for created, approved and published events
- System will automatically maintain versioning with each revise cycle that is conducted

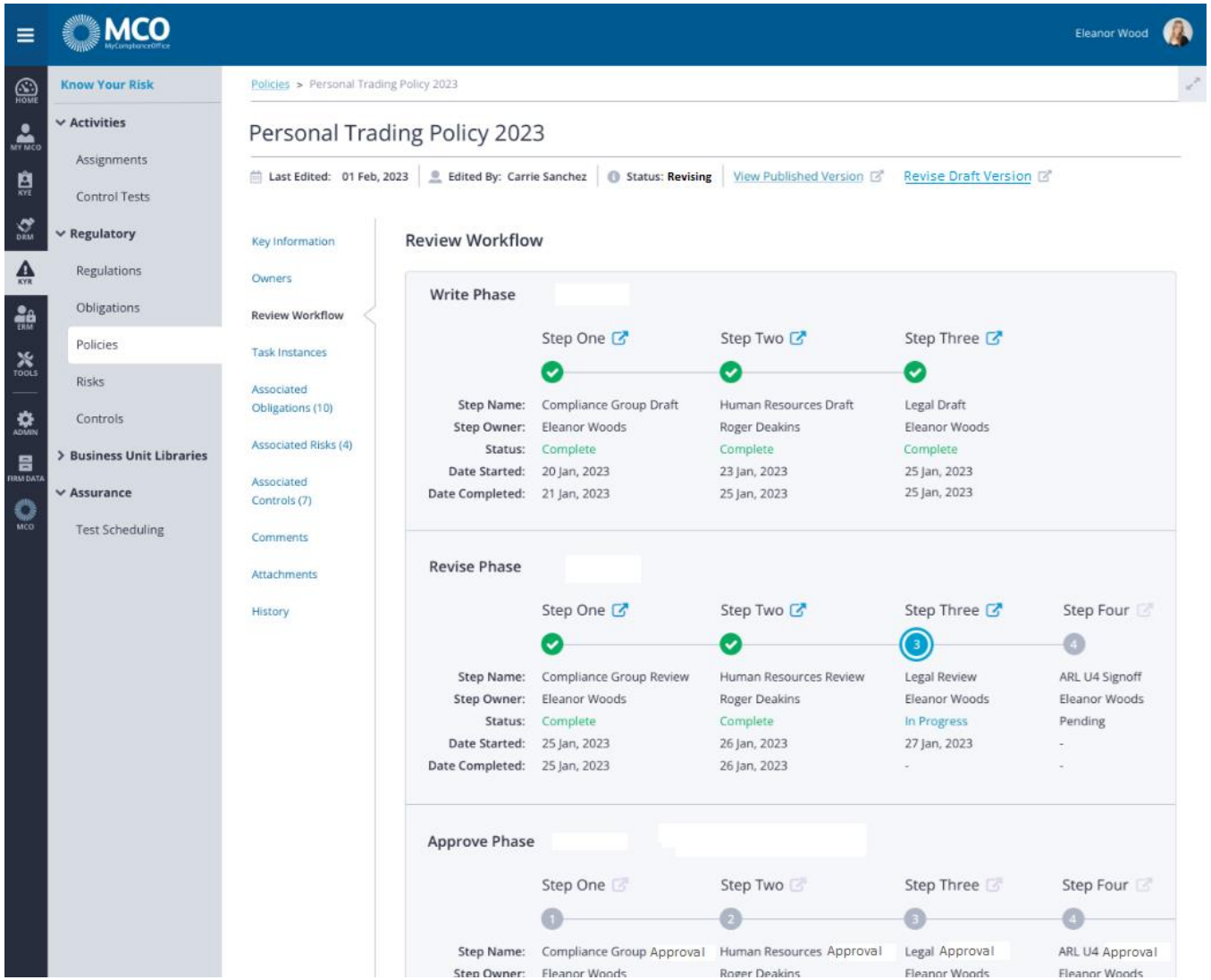


MCO's "Policy Content Governor"

Product Features

Process – Configurable Revise Cycles

- Configurable workflows manage the overall write, revise, approve and publish process while coordinating the efforts of various groups throughout the organization
- Establishes clearly defined roles and their context within the policy process
- Users are notified of their tasks and their work is tracked in an auditable manner
- Unique workflows can be configured for various types of policies and auto-assigned based upon policy type and other criteria

