The Art of
Policy Management

Intro

Policies may be considered boring and mundane - like insurance. But no business would do without insurance, and effective policy management is just as critical. Robust policies & procedures set the tone of the organization and its values by defining behaviors, processes, relationships, and transactions - creating a roadmap for day-to-day operations. Without a comprehensive set of policies, businesses open themselves up to a world of ambiguity and unforeseen costs.

A bad policy approach can cost a business in many ways. From an internal perspective it can cost time & admin resources as teams struggle to find, write, update, and sign off policies without a clearly defined process. But it can also cost a business financially in the form of fines & penalties and operational inefficiencies that arise when organizations don't have effective policies with clearly defined controls to ensure they are being followed.

In this eBook we explore the latest technology capabilities available to streamline & automate the policy management process. Plus, we explain why policy management should be managed as part of a wider GRC program to ensure organizations have sufficient policies in place to mitigate known risks, ensure staff are operating in line with compliance requirements, and to implement sufficient governance regarding company values. Organizations that have no integrated GRC framework and manage policies in silos using manual processes or legacy systems, will end up with a library of inefficient policies that don't actively address key risk areas or compliance requirements.

Policies should provide the foundation for the entire organization to embrace unified operating standards, enabling everyone to understand what is expected of them, protecting the organization from employee misconduct. By mapping policy management to other GRC processes using the latest technology, organizations will be well positioned to introduce policies that address the most pressing issues from a risk and compliance perspective. A policy management solution that fully integrates with other GRC processes will ensure a best-practice, scalable process that provides business intelligence to mature and futureproof the organization.

Understanding the Value of Policies

The Open Compliance and Ethics Group (OCEG) leaves us in little doubt about the value of policies:

> Policies are the cornerstone of compliance in organizations of all sizes. Policies establish the guidance that must be followed when establishing procedures and engaging in the day-to-day operations of the business. Policies demand adherence to applicable laws and regulations, and also set out the mandate the organization's leadership establishes and deems necessary to support its values and objectives.

Organizations that overlook the value of well-planned policies & procedures typically implement weak versions as a box-ticking exercise, resulting in common challenges: they're hard to understand; they remain unused; they're used incorrectly; they quickly become outdated; and they're not governed. Policies and procedures that lack substance restrict business operations, with staff lacking guidance, compliance & governance becoming an afterthought, and undocumented operational processes creating inefficiencies.

Businesses of all sizes across industries have implemented policies and policy management processes with different degrees of success and value creation.

According to a KPMG survey of 220 Chief Compliance Officers:
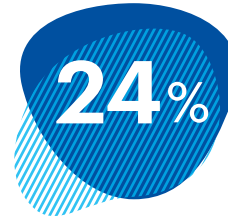
24% of businesses reported that they do not have a process to capture laws, rules, and regulations.
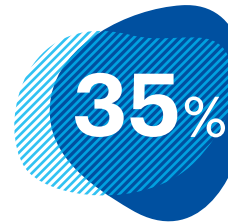
35% of businesses stated they do not have a process to maintain an inventory of laws, rules, and regulations.

This underscores a need to improve policy development and management to strengthen compliance and enhance strategic alignment to gain competitive advantage.

Disruption prompted by lockdown measures amid the COVID-19 pandemic – including remote working, fractured supply chains, and online operating models & payments – has underscored the need to have robust and agile policies and procedures in place.

Regulatory change has also been a key driver in the need for robust policy management processes - with many policies created to directly address regulatory requirements. Gifts & hospitality and Conflicts of Interest exemplify these. Just recently, an asset management firm was fined £9million (and the CEO had a personal fine of just under £250K) for breaches of regulatory requirements, not because they were looking for advantage, but because they didn't follow the rules. In the US the SEC has used the FCPA to leverage billions of dollars in fines (albeit most actors know what they are doing when they breach this law) and part of the settlement in the US is the implementation of a comprehensive anti-bribery and corruption framework applied through best practice policies and procedures. In addition to regulatory requirements, HR is another area where poor policy management can be costly to a business and ESG is likely to follow the same path as requirements grow.

In response to this changing landscape, businesses have been forced to reassess their existing policies and policy management processes in a bid to increase their efficiency and effectiveness – a mission that has seen automation emerge as a cornerstone of strong policy management.

Given the huge number of policies required to guide a business – the frequency at which they change, and the structured approval process needed to create and amend them before they go live – many organizations have turned to policy management software with wider GRC capabilities to automate the process and add structure.

Challenges of a Manual Policy Management Process

The traditional method of storing policies and procedures in a central shared location and coordinating revisions and distribution via email presents challenges for businesses. These antiquated processes create roadblocks for organizations – especially those with large numbers of policies. Here we explore some of the challenges a manual policy management process can create.

No consistent format or template

This lack of structure leads to inconsistent formatting, content, and language usage. Key areas can also be overlooked as policy templates lack a structured creation, storage and categorisation process.

