2017-05

GRC Content & Intelligence Solutions

2017 Market Landscape

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Terms & Conditions . . .

- ✓ **GRC 20/20 Research Briefings are copyrighted and protected material**. Content cannot be reused or distributed without written permission from GRC 20/20 Research, LLC.

- ✓ ***GRC Advisor Enterprise Subscribers*** get access to live and recorded Research Briefings for all employees for INTERNAL use only through the GRC 20/20 website. If they wish to have a recording to host internally there is a fee for this.

- ✓ ***GRC Basic Subscribers*** pay for either **individual** access to specific GRC 20/20 Research Briefings. ***Individual access*** is for the individual only and slides or login are not to be shared with others or viewed as a group.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Two Things to Note . . .

Complimentary Inquiry

- Organizations evaluating or considering GRC solutions are free to ask GRC 20/20 on our understanding and comparison of solutions in the market to meet your GRC requirements.
- Inquiries are single focused questions that can be answered in under 30 minutes.
- Complimentary inquiry is only available to organizations evaluating or considering GRC solutions for their internal use.

RFP Development & Support

- GRC 20/20 has an extensive library of RFP requirements across a range of GRC capability areas presented in this presentation.
- GRC 20/20 can be engaged in RFP development and support projects to streamline your process, gain perspectives learned from other organizations, and to keep solution providers honest in their responses.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

The Official Definition of GRC . . .

> GRC is the integrated collection of capabilities that enable an organization to:
>
> G) reliably achieve objectives
>
> R) while addressing uncertainty and
>
> C) acting with integrity.

SOURCE: OCEG GRC Capability Model

Governance, Risk Management & Compliance in Context

Governance

Governance sets direction and strategy for the organization to reliably achieve objectives. Governance sets the context for risk management, without context risk management fails.

Risk Management

Risk management seeks to manage and understand uncertainty by assessing and monitoring risk within context to take action on risk through acceptance, avoidance, mitigation, or transfer.

Compliance

Compliance aims to see that the organization acts with integrity in fulfilling its regulatory, contractual, and self-imposed obligations and values. Compliance follows through on risk treatment plans to assure that risk is being managed within limits and controls are in place and functioning.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

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

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

The Chaos of Interconnectedness

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

The Organization Has to be Able to See . . .

- ❑ **The Tree.** The individual area of risk
- ❑ **The Forest.** The interconnectedness of risk

LICENSED SUBSCRIBER USE
DO NOT DISTRIBUTE

The integration of GRC intelligence and content sources is critical to enterprise GRC strategies of the future. This involves the delivery of content from knowledge/content providers through GRC solutions to rapidly assess changing regulations, risks, industry and geopolitical events.

Content is tagged so it can be properly routed to the right subject matter expert to establish workflow and tasks for review and analysis. Standardized formats for measuring business impact and review of existing processes, policies and controls can take place. This integration of actionable content with GRC technology delivers on GRC maturity through achievement of risk and regulatory intelligence.

LICENCED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

GRC Intelligence: Integration of Actionable Content

Drivers & Trends: Enterprise GRC

Drivers

1 Constant Change	Exponential growth in regulatory, risk and business change is making scattered GRC processes and information constantly behind and exposing the organization.
2 Growing Relationships	The growing array of 3rd party relationships with increased regulatory and risk exposure is bearing down on organizations to include in GRC strategies.
3 Scattered Information & Platforms	Many organizations still find they are encumbered by silos of information that is disconnected, and often have several disconnected GRC platforms in different areas.
4 Growing Beyond Initial GRC Platforms	Those that have implemented a GRC platform in the past decade are often finding that the solution is out of date and cumbersome to use when compared to the new generation of solutions.
5 Need for External GRC Content	There is growing demand and need for the integration of external content and intelligence feeds into the GRC architecture.

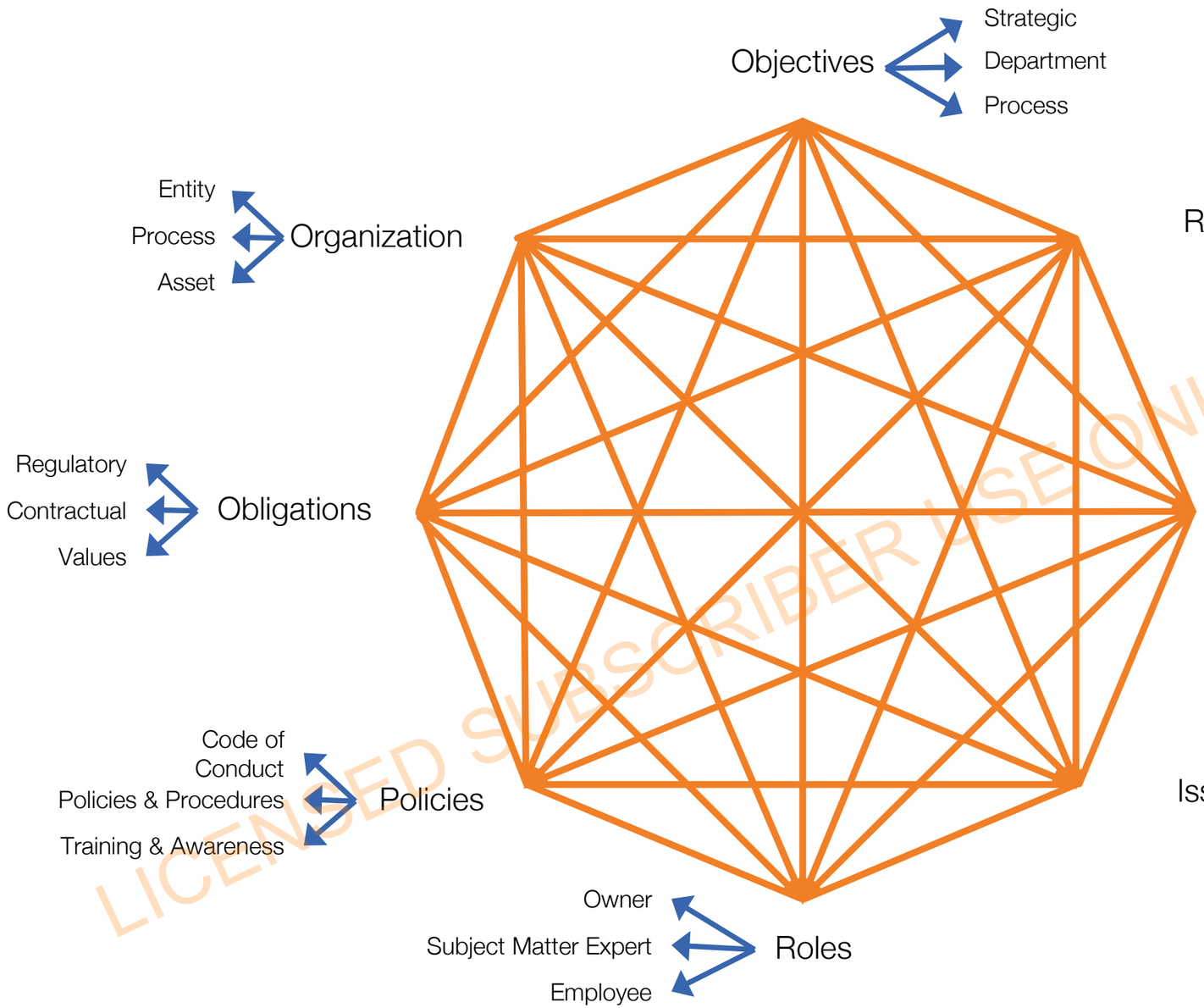
Trends

1 GRC Architecture	No platform does everything. Organizations are looking toward an information and technology architecture that integrates GRC, though there often is one central core platform.
2 Integration	Enterprise GRC Platforms are no longer self-contained solutions to manage GRC workflow and tasks, they require strong integration capabilities into a range of business systems.
3 Best of Breed Where it Makes Sense	In a GRC architecture approach, organizations are looking toward a common hub and core for Enterprise GRC but allow for best of breed solutions where they make sense.
4 Business Process Modeling	There is growing demand in RFPs for GRC solutions to have business process modeling capabilities to visually layout and document how business processes function in a GRC context.
5 GRC Mobility & Engagement	Enterprise GRC is no longer for the back-office, but needs to be intuitive and easy to use for the front-office. New releases are showing improved user interface and mobility options.

