GRC Illustrated Series

THE PATH TO COMPLIANCE OBLIGATION MANAGEMENT

DEVELOPED BY oceg®

WITH CONTRIBUTIONS FROM complí cool, calm and compliant.™

Organizations are plagued by a flood of compliance-based requirements driven by laws, contracts, standards, and other influencers. By following the path to effective Compliance Obligation Management (COM), the organization and subject matter experts can work in a synergistic way to retune the compliance program, mitigate risk, and satisfy regulators, auditors, directors, and other stakeholders.

IDENTIFY AND UNDERSTAND

RISK FACTORS

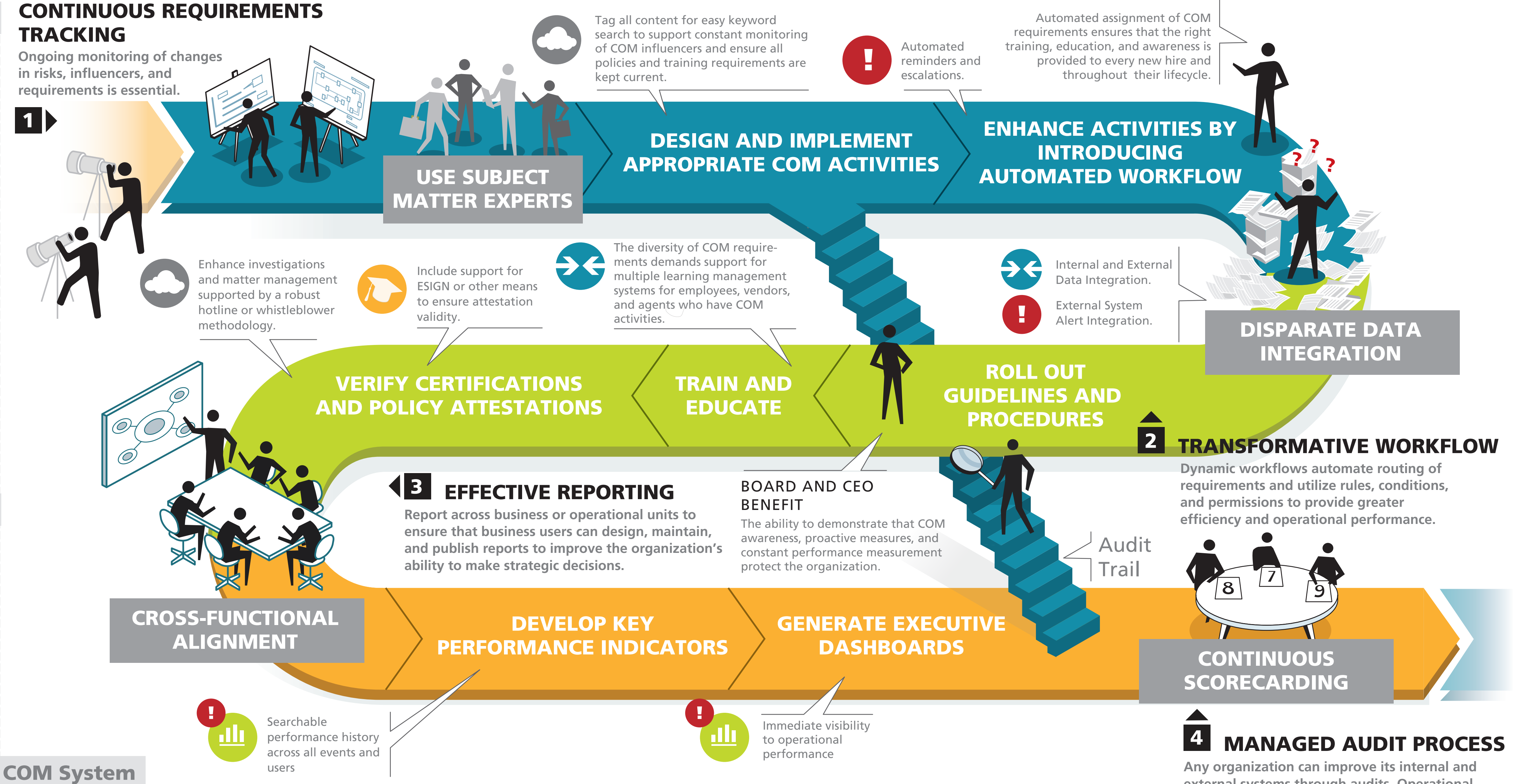
- Fines & Penalties
- Reputation Risk
- Ineligibility for Contracts
- Insurance Availability
- Event Response Costs
- Business Interruption

INFLUENCERS

- International Mandates
- Fed/State/Local Regulations
- Industry Guidelines
- CSR Initiatives
- NGO Expectations
- HR/EE Requirements
- Third-Party Relationships

COMMON COM ACTIVITIES

- Policies & Procedures
- Guidelines & References
- Attestations
- Computer-Based Training
- Classroom Training
- Incident Reports
- Escalations
- Awareness & Alerts



1 CONTINUOUS REQUIREMENTS TRACKING

Ongoing monitoring of changes in risks, influencers, and requirements is essential.

USE SUBJECT MATTER EXPERTS
DESIGN AND IMPLEMENT APPROPRIATE COM ACTIVITIES
ENHANCE ACTIVITIES BY INTRODUCING AUTOMATED WORKFLOW
DISPARATE DATA INTEGRATION
ROLL OUT GUIDELINES AND PROCEDURES
TRAIN AND EDUCATE
VERIFY CERTIFICATIONS AND POLICY ATTESTATIONS
CROSS-FUNCTIONAL ALIGNMENT
DEVELOP KEY PERFORMANCE INDICATORS
GENERATE EXECUTIVE DASHBOARDS
CONTINUOUS SCORECARDING
Audit Trail
8
7
9
?