Lack of version control

An inability to effectively track policies and procedures makes it difficult to know what the latest version is, when it was last revised, and when it is due to be revised. Manual processes make it difficult to track and view old versions and version history.

Unstructured approval process

Manual processes deprive organizations of a clear structure that indicates policies have been through the correct approval process before they go live. Without the user tracking facilitated by software it can be a challenge to obtain 'proof of sign-off'.

Difficult to track revisions and changes

Policies typically need to be reviewed and signed off by different stakeholders. Collating manual feedback can prove difficult, with written annotations and tracked changes in Word documents becoming confusing. Without structured workflows there is also a lack of visibility of which version has been approved to go live, who approved it and when.

Lack of ownership

Manual processes lack accountability creating confusion about who owns the policy and who it's relevant to. Without clear ownership of who is responsible for implementing changes relating to the policy and who signed it off, policies become outdated.

No clarity of employee attestation

When policies are circulated via email it's impossible to see who read the policy and who agreed to abide by it. This makes it difficult for an organization to confidently say that every employee has read and attested to the policies relevant to them.

Risk of information being lost

Using shared locations exposes a business to information loss: documents can be accidentally saved over; amendments can be inputted incorrectly; and information overwritten.

Risk of data breaches

Shared drives typically provide everyone with access to everything, increasing the risk of data being compromised. For example, research by Forrester has shown that 25% of data breaches were insider jobs, and 36% were the result of employee mistakes.

If shared drives sound like an outdated policy management tool, paper-based systems – which are still used by some businesses today – are a minefield of inefficiencies and risks. Not only are these traditional processes time-consuming to maintain and fraught with human error; but paper policies also pose serious security risks. In a survey by the Ponemon Institute, 61% of respondents were unsure or disagreed that the protection of paper documents is just as important as the protection of electronic records. When sensitive paper documents slip through the cracks, it can disrupt day-to-day operations, confuse employees, and create security issues.

Modern policy management requires businesses to look beyond inefficient manual processes to software that enhances the creation, approval, organization, and sharing of policy and procedure documents. These living documents must be agile enough to adapt to the changing business and threat landscapes and be circulated and tracked with ease.

Does your policy management process lack clarity?

If you can't answer these questions about your policies and procedures, your policy management process needs an overhaul.

Is this policy approved by all stakeholders?

When was this policy last reviewed?

Where is the policy saved?

Have staff reviewed this policy?

What is the process for that?

Is this policy still valid?

Are staff trained on this policy?

What is the latest version?

What policies are affected by the latest regulation Change?

Automating Policy Management with Software

Policy management software has emerged as the weapon of choice in the fight against policy-related disruption in the digital age. The global policy management software market was valued at $962.18 million in 2019 and is projected to grow to $3.06 billion by 2027.

This expanding market has given rise to innovative software tools that allow businesses to quickly upgrade their policy management processes and make changes that will have widespread and long-lasting benefits. For example, business leaders can easily assess the management of ongoing policies, identify areas that require improvement, and action worthwhile change quickly and effectively.

KPMG outlines the benefits of leveraging policy management through technology:

Identifies triggering events for new policies and updates to existing policies – such as new regulatory mandates or changes to industry-leading frameworks.

Streamlines and enhances policy development and establishes clear linkages to regulations and standards.

Ensures necessary reviews are performed and approvals are documented and retained.