LICENSED SUBSCRIBER USE ONLY. DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC 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.

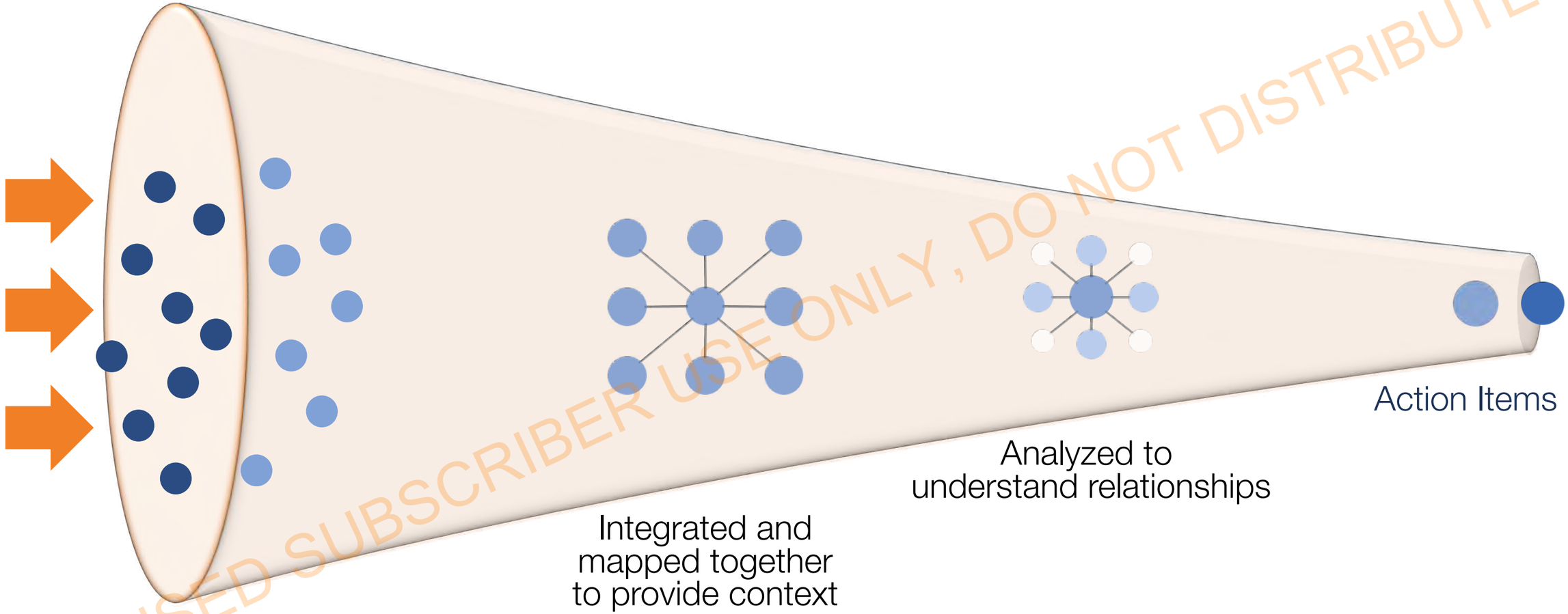
reduced costs

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

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

360° GRC Contextual Analytics & Intelligence Capabilities



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

The GRC Market: Technology, Information,& Professional Services

GRC Technology Solutions

845+ technology solution providers that offer solutions related to GRC

GRC Intelligence & Content Solutions

140+ providers with 425+ content/intelligence solutions across a range of GRC areas

GRC Professional Services Solutions

1,000+ professional service firms offering services related to GRC

LICENSED SUBSCRIBER USE ONLY - DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Technology Market Segment Definitions

GRC Technology Segment	Description
Enterprise GRC	Capability to manage an integrated architecture across multiple GRC areas in a structured strategy, process, information and technology architecture.
Audit Management	Capability to manage audit planning, staff, documentation, execution/field work, findings, reporting, and analytics..
Automated Control	Capability to automate the detection and enforcement of internal controls in business processes, systems, records, transactions, documents, and information.
Business Continuity Management	Capability to manage, maintain, and test continuity and disaster plans, and implement these plans expected and unexpected disruptions to all areas of operation.
Compliance Management	Capability to manage an overall compliance program, document and manage change to obligations, assess compliance, remediate non-compliance, and report.
Environmental Management	Capability to document, monitor, assess, analyze, record, and report on environmental activities and compliance.
Health & Safety Management	Capability to manage, document, monitor, assess, report, and address incidents related to the health and safety of the workforce and workplace,
Internal Control Management	Capability to manage, define, document, map, monitor, test, assess, and report on internal controls of the organization.
IT GRC Management	Capability to govern IT in context of business objectives and manage IT process, technology, and information risk and compliance.
Issue Reporting & Management	Capability to notify on issues and incidents and manage, document, resolve, and report on the range of complaints, issues, incidents, events, investigations, and cases.
Legal Management	Capability to manage, monitor, and report on the organization's legal operations, processes, matters, risks, and activities.
Physical Security Management	Capability to manage risk and losses to individuals and physical assets, facilities, inventory, and other property..
Policy & Training Management	Capability to mange the development, approval, distribution, communication, forms, maintenance, and records of policies, procedures and related awareness activities.
Quality Management	Capability to manage, assess, record, benchmark, and track activity, issues, failures, recalls, and improvement related to product and service quality.
Risk Management	Capability to identify, assess, measure, treat, manage, monitor, and report on risks to objectives, divisions, departments, processes, assets, and projects.
Strategy & Performance Management	Capability to govern, define, and manage strategic, financial, and operational objectives and related performance and risk activities.
Third Party Management	Capability to govern, manage, and monitor the array of 3rd party relationships in the enterprise, particularly risk and compliance challenges these relationships bring.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Intelligence Market Segment Definitions

GRC Intelligence Segment	Description
Audit Content & Intelligence	Content providers of audit templates, forms, and intelligence.
Business Continuity Content & Intelligence	Content providers of business continuity templates, forms, and intelligence
Compliance Content & Intelligence	Content providers of regulatory libraries, regulatory intelligence, compliance forms and templates.
Environmental Content & Intelligence	Content providers of environmental intelligence, forms, and templates.
Health & Safety Content & Intelligence	Content providers of health & safety libraries, content, forms, and templates.
Internal Control Content & Intelligence	Content providers of internal control libraries, forms, and templates.
IT GRC Content & Intelligence	Content providers of IT GRC/security control libraries, threat and vulnerability intelligence, forms, and templates.
Legal Content & Intelligence	Content providers of legal databases, libraries, legislation tracking, forms, templates, and spend intelligence.
Policy & Training Content & Intelligence	Content providers of policy libraries, training courses, and policy and training related content, forms, and templates.
Risk Management Content & Intelligence	Content providers of risk intelligence feeds, risk libraries, loss data, risk forms, and templates.
Third Party Management Content & Intelligence	Content providers of third party management intelligence, due diligence, watch lists, negative news, ratings, monitoring, forms, and templates
Issue Specific Content & Intelligence	Content providers of content and intelligence related to specific issues, regulations, and risks (e.g., bribery/corruption, conflict minerals, labor)
Industry Specific Content & Intelligence	Content providers of industry specific content and intelligence.