Tag all content for easy keyword search to support constant monitoring of COM influencers and ensure all policies and training requirements are kept current.

Automated reminders and escalations.

MANAGEMENT BENEFIT

Automated assignment of COM requirements ensures that the right training, education, and awareness is provided to every new hire and throughout their lifecycle.

Enhance investigations and matter management supported by a robust hotline or whistleblower methodology.

Include support for ESIGN or other means to ensure attestation validity.

The diversity of COM requirements demands support for multiple learning management systems for employees, vendors, and agents who have COM activities.

Internal and External Data Integration.

External System Alert Integration.

2 TRANSFORMATIVE WORKFLOW

Dynamic workflows automate routing of requirements and utilize rules, conditions, and permissions to provide greater efficiency and operational performance.

3 EFFECTIVE REPORTING

Report across business or operational units to ensure that business users can design, maintain, and publish reports to improve the organization's ability to make strategic decisions.

BOARD AND CEO BENEFIT

The ability to demonstrate that COM awareness, proactive measures, and constant performance measurement protect the organization.

Searchable performance history across all events and users

Immediate visibility to operational performance

4 MANAGED AUDIT PROCESS

Any organization can improve its internal and external systems through audits. Operational history, easily navigated audit trails, and general process understanding can strengthen two-way communication and inspire teamwork based on trust. Whether it is compliance, quality, safety, environment, or data security, audit reports are necessary to improve business operations.

Key Elements of an Effective COM System

Cloud-Based Storage & Data
The cloud offers boundless capacity: maintaining security requirements and respecting compliance mandates. Cloud-based storage reduces costs and minimizes the complexity required to deliver services, making organizations more agile and productive.

Dashboards & Reporting
Today's users need the ability to control the visualization and analysis of their data in real-time. Flexible, tailored dashboards and integrated reports allow executives and managers to quickly drill down and assess areas of concern and operational progress.

Alerts & Notifications
Throughout the COM process, various events require the generation of automatic alerts and notifications for submissions, approval and items for review, or critical incidents and other escalations that require immediate attention.

API Connectors
A robust application programming interface (API) is essential for high-performing COM execution. APIs allow for seamless internal and external interoperable applications, data sources, Web services, and legacy systems.

Training & Certification
A robust education and certification solution will support multiple LMS and provide access to irrefutable certification methodology, whether the training was instructor-led, self-paced, or delivered online.

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

GRC Illustrated

The Journey to Advantaged GRC

As organizations mature their approach to GRC, they transition from a structure of siloed departments and units to a fully engaged business operation where everyone has a part in managing risk, ensuring compliance and contributing to performance outcomes. This leads to greater confidence, agility and resilience - advantages that ensure success.

DEVELOPED BY
OCEG®

WITH CONTRIBUTIONS FROM
RSA®
The Security Division of EMC

Siloed GRC

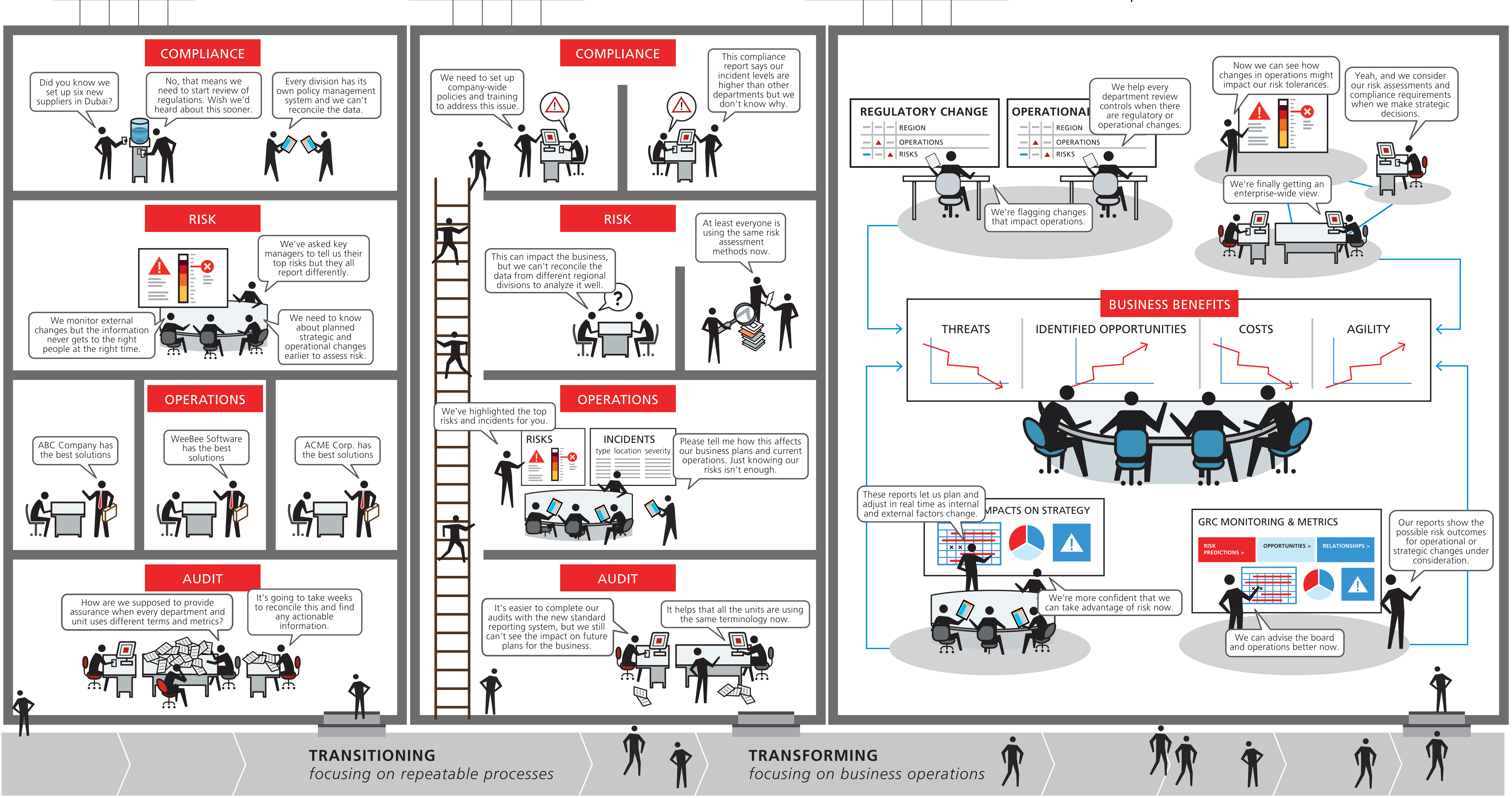
- Focus on compliance
- Reporting is disconnected
- Processes are isolated