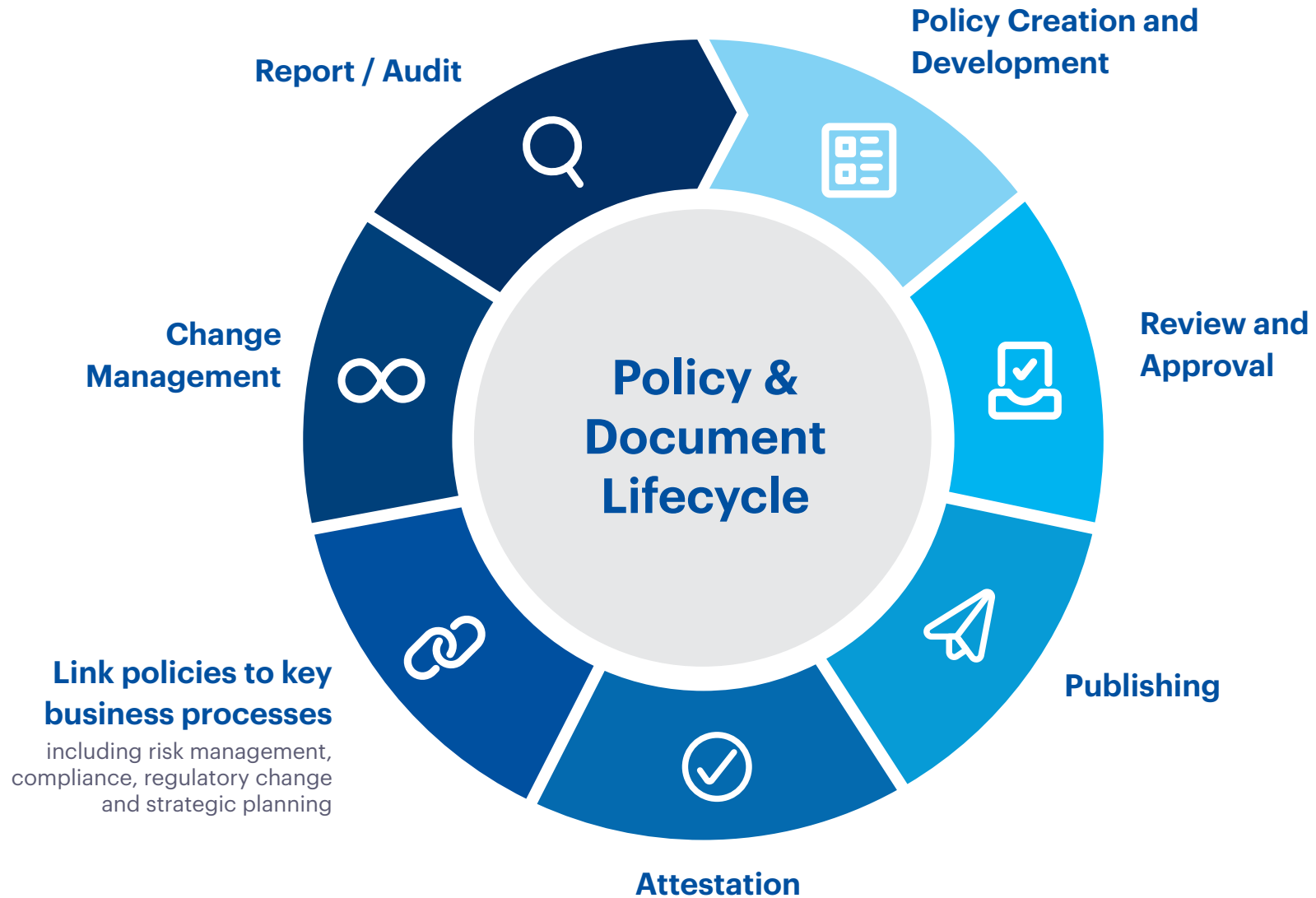Facilitates communication and training based on policy enhancements.

Monitors ongoing policy compliance by impacted groups by linking policy attestations, control testing results, and issues to relevant policy requirements.

Provides policy owners with meaningful insights into the entire policy management lifecycle: policy creation, maintenance, compliance issues, and remediation.

Policy Management Lifecycle

Policy & Document Lifecycle

- Policy Creation and Development
- Review and Approval
- Publishing
- Attestation
- Link policies to key business processes
  including risk management, compliance, regulatory change and strategic planning
- Change Management
- Report / Audit

With multiple policies to manage at once and many stages involved in their lifecycle – from creation & implementation to management & updating – automation can streamline your policy management program in many compelling ways.

Policy Creation

Proactive businesses harness technology that streamlines policy authoring and issuance to ensure a continual process, whether creating new policies or revising existing ones. Policy management software enables real-time collaboration, empowering stakeholders to simultaneously shape policies before implementing them. This ability to record additions, amendments and approvals provides a comprehensive history and audit trail of the development process.

Policy creation is a balancing act: too many policies can overwhelm an organization, while too few expose it to unnecessary risk. Software can prevent policies from being created for policy's sake or them being overlooked altogether by monitoring internal and external events and changes.

Once it has been established which policies will add value to the business, software enables you to create a template document for each. This contains specified fields that allow you to capture relevant information. Some fields will be bespoke, while others are relevant to all policies, such as:

✓ Policy name	✓ Approval required date
✓ Version	✓ Owners
✓ Start date	✓ Author
✓ Expiry date	✓ Reviewer
✓ Policy category	✓ Approval status

These common fields should be standardized and captured in a consistent format – making reporting on policies and their status more efficient.

With the right software, your business can automate Deloitte's seven recommendations for creating internal corporate policies that work:

💡 Determine how the relevant business process functions.

💡 Policies should be written in simple, understandable language with a clear structure.

💡 Avoid writing overly long documents and don't forget to cite existing company policies.

💡 Name the responsible persons to whom employees can turn for help and clarification of their questions and give their contact details.

💡 Once a new policy is adopted, send out an informational email briefly describing the new policy and how it should be implemented. Then, follow up with periodic refresher courses for employees.

💡 Send out periodic email reminders about the key provisions of the policy.

💡 Create a quick sheet or checklist outlining the key provisions of core policies.

Automating the Policy Approval Process

The comprehensive policy approval process facilitated by software provides the documents with validity that underpins their successful implementation. This validation from relevant stakeholders ensures consistency with current company-wide expectations. Without a robust approval process - your policies run the risk of being challenged at different levels of the organization, and as a result could remain unused.