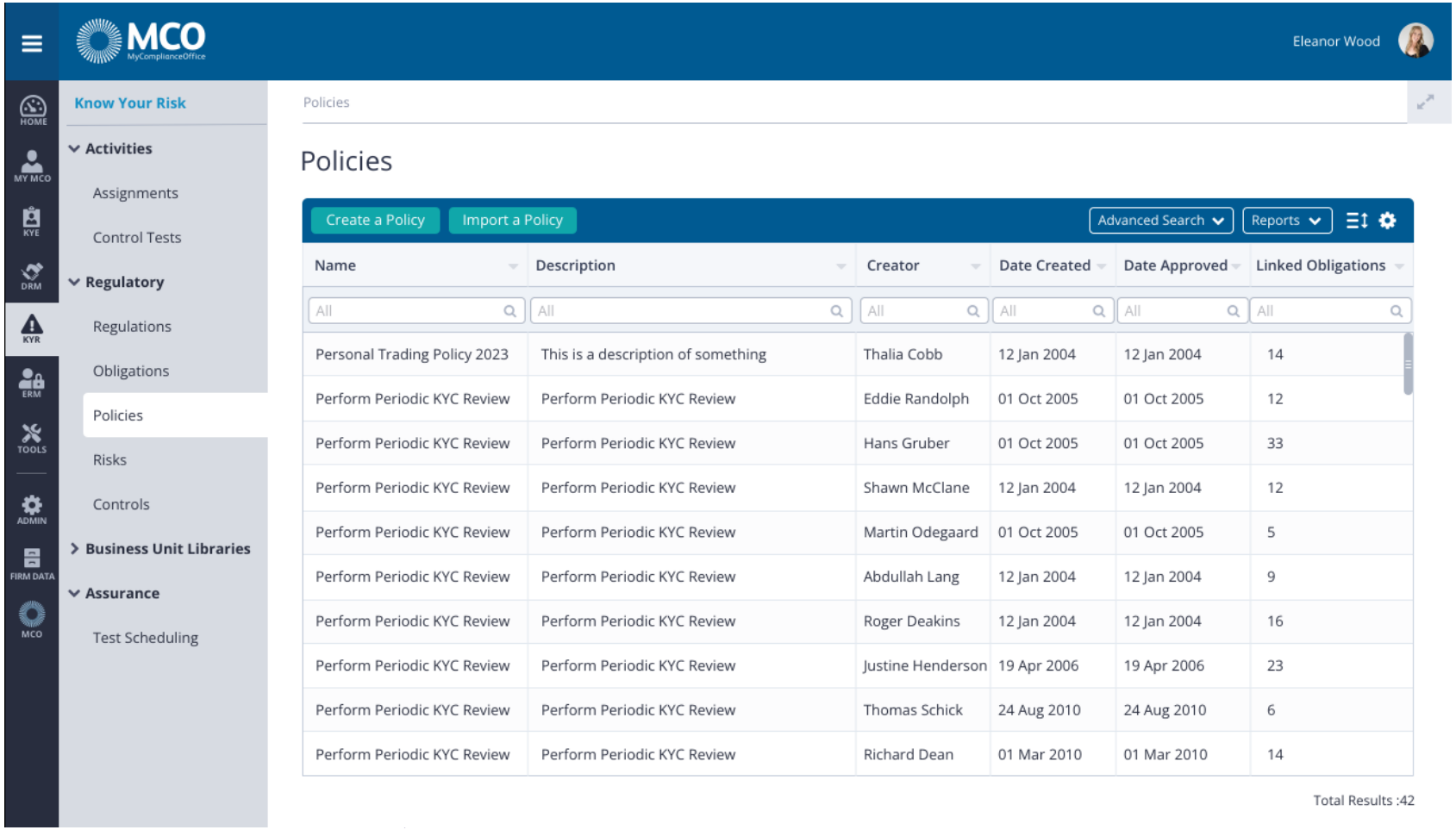


MCO's "Policy Content Governor"

Product Features

Storage & Distribution

- Single repository for all policy source content
- Restricts access to policies to the appropriate parties
- Provides robust version control
- Locate policies by primary attributes or configurable values and tags
- Proactively assign forms to users to solicit understanding and acknowledgement of a document.



Questions?

GRC 20/20 Research, LLC (GRC 20/20) provides clarity of insight into governance, risk management, and compliance (GRC) solutions and strategies through objective market research, benchmarking, training, and analysis.

Michael Rasmussen, J.D.

GRC 20/20 Research, LLC

The GRC Analyst, Pundit, & OCEG Fellow

mkras@grc2020.com

www.**grc2020**.com

+1.262.3329188

The GRC Report is the first word in governance, risk, and compliance news – providing leading analysis, insights, and updates for GRC professionals.

We are dedicated to delivering transparency and providing relevant news to help individuals and organizations stay informed in this ever-evolving field.

hello@**grcreport**.com

www.**grcreport**.com

© GRC 20/20 Research, LLC

Thank you!

For more information or to see an MCO demo email us at:

marketing@mycomplianceoffice.com