Managed GRC

- Focus is on risk
- Reporting is coordinated
- Processes are defined

Advantaged GRC

- Focus is on business opportunity
- Reporting is enterprise-wide
- Processes are optimized


COMPLIANCE
Did you know we set up six new suppliers in Dubai?
No, that means we need to start review of regulations. Wish we'd heard about this sooner.
Every division has its own policy management system and we can't reconcile the data.
RISK
We've asked key managers to tell us their top risks but they all report differently.
We monitor external changes but the information never gets to the right people at the right time.
We need to know about planned strategic and operational changes earlier to assess risk.
OPERATIONS
ABC Company has the best solutions
WeeBee Software has the best solutions
ACME Corp. has the best solutions
AUDIT
How are we supposed to provide assurance when every department and unit uses different terms and metrics?
It's going to take weeks to reconcile this and find any actionable information.
COMPLIANCE
We need to set up company-wide policies and training to address this issue.
This compliance report says our incident levels are higher than other departments but we don't know why.
RISK
This can impact the business, but we can't reconcile the data from different regional divisions to analyze it well.
At least everyone is using the same risk assessment methods now.
OPERATIONS
We've highlighted the top risks and incidents for you.
RISKS
INCIDENTS
type location severity
Please tell me how this affects our business plans and current operations. Just knowing our risks isn't enough.
AUDIT
It's easier to complete our audits with the new standard reporting system, but we still can't see the impact on future plans for the business.
It helps that all the units are using the same terminology now.
REGULATORY CHANGE
REGION
OPERATIONS
RISKS
OPERATIONAL
REGION
OPERATIONS
RISKS
We help every department review controls when there are regulatory or operational changes.
We're flagging changes that impact operations.
Now we can see how changes in operations might impact our risk tolerances.
Yeah, and we consider our risk assessments and compliance requirements when we make strategic decisions.
We're finally getting an enterprise-wide view.
BUSINESS BENEFITS
THREATS
IDENTIFIED OPPORTUNITIES
COSTS
AGILITY
These reports let us plan and adjust in real time as internal and external factors change.
MPACTS ON STRATEGY
We're more confident that we can take advantage of risk now.
GRC MONITORING & METRICS
RISK PREDICTIONS >
OPPORTUNITIES >
RELATIONSHIPS >
We can advise the board and operations better now.
Our reports show the possible risk outcomes for operational or strategic changes under consideration.
TRANSITIONING
focusing on repeatable processes
TRANSFORMING
focusing on business operations

Contact info@oceg.org for comments, reprints or licensing requests ©2016 OCEG for additional GRC illustrations and resources visit www.oceg.org/resources

How Business, IT and Security Teams Gain a Common View of Risk

In today's digital business ecosystem, information technology and security teams need to build more proactive and value-driven IT risk and IT compliance programs. They need to preserve business operations and their supporting technology environment, and protect regulated and sensitive information from security breaches and adverse events. They must ensure their organizations can perform exceptionally well in the face of political, environmental, competitive, regulatory and technology changes. In this illustration, we outline the five key areas in which business, IT and security teams need to 'get on the same page' in developing an integrated view of risk and resilience.