Once policies are created, they must pass through a series of approvals before going live. New or revised policies will be subject to sign off from various stakeholders across the business, including department heads, compliance managers, HR leaders and IT teams. Stakeholders involved in the sign off process might want to make alterations to the policy. It is the responsibility of the policy owner to collate any alterations, addressing any conflicting changes and amending the policy to reflect the changes. Amendments may be identified in several ways – from handwritten notes and instructions via email to tracked changes in Microsoft Word – all of which should be recorded centrally. Therefore, if there are questions regarding an amendment while the policy is in use, it can be easily referenced by the relevant stakeholders.

Mature organizations with multiple policies to manage, use purpose-built policy management tools to automate the approval process through a series of workflows. The software adds structure to the approval process by facilitating comprehensive and accurate record-keeping of all amendments made during policy creation and attaching them to the final policy document.
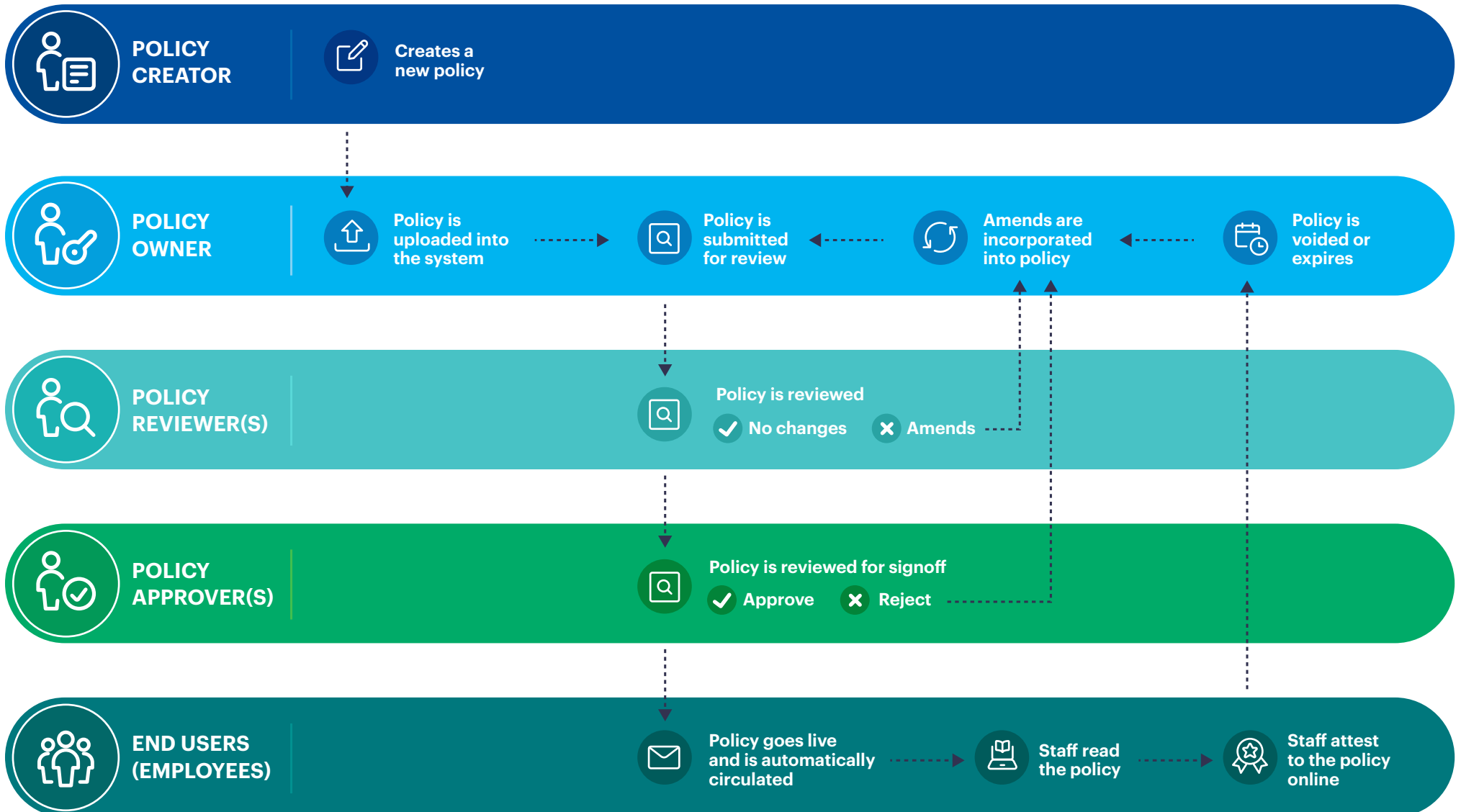
Once a policy is drafted by the policy owner and uploaded to the system, a predefined approval workflow is triggered, automatically sending the draft document to the relevant stakeholders in the approval chain. They will receive notifications regarding deadlines for feedback - and follow-up emails if they are late to respond. The policy owner is then automatically notified when all changes have been submitted, so they can make the necessary updates.