LICENSED SUBSCRIBER USE ONLY. DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

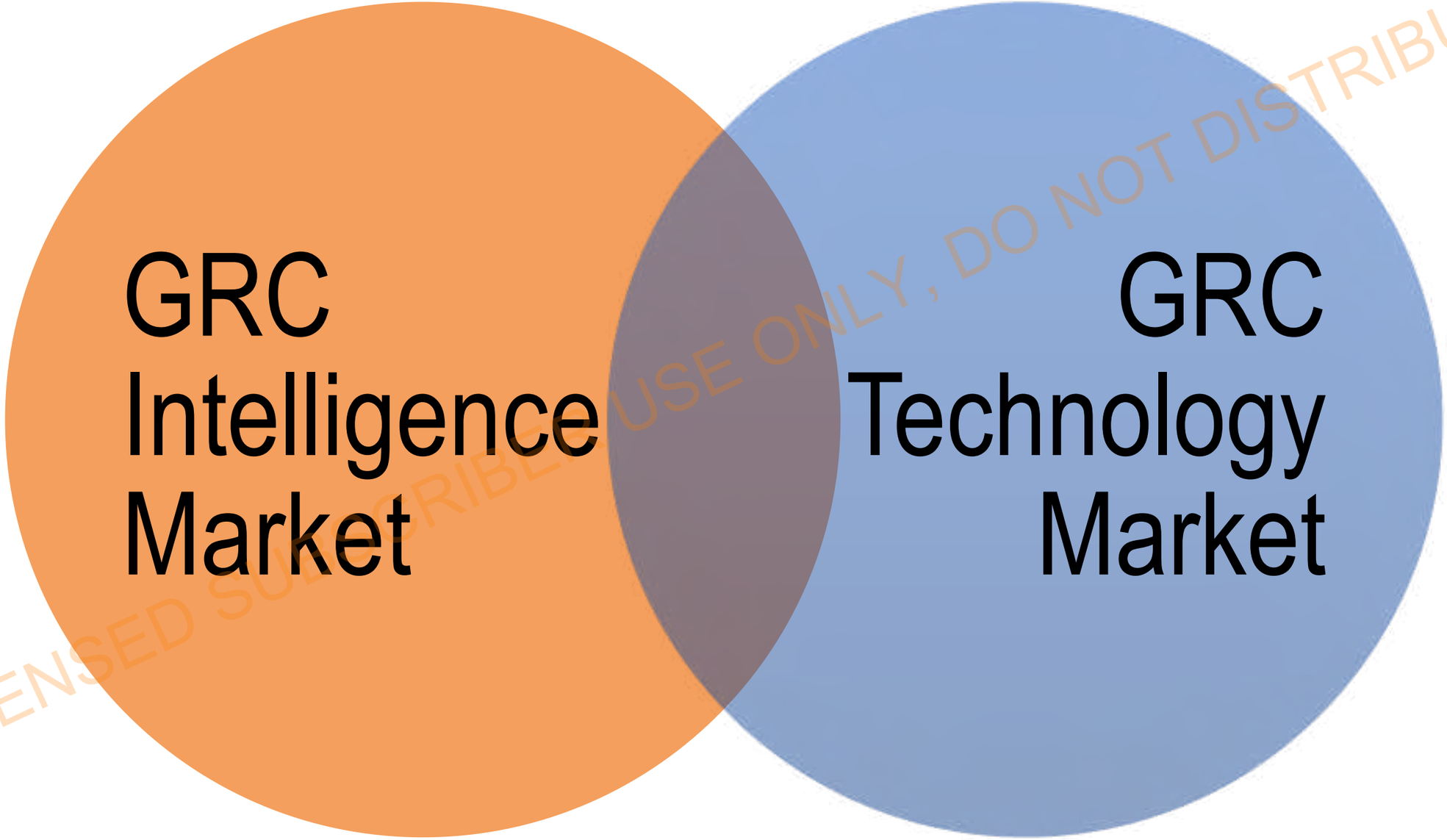
GRC Professional Services Market Segment Definitions

GRC Professional Services Segment	Description
Audit Services	Services focused on external audits as well as internal audit staffing and management.
Consulting Services	Services focused on GRC related management and strategy consulting.
Legal Services	Services focused on legal matters and advice related to GRC.
Outsourced Services	Services that are outsourced such as specific GRC functions, monitoring, certification, etc.
Systems Integration Services	Services focused on implementation, build out, and development of GRC related information and technology architecture and solutions.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

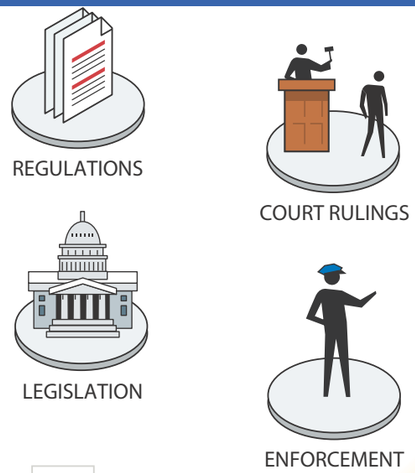
GRC Intelligence & Technology Market Overlap



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

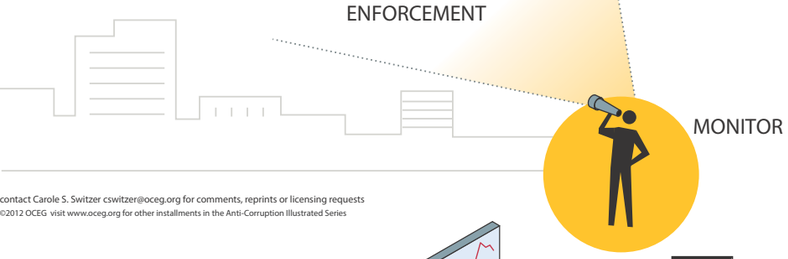
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Change is the Greatest Challenge Impacting GRC



Regulatory/Legal Change

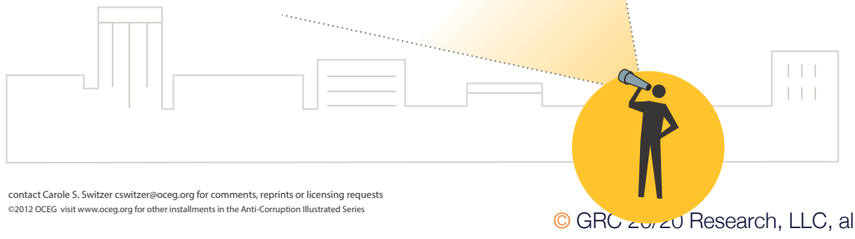
Monitor change in the legal and regulatory environment to determine how pending legislation, court decisions, new/changing regulations, and enforcement actions affect current and needed policies.



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

External Risk Change

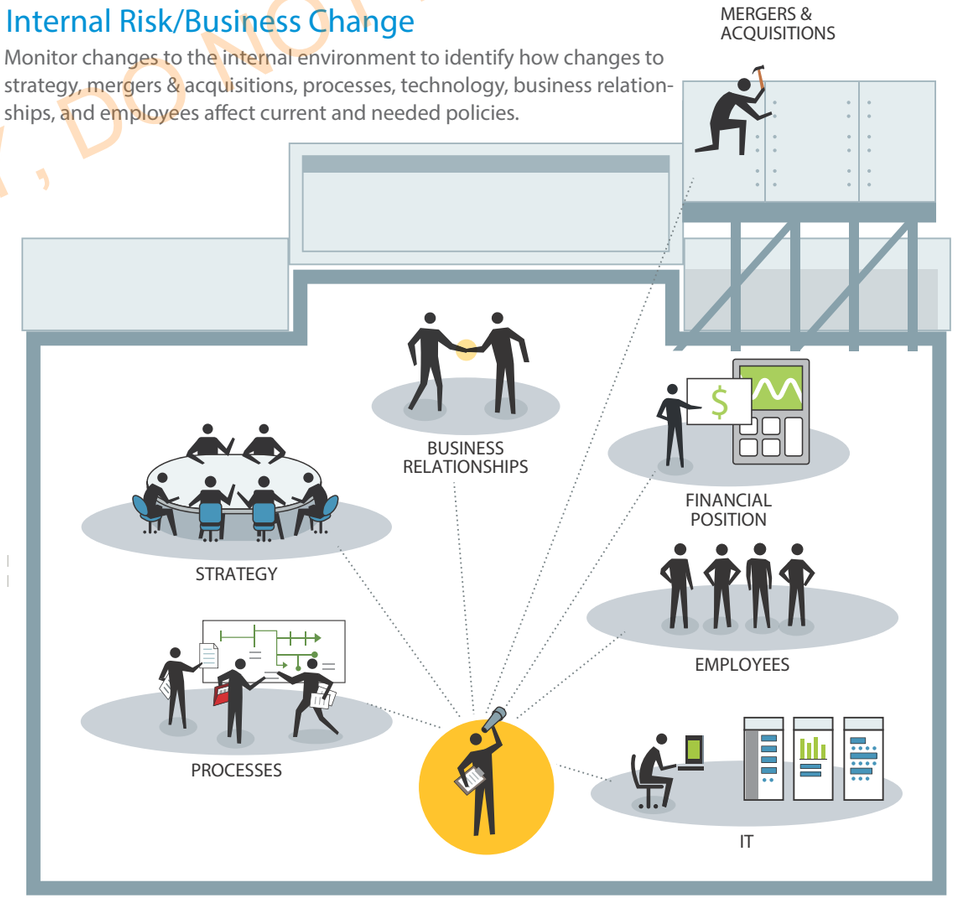
Monitor change in the external risk environment to determine how uncertainty in economic, geo-political, environmental, industry, societal, and market forces affect current and needed policies.