DEVELOPED BY

OCEG®

1 BUSINESS OPERATIONS

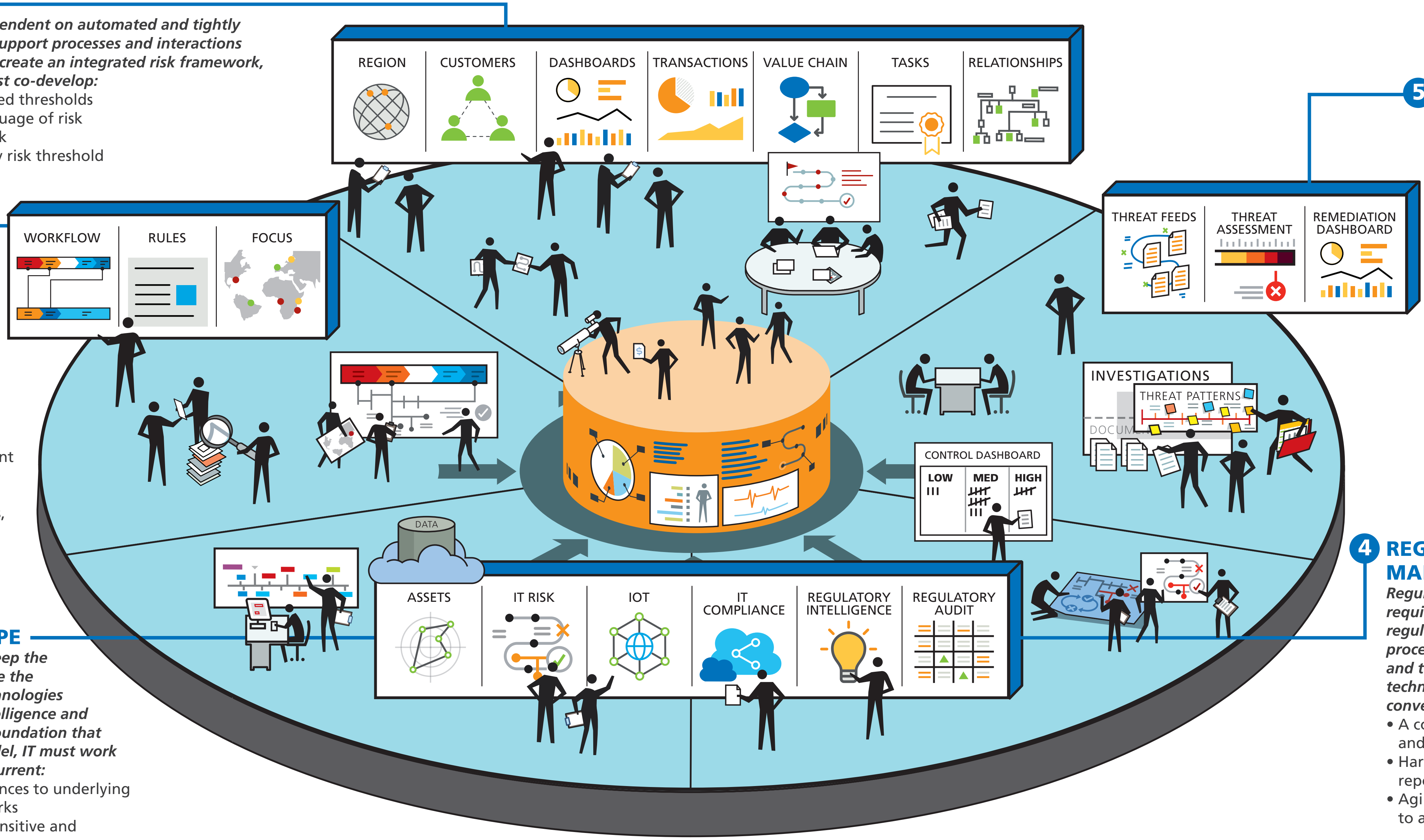
Business Operations are highly dependent on automated and tightly integrated technology systems to support processes and interactions with 3rd parties and customers. To create an integrated risk framework, Business, IT and Security teams must co-develop:

- Risk Appetite translated to required thresholds
- Common, organization-wide language of risk supporting an analytics framework
- Contextual Intelligence to identify risk threshold breaches and respond with agility

2 CHANGE MANAGEMENT

Business Resilience must be continuously optimized with planning and preparedness to support business operations and the technology environment. Business, IT and Security teams must vigilantly align on:

- Business Impact Analysis with appropriate RTO and RPOs
- High state of readiness with current plans and rigorous testing
- Maximum responsiveness from employees, suppliers, third parties, customers and government agencies



3 TECHNOLOGY LANDSCAPE

Technology Landscape – IT must 'keep the lights' on and continuously improve the landscape while adopting new technologies such as cloud, mobile, Artificial Intelligence and the Internet of Things. To lay the foundation that will support an integrated risk model, IT must work with business to define and keep current:

- Business process maps with references to underlying technology apps, data and networks
- Best Practices in GRC to protect sensitive and regulated information
- Agile processes to adopt emerging technologies

4 REGULATORY COMPLIANCE MANAGEMENT

Regulatory ¬Compliance Management requires proactive analysis of regulatory requirements to business processes, information, third parties and the extended global and local technology environment. Teams must converge on:

- A common understanding of global and local regulatory obligations
- Harmonized control testing and reporting across all regulations
- Agile regulatory management process to assess the impact of change

5 THREAT INTELLIGENCE MANAGEMENT

Threat Intelligence and Response must continuously evolve to adequately respond to risks and vulnerabilities across the IT landscape. IT and Security teams must align on:

- Future-Ready assessments that leverage continuous monitoring of threat feeds
- Threat Intelligence and analysis supported by machine learning and AI
- Breach Readiness aligned with crisis and incident management

COMMON DRIVERS FOR BUSINESS, IT AND SECURITY RISK TEAMS

Business, IT and Security Risk teams benefit from an integrated risk program that allows them to:

- Rapidly respond to risk with insight and agility to support better decisions
- Gain visibility and context into the most urgent business risks across operations
- Effectively serve finance, legal, corporate compliance, vendor management and operations
- Manage a broad and dynamic landscape of 3rd parties, suppliers and customers

Contact info@oceg.org for comments, reprints or licensing requests for additional resources visit www.oceg.org/resources

GRC Illustrated

DEVELOPED BY OCEG®

What are the elements of privacy risk management and compliance?