The policy owner can then recirculate the policy and repeat this automated process until the document is signed off by all stakeholders, before setting it to go live. Controls can be set to notify policy owners when it's due to expire. A record of the old versions – including all amendments and feedback – is automatically saved in the system before being attributed to the relevant user. This adds a layer of security to version control and document history and keeps a comprehensive log of all actions.

Policy Approval Workflow

Here is a typical example of a policy approval workflow from creation and approval to publication and attestation. Most policy management solutions will let you tailor the workflows to suit the specific needs and structure of your organization.

POLICY CREATOR
- Creates a new policy

POLICY OWNER
- Policy is uploaded into the system
- Policy is submitted for review
- Amends are incorporated into policy
- Policy is voided or expires

POLICY REVIEWER(S)
- Policy is reviewed
  - ✓ No changes
  - ✗ Amends

POLICY APPROVER(S)
- Policy is reviewed for signoff
  - ✓ Approve
  - ✗ Reject

END USERS (EMPLOYEES)
- Policy goes live and is automatically circulated
- Staff read the policy
- Staff attest to the policy online

By automating the policy approval process, you will benefit from a complete time-stamped history once it's live including: when the policy was created, who by, who approved it and when, and what amendments they requested. This data streamlines the policy reporting process, allowing you to view reports on policy owners, expiry dates, active policies, policies that are in the approval chain, and obsolete policies.

Software triggers automatic workflows that send email notifications when actions are due, for example:

Inbox

- A policy is due to expire
- A policy needs reviewing or approving
- You have an overdue task
- Please read and attest to this policy.

The automated emails contain links to the software - taking the user to the relevant screen to complete their policy related task. Once the action is complete, the system will then notify the next stakeholder in the workflow, requesting them to complete their action. This establishes open lines of communication between teams and keeps processes moving, flagging deadlines before they become critical.

Empowered by a clear view of their related tasks, policy managers & approvers have oversight of which policies need approval, which policies they need to write, when a policy they own is about to expire, and what current policies owned by them have outstanding actions – allowing them to drill down into the detail of each policy, including version history and approval status.

Accountability & Permissions

Policy management technology removes the clutter, ensuring both end-users and managers & approvers only see information that's relevant to them. They will be presented with their own dashboards. If an employee is not involved in owning, writing, attesting, or approving a policy, they will not see the information on that policy unless permissions are changed. This reduces the noise and helps employees focus on relevant tasks. Software still allows you to create a library of current policies that can be viewed by everyone - and end-users of the policy will only see relevant live policies that they must attest to and follow.

Most policy management solutions allow employees to attest to policies within the system. An email alert will be triggered asking them to read and attest to the policy by a certain deadline. Automatic email reminders will be sent if they fail to attest to the policy. This provides managers with a clear view of which employees have read and agreed to the policy. If the policy is not adhered to, managers will have sufficient proof that the policy was rolled out and the employee agreed to abide by it. This evidence can be used in employee disciplinaries and tribunals and to satisfy requirements from auditors and regulators.

Taking Policy Management to Another Level

Business leaders can break down operational silos by linking policy management data with risk registers, compliance obligations libraries, incident management portals, and strategic plans to ensure policies are always up to date with the latest laws and guidance. Here we explore how different business areas can be linked to policy management and highlight some of the benefits.
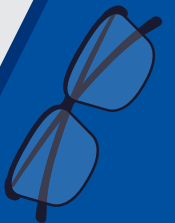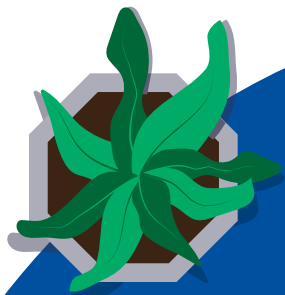
Linking Policy Management and Regulatory Change
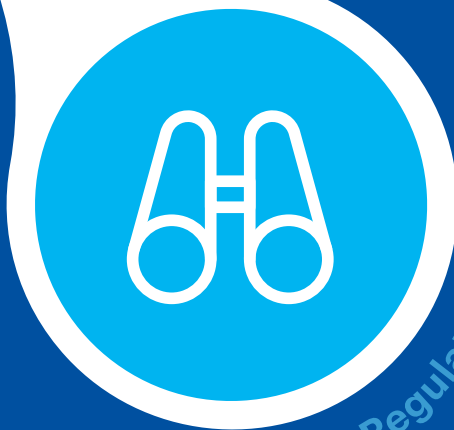
To say the regulatory landscape is subject to change is an understatement: businesses are spending more than $300billion dealing with regulatory change amid a determination by regulators to create a watertight system in the wake of tumultuous events like the 2008 financial crisis and the COVID-19 pandemic.