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

Internal Risk/Business Change

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



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

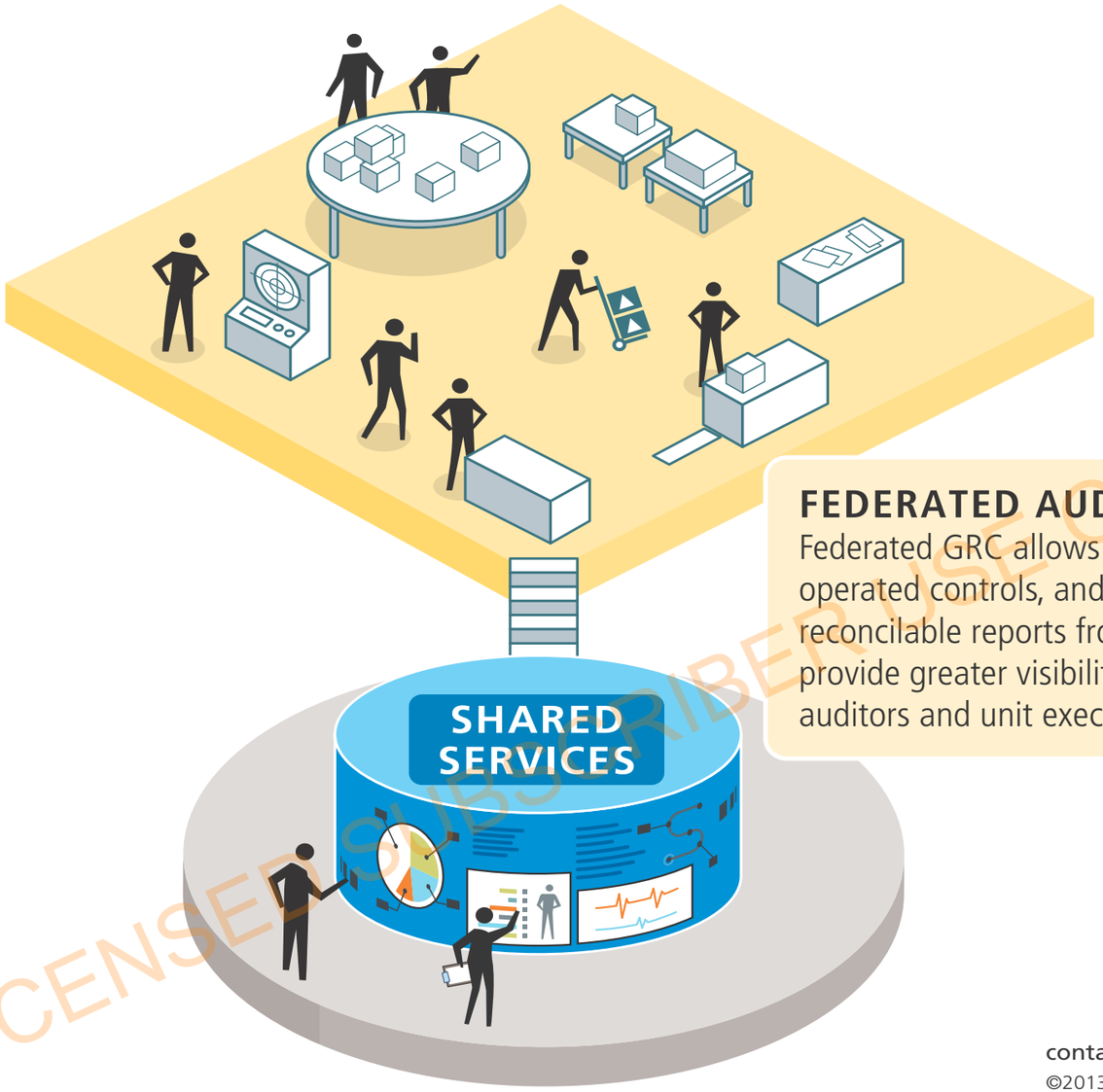
LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Audit Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Federated Audit Management



FEDERATED AUDIT MANAGEMENT

Federated GRC allows auditors to provide greater assurance of properly designed and operated controls, and insight into business performance, through consistent and reconcilable reports from operational and field audits. A federated model strives to provide greater visibility into emerging risks by enhancing communication between auditors and unit executives.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

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

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Enabling Efficient, Effective & Agile Audit Management

ANALYZE & ACT ON FINDINGS

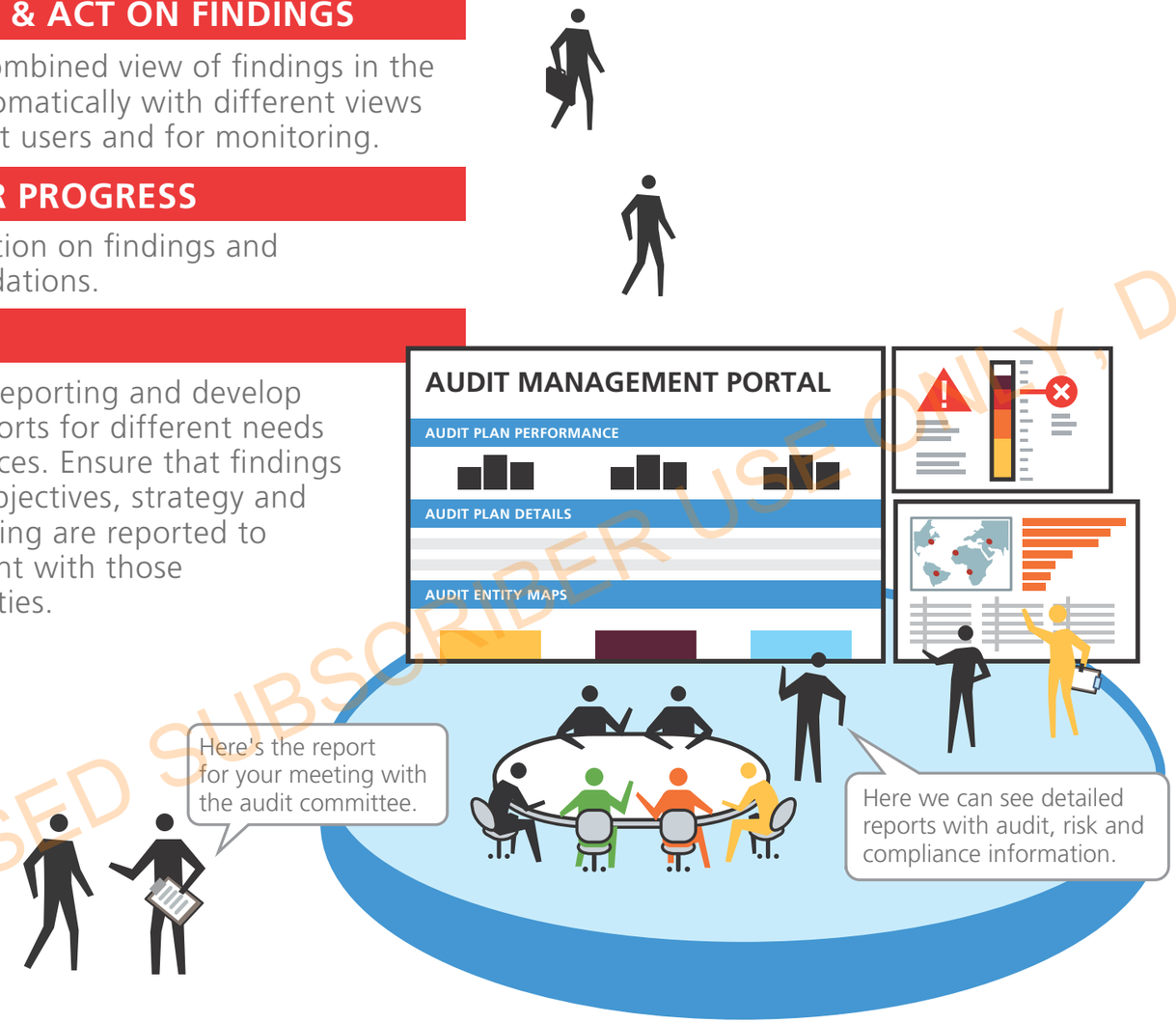
Establish combined view of findings in the system automatically with different views for different users and for monitoring.