Organizations that handle personal information face increasingly complex challenges to effectively manage privacy risk and compliance. The impact of these challenges covers the entire information life cycle.

An Effective Data Privacy Management Capability

An effective data privacy management has defined, auditable processes and policies that are consistent with the Fair Information Practice Principles. Key components include:

- Collection Need Assessment
- Use Risk Assessment
- Privacy Policy with Pre-Approval, Access and Use Provisions
- Transfer Policy and Procedures
- Security and Disposal Policy and Procedures
- Assessment and Monitoring
- Effective Technology Support

Fair Information Practice Principles

Issued by the U.S. Federal Trade Commission

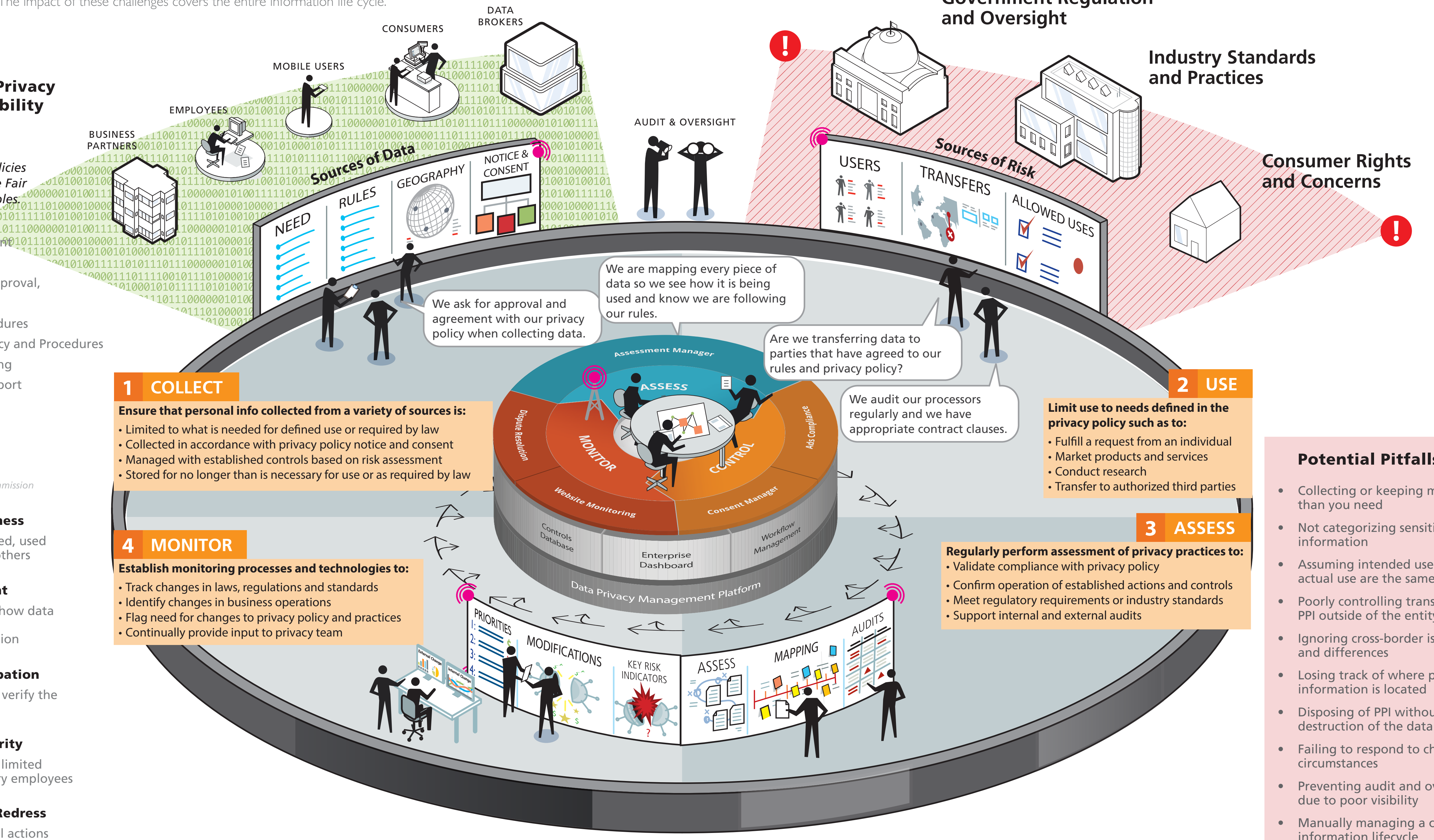
1. Notice/Awareness
How data is collected, used and transfered to others

2. Choice/Consent
Options to control how data is used beyond the immediate transaction

3. Access/Participation
Ability to view and verify the data collected

4. Integrity/Security
Securing data with limited access for neccessary employees

5. Enforcement/Redress
Self-regulation, civil actions and government enforcement


CONSUMERS
DATA BROKERS
MOBILE USERS
EMPLOYEES
BUSINESS PARTNERS
Sources of Data
NEED
RULES
GEOGRAPHY
NOTICE & CONSENT
AUDIT & OVERSIGHT
Government Regulation and Oversight
Industry Standards and Practices
Consumer Rights and Concerns
Sources of Risk
USERS
TRANSFERS
ALLOWED USES
We ask for approval and agreement with our privacy policy when collecting data.
We are mapping every piece of data so we see how it is being used and know we are following our rules.
Are we transferring data to parties that have agreed to our rules and privacy policy?
We audit our processors regularly and we have appropriate contract clauses.
Assessment Manager
ASSESS
Dispute Resolution
MONITOR
CONTROL
Ads Compliance
Website Monitoring
Consent Manager
Controls Database
Enterprise Dashboard
Workflow Management
Data Privacy Management Platform
PRIORITIES
MODIFICATIONS
KEY RISK INDICATORS
ASSESS
MAPPING
AUDITS