To stay ahead of the curve, policy management must be a dynamic process that links back to your regulatory change management program. By linking policies with regulatory or legislative content, policy documents can be updated to align with new guidelines – ensuring the business remains compliant. When a regulatory change arises, policy owners should be automatically notified to review any associated policies and assess if they need updating to align with recent guideline changes.

Extensive obligations libraries that house both policies and regulatory & legislative content will help you identify any required changes to policies and procedures – and roll them out across the business efficiently. For ultimate visibility, choose software that offers horizon scanning – this functionality feeds in regulatory content from relevant third-party providers in easily digestible chunks, providing details of upcoming regulatory changes and explanatory details detailing how they will impact operational procedures. The ability to monitor regulatory change and link it to relevant policies without delay creates an agile approach. This real-time tracking of global regulatory change, combined with intuitive linkage of impacted policies, fosters dynamic controls amid constant flux in the regulatory landscape. It demonstrates that the business is taking the due care and attention needed to address regulatory change at a companywide level without delay and provides an essential audit trail for regulators.

Policy Management

Regulatory Change

Linking Policy Management and Compliance using Automated Control Monitoring

Policy Management

Compliance

Automated Control Monitoring

Policy management and compliance go hand in hand: both require staff to behave in a certain way; both require structured processes to get staff to comply; both require version control; both require approval, sign-off, adoption and implementation; and both are subject to change.

Common frameworks can facilitate and link compliance and policy management – notably, an internal control framework backed up by automated workflows and trigger notifications. This functionality provides an essential layer of policing in the compliance process. These mechanisms, rules and procedures ensure ongoing compliance with external laws and legislation as well as your own internal policies & procedures.

From a compliance perspective, internal control thresholds can be established to notify relevant stakeholders about potential scenarios including when there is a risk of non-compliance, when revisions of compliance obligations are overdue; when signoffs and approvals are required or missed, to flag anomalies or thresholds in large data sets, and to request attestations for new policies or procedures that have changed.

Robust internal controls that support the compliance process have holistic benefits, it stabilizes internal operations and business functions by providing C-level executives with better control and visibility of what policies & procedures are being followed and highlights any risks of non-compliance. It eliminates manual work, admin, and checks - and adds a layer of automation saving both time and resources.

Linking Policy Management and Risk Management

Policy management & risk management are closely linked, when policies and regulations are not followed correctly, this ultimately becomes a risk to the business. Similarly, if no policy is in place or policies are out of date it could enable employees to go rogue and undermine the business.

Appropriate policies and procedures also underpin an effective risk management process, businesses should set out formal processes to communicate, escalate, and report risks. But is enough being done? McKinsey's annual global board survey of approximately 1,500 corporate directors found that just 7% of respondents gave their boards the highest rating for risk management, and only 40% say their organizations are prepared for the next large crisis.

The tide is turning, but it's taken the worst public health crisis in modern history for businesses to realize the value of risk management. Amid enforced homeworking, fractured supply chains and heightened cyber threats, many organizations soon realized they were underprepared for a black swan event. This realization that proactive risk management is a vital element of business resilience has cemented the value of robust policies & guidelines around the reporting of incidents and near misses, and the need to keep procedures up to date. Businesses a viewing those 'unlikely' yet 'high-impact' risks through a new lens and exploring these scenarios as part of a strategic risk program.

Some policies spring into action when a certain level of risk tolerance is reached, while some policies adopt the 'prevention is better than the cure' approach. They empower you to react proactively by anchoring risk management into existing strategic planning processes. This instils a culture of actionable risk-informed decision-making from the top down that provides the foresight to prevent high-risk incidents and ensure sustainability. Automated control monitoring can be used to flag risk levels and trigger policy revisions when required.

Linking Policy Management and Third-Party Risk

Managing the risks posed by the network of third-party vendors that businesses use to facilitate their operations is becoming increasingly complex. A lack of appropriate controls within this network can have a detrimental impact on your business – from financial stability to cybersecurity, equally a wrong action from a third-party can tarnish your company reputation.

To mitigate these risks, it's essential to have strong governance and oversight of your extended vendor operations. This includes visibility and influence over supply chains, software and technology providers and external contractors to ensure they comply with relevant operating standards and regulations, SLA's, KPIs and relevant cyber & data privacy laws.

By aligning relevant policies with your third-party risk management program – including vendor analysis and vendor risk assessments – it's possible to achieve a holistic and converged approach to managing the myriad of risks posed by these service providers. Get this right and you will benefit from value protection and value creation through the identification of vendors that enhance your business.

Relevant policies should be shared with third parties, and they must attest to them. If you have specific policies linked to specific third parties regarding service level agreements (SLAs) or key performance indicators (KPIs), they should be fully documented and agreed by both parties. You can introduce policies as part of your third-party selection process.