MONITOR PROGRESS

Monitor action on findings and recommendations.

REPORT

Automate reporting and develop custom reports for different needs and audiences. Ensure that findings affecting objectives, strategy and audit planning are reported to management with those responsibilities.



COMMON MISTAKES

- Establishing a purely rotational approach for every area of audit
- Equally distributing available resources without prioritizing
- Failing to consider scheduling burdens or to create a unified audit plan
- Designing an audit that does not tie to specific objectives and related risks
- Auditing what you know, not what is important based on risk assessments
- Limiting audits based on available resources rather than asking for more

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

contact info@oceg.org for comments, reprints or licensing requests
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com ©2014 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

GRC Technology Market: Audit Management & Analytic

Audit Management & Analytic

- *Audit Management Platforms*
- *Audit Analytic Solutions*
- *Miscellaneous Audit Tools*

Audit Management & Analytic technologies are used by auditors to manage and perform audits.

- **Audit management solutions** are used to manage audit cycles – this includes audit planning, resource scheduling/calendaring, work paper management, audit execution, audit process management, and audit reporting. They also support a risk-based approach to audit planning to prioritize audits based on the risk to the business.
- **Audit analytic solutions** utilize data analytics and and continuous auditing (automated control enforcement & monitoring) to extract insights from operational and financial data to assist in audits and provide assurance.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Audit Management Content & Intelligence Providers

- ✓ AuditNet
- ✓ Protiviti Knowledge Leader

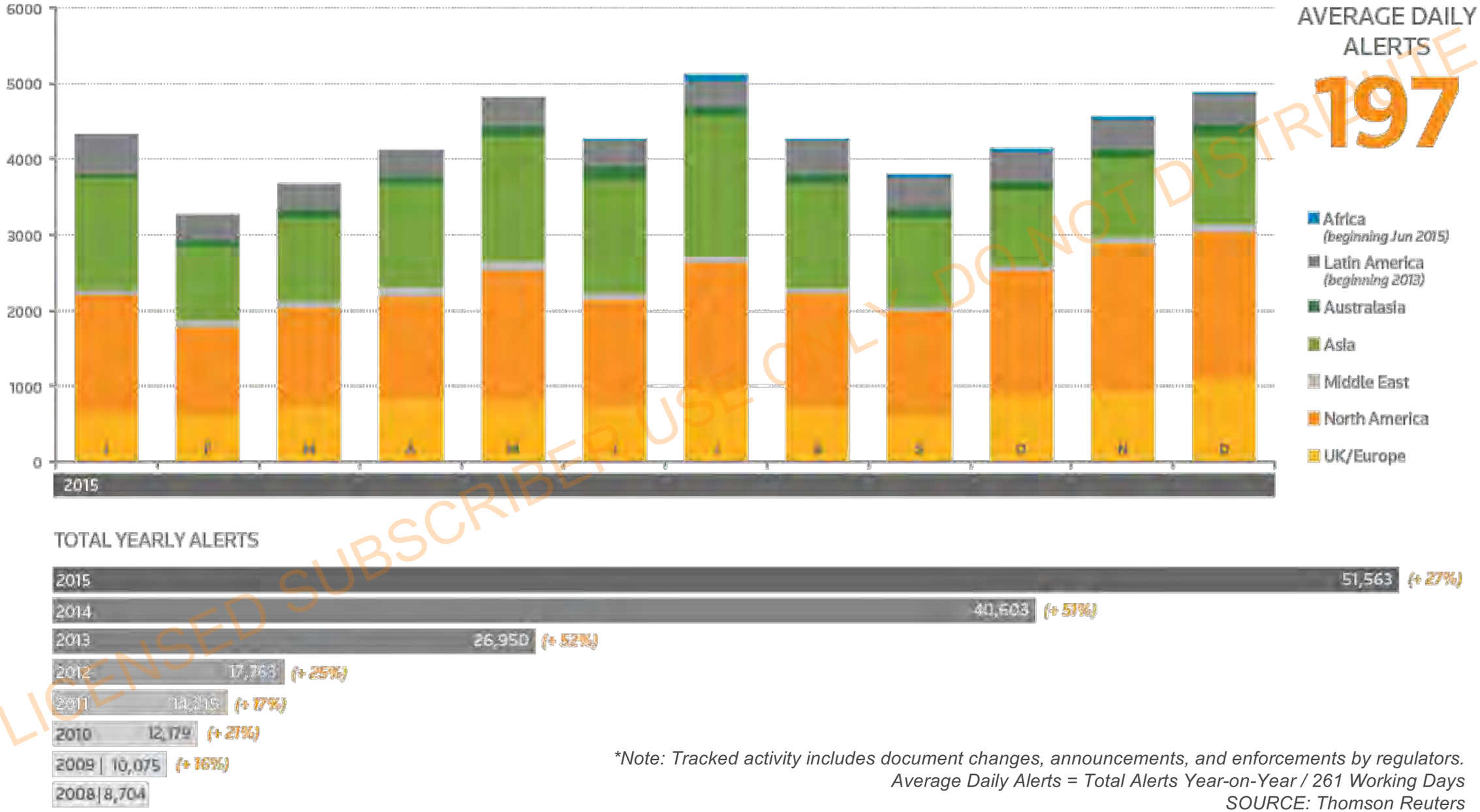
LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Compliance Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Regulatory Activity in Financial Services 2008 to 2015

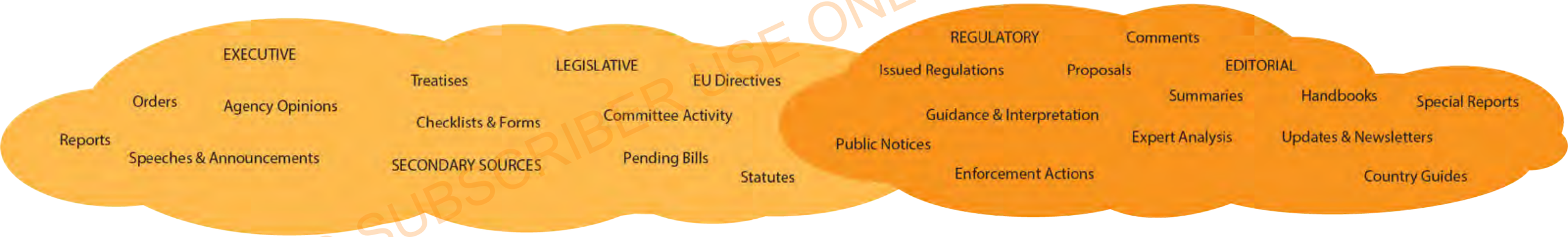


**Note: Tracked activity includes document changes, announcements, and enforcements by regulators.*
Average Daily Alerts = Total Alerts Year-on-Year / 261 Working Days
SOURCE: Thomson Reuters

LICENSED SUBSCRIBER USE ONLY. DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Regulatory Intelligence Content Types