1 COLLECT

Ensure that personal info collected from a variety of sources is:

- Limited to what is needed for defined use or required by law
- Collected in accordance with privacy policy notice and consent
- Managed with established controls based on risk assessment
- Stored for no longer than is necessary for use or as required by law

2 USE

Limit use to needs defined in the privacy policy such as to:

- Fulfill a request from an individual
- Market products and services
- Conduct research
- Transfer to authorized third parties

3 ASSESS

Regularly perform assessment of privacy practices to:

- Validate compliance with privacy policy
- Confirm operation of established actions and controls
- Meet regulatory requirements or industry standards
- Support internal and external audits

4 MONITOR

Establish monitoring processes and technologies to:

- Track changes in laws, regulations and standards
- Identify changes in business operations
- Flag need for changes to privacy policy and practices
- Continually provide input to privacy team

Potential Pitfalls

- Collecting or keeping more than you need
- Not categorizing sensitive information
- Assuming intended use and actual use are the same
- Poorly controlling transfer of PPI outside of the entity
- Ignoring cross-border issues and differences
- Losing track of where private information is located
- Disposing of PPI without full destruction of the data
- Failing to respond to changed circumstances
- Preventing audit and oversight due to poor visibility
- Manually managing a complex information lifecycle

contact info@oceg.org for comments, reprints or licensing requests

How to implement and enforce policy compliance

This illustration advises on how to implement and enforce policies in the organization. A well-written policy that is not adhered to can become a liability and increase exposure to the organization. Policies that are complied with become assets that help the organization direct behavior, reliably achieve objectives, reduce uncertainty, act with integrity, and enhance corporate culture.

DESIGNED BY: OCEG® grc2020

SPONSORED BY: MetaCompliance®

INVESTIGATIONS & REPORTING

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

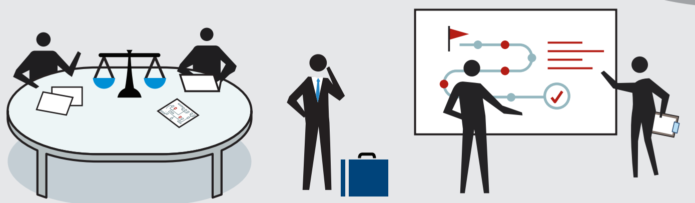
COMPLIANCE

The compliance department provides oversight and accountability by ensuring that policies are adhered to, from monitoring for actions of non-compliance, and overseeing action plans to correct them.