Linking Policy Management and **Business Continuity**

Policy Management

Business Continuity

Since the pandemic, business continuity has become a high priority on the boardroom agenda – and effective policies provide the bedrock for continuing business operations in the event of a crisis. In tandem, they form a vital tool in your business's risk management arsenal: having access to a set of up-to-date policies, standards and guidelines instils resilience by supporting your business to get back up and running quickly when unexpected events occur.

Implementing effective policies, rules and procedures embeds the agility needed to react quickly and efficiently to potentially detrimental events, so essential services can resume, and recovery can be achieved in the shortest possible timeframe. The benefits of this approach are compelling as it supports the strategy, creates strategic advantage, provides stakeholder, investor, and customer reassurance, and mitigates operational vulnerabilities.

To achieve this, business policies should comprise a library of business procedures that can be harnessed when a disruption occurs – especially major incidents such as an IT system being compromised by a cyber-attack. Before this can occur, you must understand the specific risks your organization is likely to face and how often they will occur using a risk assessment.

Linking Policy Management and IT Security

Businesses' ever-increasing reliance on data and IT systems have made IT security a corporate touchstone. The attack surface was already widening at an alarming rate for cybercriminals before the pandemic dealt an indiscriminate blow to businesses. Cyber-attacks suddenly escalated in frequency and scope amid lockdown restrictions – bringing robust IT security policies and procedures into even sharper focus for business leaders.

The confluence of well-rounded policies and IT security leads to the creation of another vital element of risk management: IT security policy management – the process of identifying, implementing, and managing the policies and procedures that everyone must adhere to when accessing and using your IT assets and resources.

IT security policies set out the protocol for a range of related actions, including connecting to the network with personal devices, defining how data is classified, and outlining security controls. By successfully linking policy management and IT security, you can keep everyone working towards a common goal as both security threats and your business evolve. Effective security policy management in this respect provides guidelines for how employees should interact with technology, includes regulatory requirements for data protection, and helps prevent security misconfigurations.

Failure to link the two may expose you to legal liability. For example, necessary policy changes from a regulatory perspective might slip through the cracks, leaving existing policies outdated and making the risk of non-compliance a threat.

Linking Policy Management and Corporate Strategy

A common misconception exists in the business world: policies exclusively impact operations. It's easy to erroneously assume that policies and procedures are only important within the context of day-to-day operational activities – after all, a policy is concerned with guiding actions. But strategy and operations are inextricably linked; therefore, business leaders can't make informed strategic decisions without considering operational realities. Strategic decision-makers must both understand the policy management process within their organization and the impact their decisions will have on operations.

In reality, policies are created to support strategies, such as achieving operational goals. A strategic vision is typically set by business leaders to provide an overarching plan for the business. New or established policies provide a framework for informed decision-making and activities carried out throughout the business that contribute to achieving that vision.

Efficient policy management processes and extensive obligations libraries will help you keep track of strategic requirements, monitor progress, identify changes to policies and procedures – and roll them out across the business.
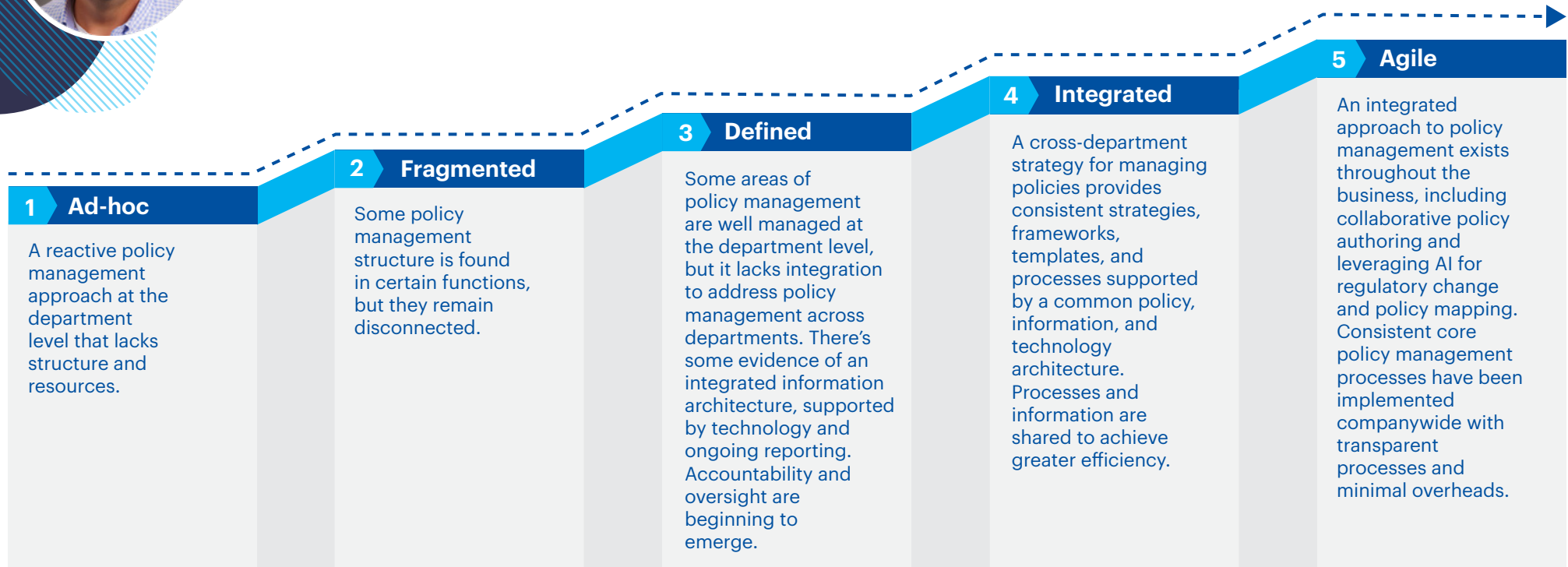
Policy Management Maturity