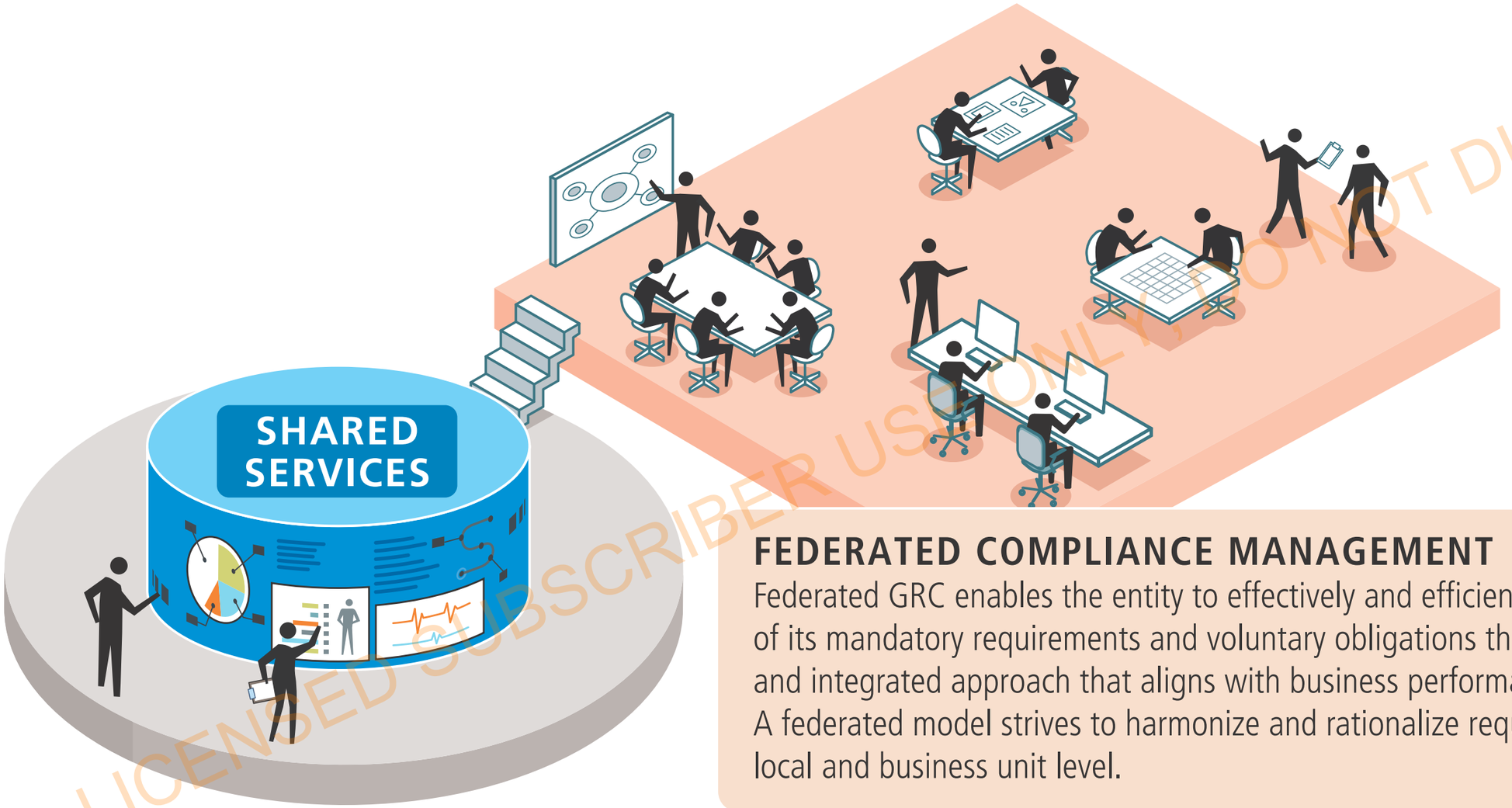


Contact info@oceg.org for comments, reprints or licensing requests ©2017 OCEG for additional resources visit www.oceg.org/resources

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Federated Compliance Management



FEDERATED COMPLIANCE MANAGEMENT

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

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

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

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

USSC Organizational Sentencing Guidelines: 7 Elements of Effective Compliance

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

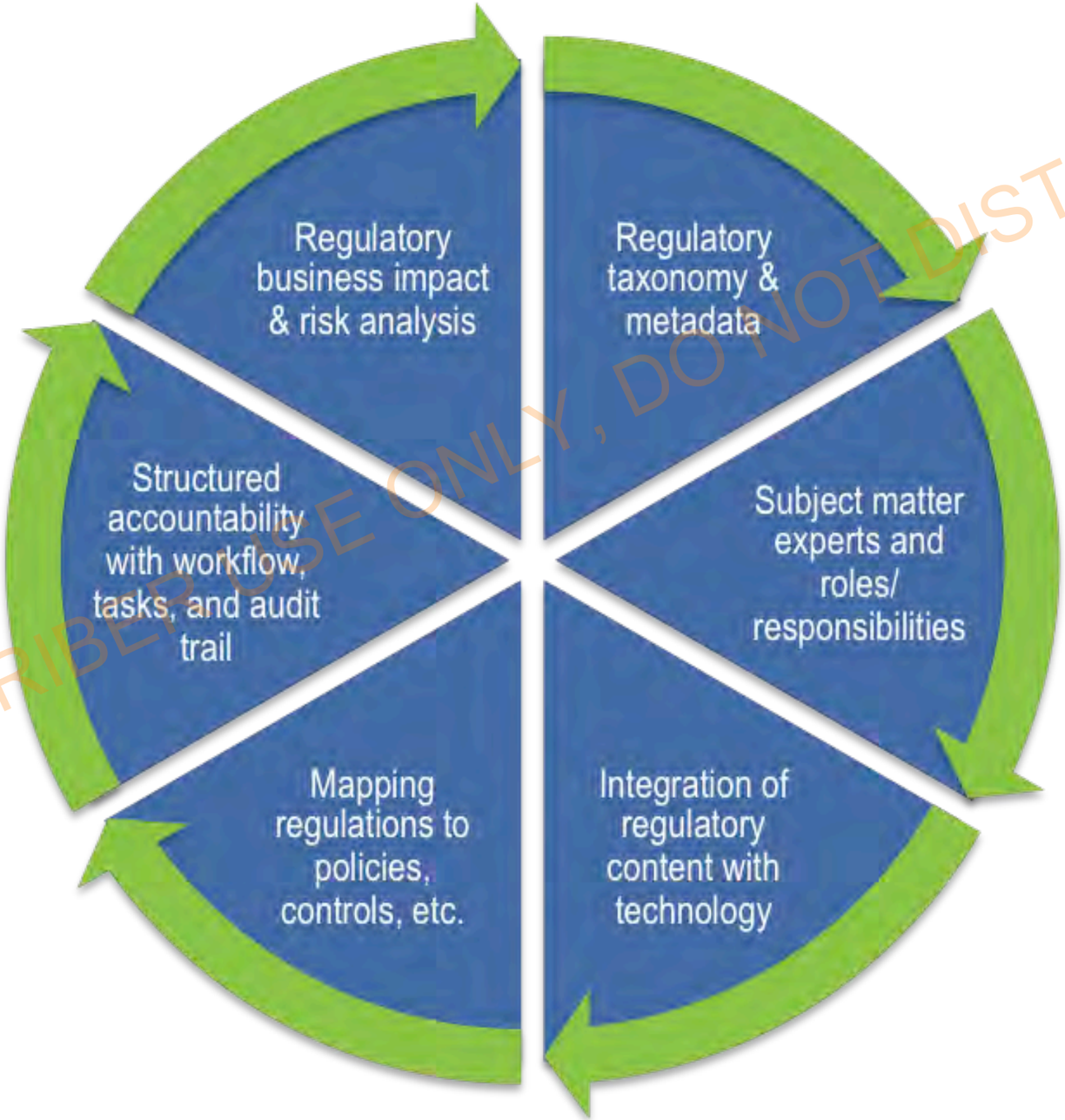
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Elements of a Regulatory Change Management Process