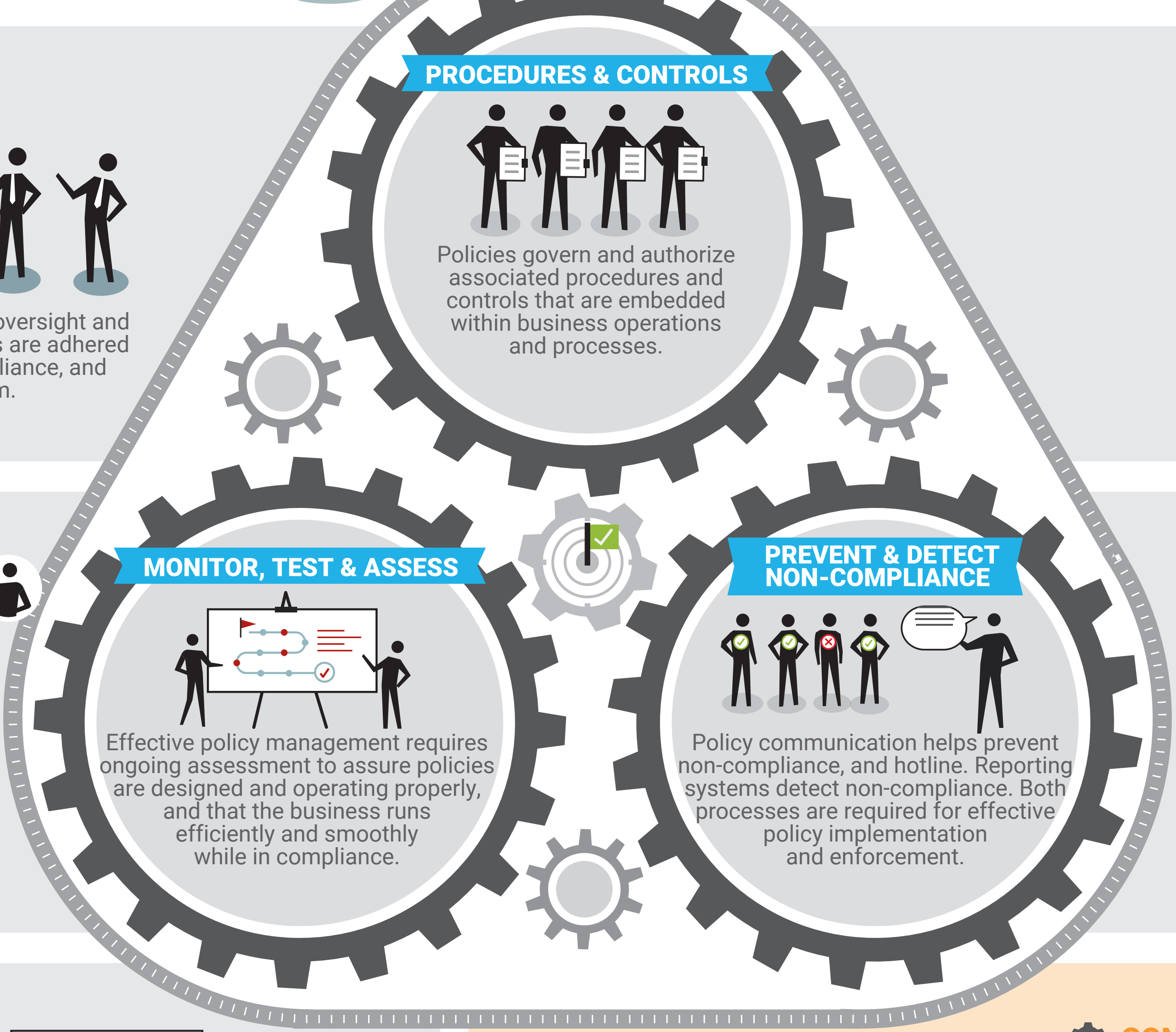
HUMAN RESOURCES

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

LEGAL



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



PROCEDURES & CONTROLS

Policies govern and authorize associated procedures and controls that are embedded within business operations and processes.

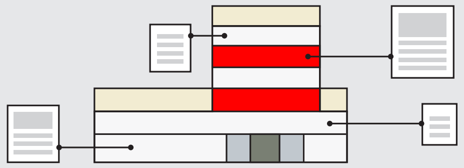
MONITOR, TEST & ASSESS

Effective policy management requires ongoing assessment to assure policies are designed and operating properly, and that the business runs efficiently and smoothly while in compliance.

PREVENT & DETECT NON-COMPLIANCE

Policy communication helps prevent non-compliance, and hotline. Reporting systems detect non-compliance. Both processes are required for effective policy implementation and enforcement.

INTERNAL AUDIT



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

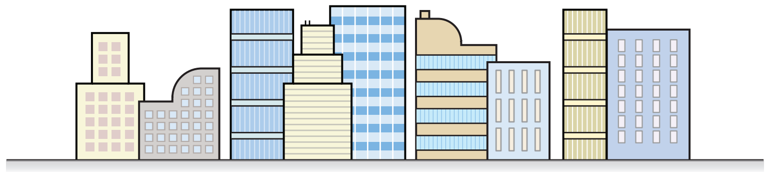
OPERATIONS

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

MANAGE EXCEPTIONS

- 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.

EXTENDED ENTERPRISE CONSIDERATIONS

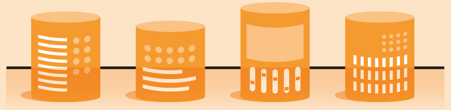


- The organization does not stop with traditional brick and mortar - the modern organization is a web of business relationships that cross boundaries.
- Clearly define which policies cross business relationships and ensure compliance is covered in contracts.
- Periodically communicate policies across all business relationships and provide training where needed.
- Require business partners to undergo a minimum annual self-assessment process to attest to their compliance status to governing policies, procedures, and controls.
- The organization should have defined processes to exercise right to audit clauses/inspections to validate compliance to policies and contracts in extended business relationships.

THE BENEFITS OF TECHNOLOGY

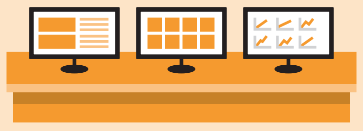
REPOSITORY

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.



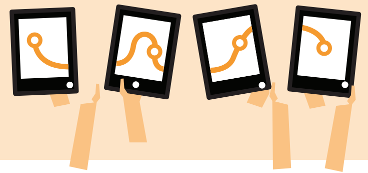
CONSISTENCY

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.



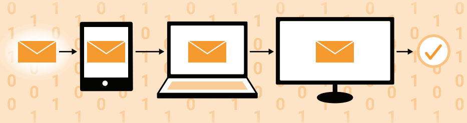
ACCOUNTABILITY

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.



Conducting Defensible Supply Chain Due Diligence

Having the right supply chain can be a competitive advantage but failing to control supplier risk can have devastating effects. With thousands of suppliers in play, due diligence requires more than a shallow review of readily available information at the time of onboarding. Real risk-based supply chain management demands ongoing due diligence with advanced methods and readily auditable supplier records. Records must not only enable oversight of each supplier but also should support reports and views of risk across the entire supply chain to enable true governance.

DEVELOPED BY
OCEG®

WITH CONTRIBUTIONS FROM
ARAVO
REFINITIV

1. Start with Effective Governance

Establish a supply chain governing body to set "tone at the top", oversee critical risk identification and drive establishment of a unified data management capability.

RISKS TO THE BUSINESS

IDENTIFY HIGH LEVEL RISKS

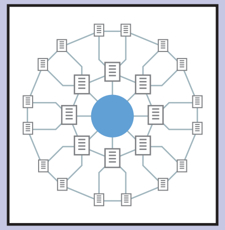
Evaluate each area of risk in relation to business operations, products and services to identify those with the highest potential impact. Consider each type of risk and limitations established by leadership and by legislation/regulation. Determine level of importance for addressing each risk or risk category.