Can you look around the corner and build a clear view of policy development, implementation, and maintenance? If the answer is no, your business will be hamstrung by reactive policy management – a short-sighted approach to policies and procedures that restricts your organization's holistic view, inhibiting planning and transparency. This siloed policy management style typically occurs at the departmental level, leading to a detached, obscure layer of scattered documents on shared drives and internal websites. A subsequent lack of planning, engagement, and communication means policies are created on an ad-hoc basis where stakeholders are forced into a box-ticking process that lacks substance. Your business must, therefore, embark on a journey of policy management maturity.

According to GRC 20/20 Analyst and Pundit Michael Rasmussen, there are five stages of maturity:

1 Ad-hoc

A reactive policy management approach at the department level that lacks structure and resources.

2 Fragmented

Some policy management structure is found in certain functions, but they remain disconnected.

3 Defined

Some areas of policy management are well managed at the department level, but it lacks integration to address policy management across departments. There's some evidence of an integrated information architecture, supported by technology and ongoing reporting. Accountability and oversight are beginning to emerge.

4 Integrated

A cross-department strategy for managing policies provides consistent strategies, frameworks, templates, and processes supported by a common policy, information, and technology architecture. Processes and information are shared to achieve greater efficiency.

5 Agile

An integrated approach to policy management exists throughout the business, including collaborative policy authoring and leveraging AI for regulatory change and policy mapping. Consistent core policy management processes have been implemented companywide with transparent processes and minimal overheads.

The journey to achieving – and maintaining – agile policy management must be underpinned by a common thread that runs throughout this evolution: technology. By automating the policy management process, your business will be empowered by proactive policy insight that allows you to identify, analyse, manage, and monitor them in the context of operations, processes, and roles – from harnessing a central policy register that can be viewed by all for a top-down view of policies and bottom-up participation, to building a clear view of policy ownership, sign-off, and attestation. As well as exploring the current state of policies and policy management, technology provides you with invaluable foresight by continuously monitoring change and capturing those adjustments in your policies.

All of which combines to transform policy management from a reactive to a proactive process, creating greater alignment between your business's policies and its strategy, culture, speed to market, efficiency, and regulatory requirements.

About Camms.

Camms software can help you make the right business decisions and add structure to your operations using a centralized platform that provides a comprehensive approach to policy management.

By automating the policy management process, Camms software has the power to:

- Link policy management to your broader GRC universe by mapping policies to risk management, strategic planning, compliance obligations, and incident management.

- Horizon scan and notify you of relevant regulatory changes that will impact your policies.

- Set up workflows to facilitate the implementation, approval, sign off, and maintenance of policies throughout your organization.

- Host centralized registers and libraries that provide a transparent, holistic view of all policies – enhancing ownership, sign-off, and attestation.

- Facilitate informed decisions based on real-time analytics and up-to-date information.

- Align your policies with industry best practice workflows, including change notifications, risk assessments, automated review processes and detailed action plans.

- Generate sophisticated reports and audit trails instantaneously.

- Provide business leaders with access to a centralized dashboard for improved policy analysis.
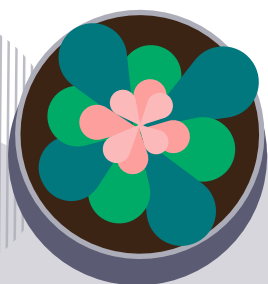
Achieve Proactive Policy Management with Camms

Our solution enables organizations to access policy creation templates and establish an on-line policy library - capturing key information regarding policy owner, expiry date, approval stage, and version number.

The software enables organizations to automate the entire policy management life cycle including policy creation, version control, approval, publishing, and attestation - creating a comprehensive log for audit purposes & employee tribunals. The solution is part of our wider GRC platform enabling organizations to link policy management to risk management, compliance, and strategic planning to further mature their processes.

Our team would love to learn about your policy management challenges, and wider GRC priorities, and explore how technology can help you achieve success.

Visit Website   **Request Demo**

Camms.
Software to Change Tomorrow.