Regulatory Taxonomy

Regulatory Content

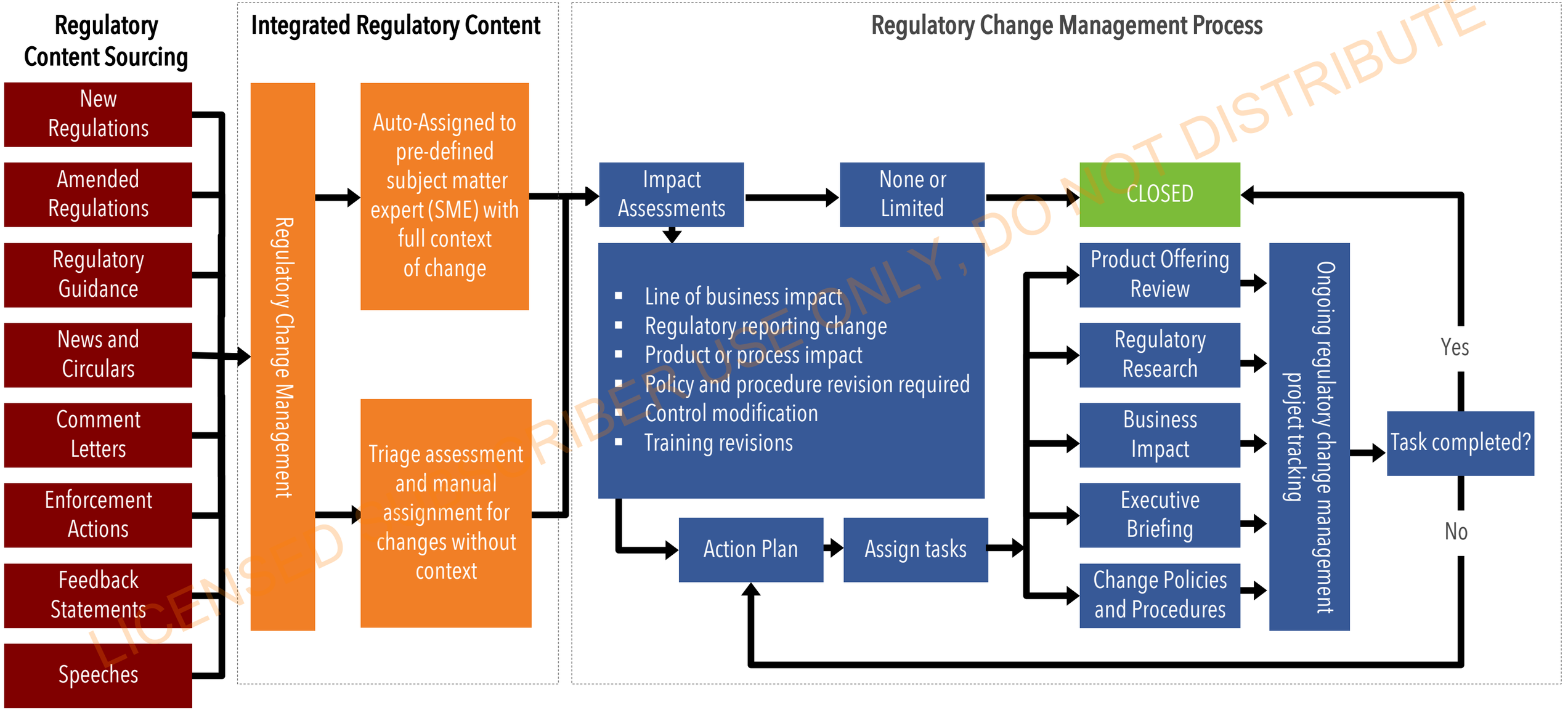
Technology Enablement



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

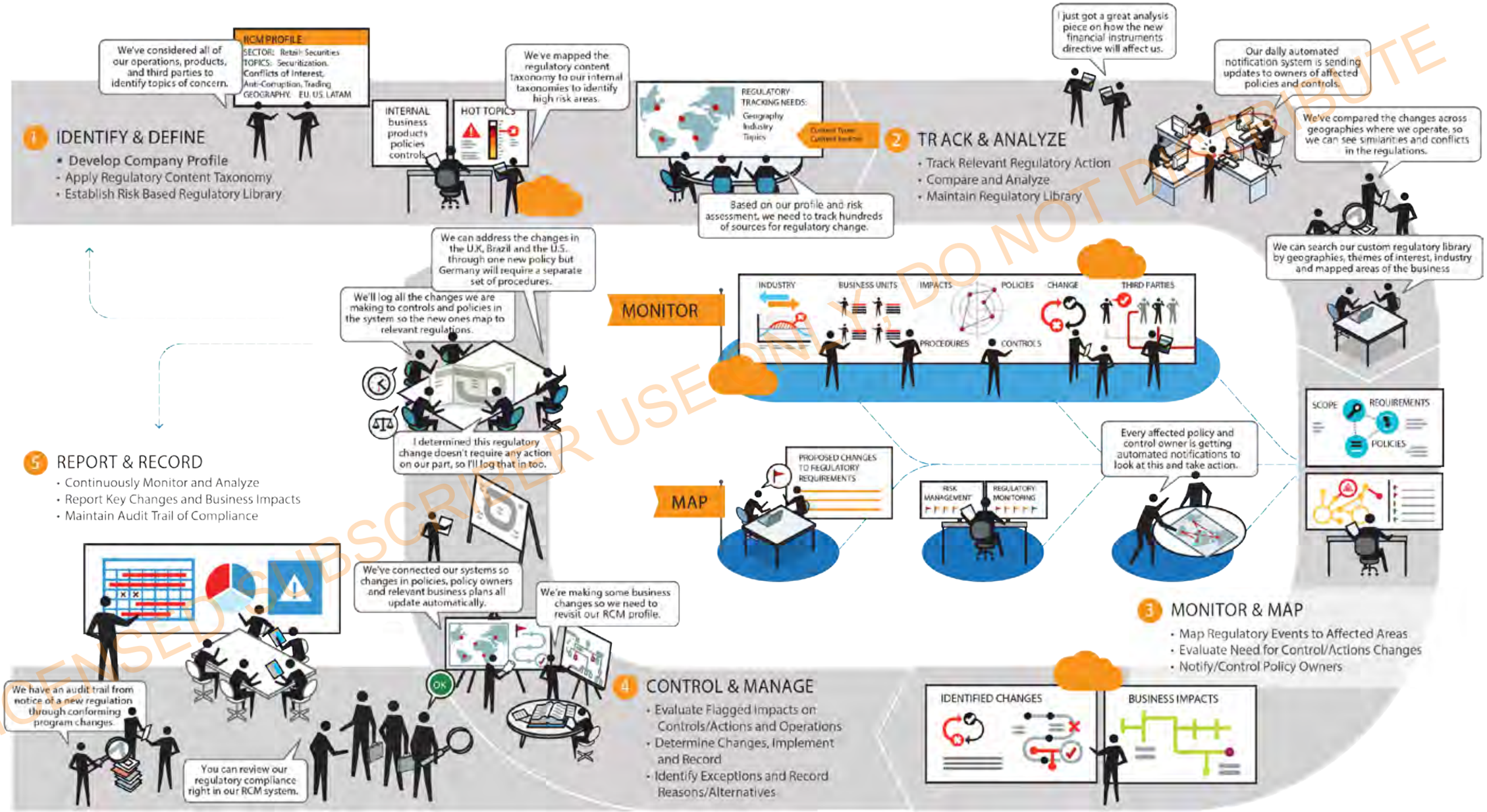
Conduct Analysis and Manage Regulatory Change Process



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Regulatory Change Management Process



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Contact info@oceg.org for comments, reprints or licensing requests ©2017 OCEG for additional resources visit www.oceg.org/resources

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Regulatory Change Management Success Factors

RCM CRITICAL SUCCESS FACTORS

- Regulatory content taxonomy organized by geography, sector, content type and defined themes
- Mapping of regulatory content taxonomy to internal taxonomies for organization structure, products, policies and controls
- Real time tracking of thousands of varied sources and types of content
- Flagging of proposed and final regulatory changes
- Risk profiling of the organization
- Expert analysis for impact based on company profile
- Automatic notification to affected policy/control and business process owners
- Tracking of responding policy/control changes
- Audit trail throughout process
- Enhanced reporting capabilities

LICENSED SUBSCRIBER USE ONLY DO NOT DISTRIBUTE

Contact info@oceg.org for comments, reprints or licensing requests ©2017 OCEG for additional resources visit www.oceg.org/resources
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Technology Market: Compliance Management

- Compliance Management
  - *Compliance Management Platforms*
  - *Compliance Assessment Solutions*
  - *Regulatory Change Management Solutions*
  - *Stakeholder & Regulatory Interaction Solutions*
  - *Compliance Forms, Reporting & Filing Solutions*
  - *Social Responsibility & Reporting Solutions*
  - *Miscellaneous Compliance Tools*