POLICY DEVELOPMENT

- Supplier selection
- Risk assessment
- Continuous monitoring
- Supplier reporting
- Templates

ESTABLISH POLICIES AND TEMPLATES

Use the organization's established guidance for development of policies including assignment of roles for authoring and management, templates and specific limitations for supplier use established by leadership. Provide policies for each stage of the due diligence process.



DEFINE DATA INTEGRATION

Provide guidance and resources to enable integration of internal and external data sources for use in due diligence, single system of record for each supplier, reporting and audit trail of due diligence process.

2. Apply Advanced Methods of Data Collection and Analysis

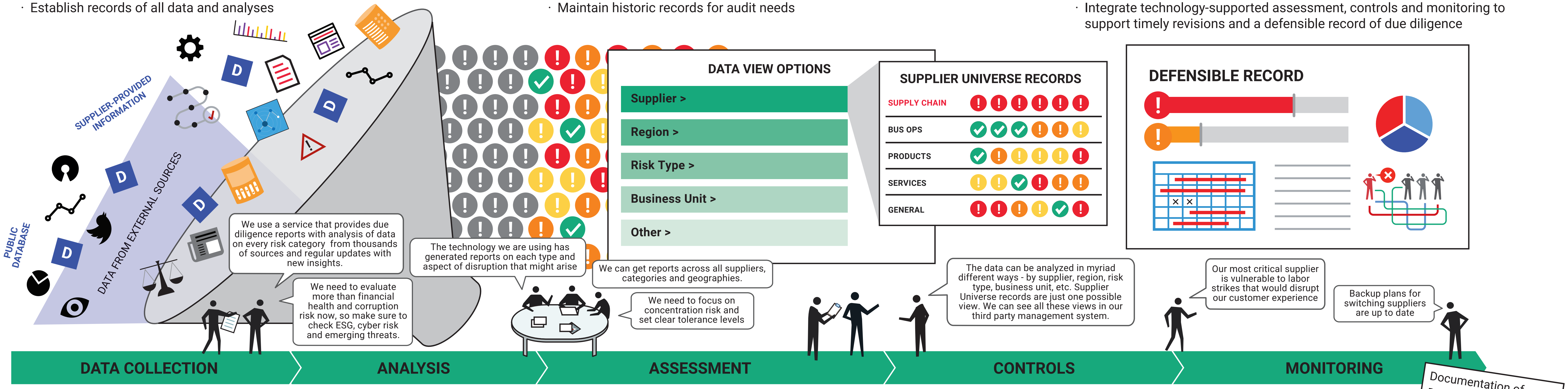
- Use information providers that provide consolidated data
- Ensure timely updates with ongoing monitoring
- Assess and monitor each supplier's risk
- Establish records of all data and analyses

3. Maintain Supplier Records and Audit Trail

- Identify categories of information for the supplier record
- Update record as changes are identified through data monitoring
- Enable views for different needs per record and across supplier universe
- Maintain historic records for audit needs

4. Manage Integrated Assessment, Controls and Monitoring

- Conduct risk assessments with scope based on initial analysis of need
- Apply controls based on identified risk levels for each supplier
- Revisit the process when changes in supplier information are flagged
- Integrate technology-supported assessment, controls and monitoring to support timely revisions and a defensible record of due diligence



DATA VIEW OPTIONS

- Supplier >
- Region >
- Risk Type >
- Business Unit >
- Other >

SUPPLIER UNIVERSE RECORDS

SUPPLY CHAIN	🔴	🔴	🔴	🔴	🔴	🔴
BUS OPS	✓	✓	✓	🟠	🟠	🟡
PRODUCTS	✓	🟠	🟡	🟡	🟡	🔴
SERVICES	🟡	🟡	✓	🔴	🟠	🟠
GENERAL	🔴	🔴	🟠	🟡	✓	🔴

We use a service that provides due diligence reports with analysis of data on every risk category from thousands of sources and regular updates with new insights.

We need to evaluate more than financial health and corruption risk now, so make sure to check ESG, cyber risk and emerging threats.

The technology we are using has generated reports on each type and aspect of disruption that might arise

We can get reports across all suppliers, categories and geographies.

We need to focus on concentration risk and set clear tolerance levels

The data can be analyzed in myriad different ways - by supplier, region, risk type, business unit, etc. Supplier Universe records are just one possible view. We can see all these views in our third party management system.

Our most critical supplier is vulnerable to labor strikes that would disrupt our customer experience

Backup plans for switching suppliers are up to date

Today, the best supplier due diligence is managed in a technology-driven system supported by AI and automation. *Data collection, risk analysis and assessment is ongoing. Controls are established and monitored and are revisited as risk assessments change because of new data. When issues are detected, corrective action plans are triggered.*

Monitoring Key Risks

Each vendor may have different risks but these are common across supply chains. Each risk requires monitoring of different data sources. Here are a few examples you may not have thought about:

POLITICAL INSTABILITY

- Regime changes
- Political upheaval
- Uncertainty in government policy
- Civil unrest

OPERATIONAL DISRUPTION

- Extreme weather events
- Concentration risks
- Border disruptions
- Resource shortages

CYBER ATTACKS

- Network security
- DNS Health
- Patching cadence
- Data breaches

BRIBERY AND CORRUPTION

- Sanctions
- Enforcement Actions
- Politically Exposed Persons (PEPs)
- Beneficial Ownership

MODERN SLAVERY/TRAFFICKING

- Product/materials
- Location
- Labor practices
- Enforcement actions

FINANCIAL HEALTH

- Profitability
- Operating Efficiency
- Z-score
- Liquidity