Compliance Management technologies support the overall coordination of legal, regulatory, contractual, values, ethics, and corporate obligations and responsibilities with associated compliance documentation, assessments, tasks, and records. This includes the ability to monitor, document, and manage changes to the regulatory environment and other obligations; to document all obligations of the organization; to perform compliance assessments against obligations; manage regulator and stakeholder interactions on compliance; and report on the state of compliance to regulators and stakeholders.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Compliance Management Content & Intelligence Providers

- ✓ AllRegs
- ✓ Avior
- ✓ Bloomberg BNA
- ✓ C2C Smart Compliance
- ✓ Clear Market Practices
- ✓ Compliance Mentor
- ✓ Compliance Online
- ✓ Compliance Publishing Corporation
- ✓ Deloitte RCCS
- ✓ Dow Jones
- ✓ Fenergo
- ✓ Greenlight Technologies
- ✓ GreenPoint Law & Compliance
- ✓ IBM Promontory
- ✓ JWG
- ✓ LexisNexis
- ✓ Littler
- ✓ Propylon
- ✓ Protiviti Knowledge Leader
- ✓ Radar Risk
- ✓ RDC – Regulatory Data Corp
- ✓ Reg-Room
- ✓ RegEd
- ✓ RegRadar
- ✓ RegScan
- ✓ Regulations.gov
- ✓ Regulatory Consulting Limited
- ✓ StateScape
- ✓ StateSide Associates
- ✓ Thomson Reuters

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Compliance Management Content & Intelligence Providers, continued

- ✓ TRUSTe
- ✓ Unified Compliance Framework
- ✓ Wolters Kluwer Financial Services
- ✓ Wolters Kluwer Law & Business

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Environmental Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

GRC Technology Market: Environmental Management

Environmental Management

- *Environmental Management Platforms*
- *Air, Water, Waste Management Solutions*
- *Chemical Management Solutions*
- *Energy & Carbon Management Solutions*
- *Land Use & Permit Solutions*
- *Sustainability & Environmental Reporting Solutions*
- *Miscellaneous Environmental Tools*

Environmental Management technologies help monitor, analyze, record, and report organizational activity focused on compliance with environmental laws and regulations, related corporate policy related to managing environmental controls and conditions, and assessing the environmental impact of the corporation's operations, strategies, and plans.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Environmental Content & Intelligence Providers

- ✓ Bloomberg BNA
- ✓ Citation Technologies
- ✓ EcoDesk
- ✓ Enhesa
- ✓ Integrated Compliance Information System
- ✓ RegScan
- ✓ Specialty Technical Publications
- ✓ Thompson Information Services

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Health & Safety Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

GRC Technology Market: Health & Safety

Health & Safety Management

- *Health & Safety Management Platforms*
- *Health & Safety Forms & Document Solutions*
- *Health & Safety Incident Solutions*
- *Occupational Safety Solutions*
- *Hazard Analysis Solutions*
- *Chemical Management & Labeling Solutions*
- *Miscellaneous Health & Safety Tools*

Health & Safety technologies manage the regulatory and policy-based guidelines and processes for protecting and reporting on the workforce, workplace, resources-under-management and external environment impacted by an organization's activities.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Health & Safety Content & Intelligence Providers

- ✓ 3E
- ✓ Bloomberg BNA
- ✓ Citation Technologies
- ✓ Compliance Publishing Corporation
- ✓ Enhesa
- ✓ iJet
- ✓ MSDSonline./Velocity EH&S
- ✓ RegRadar
- ✓ RegScan
- ✓ Specialty Technical Publications

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Internal Control Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Categories of Internal Controls

Proactive
Actions and Controls

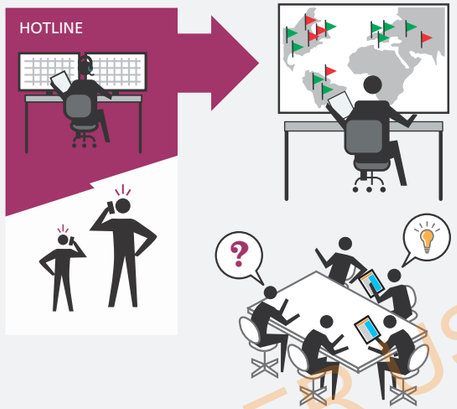
Being proactive means taking action and establishing controls to prevent undesired conduct conditions and encourage or identify what is desired. This requires having policies, training, communication, incentives and strong analysis to manage conditions in performance, risk and compliance.

KEY STEPS

1. Define and establish policies and policy management structure, including processes for exceptions, and define role-based procedures to follow
2. Design and deliver appropriate training and education opportunities through multiple channels and modes of delivery, using different methodologies and risk based curriculum
3. Communicate about risk decision-making guidance and expectations in a determined flow through multiple channels
4. Monitor key indicators and ongoing operational information to ensure issues are resolved and processes and controls are adjusted as necessary to align with risk profiles and remediation plans

Detective
Actions and Controls

Finding out about desirable and undesirable conduct or conditions in a timely fashion is as important as proactively driving what you want. Discovering opportunities for risk taking, as well as identifying downside risk, is critical to achieving superior performance. Systems, both digital and human, that detect both internal and external anomalies are critical to success.



KEY STEPS

1. Define and establish pathways for individuals to push reports of concerns or information about threats, undesirable conduct or incidents, and passing along information about opportunities.
2. Use multiple channels to pull both internal and external information to support early detection of threats, improper conduct or conditions, and possible opportunities.
3. Use available technology systems for detecting variances, anomalies, breaches, inappropriate controls, and early warnings about possible violations of policies/procedures or control avoidance.
4. Evaluate information, forward opportunities and issues for resolution, and adjust controls as necessary.

Responsive
Actions and Controls

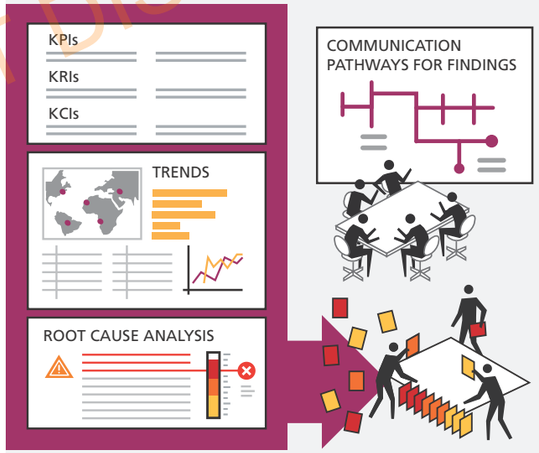
Action must be taken on analyses of information received from proactive and detective controls. Sometimes this is process driven; other times automated technology responses (such as access control change) are established. Ensure processes and controls are established to investigate and manage incidents, launch consideration of opportunities or risk reassessment, and manage change.

KEY STEPS

1. Define and implement pathways for triage of identified issues,concerns and opportunities, using established procedures and supportive technology, in some cases enabling automated resolution of issues.
2. Establish investigation and issue resolution procedures, identifying key personnel and tools to be used in conducting processes and maintaining an audit trail of resolution of each issue.
3. Ensure timely reporting to internal and external stakeholders when required or appropriate.
4. Evaluate information received throughout resolution processes and use to adjust established actions and controls as necessary.

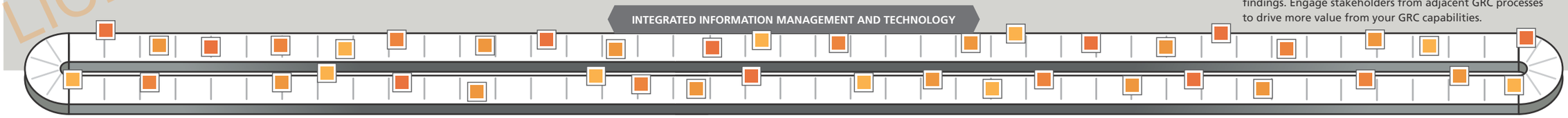
Analytics
Throughout

Analytics tied to performance indicators unleash the power of unstructured and structured information. Use analytics to prioritize and analyze trends, identify root causes of problems, predict behaviors and conditions, and gain insight for risk-based decisions. Leverage analytics to see potential impacts and become more agile in meeting performance objectives.



KEY STEPS

1. Establish Key Indicators for Performance, Risk and Compliance tied to strategic objectives and appetites; develop processes for collecting data and analyzing results.
2. Design information architecture to support the analytics framework, using reliable internal and external datasets to provide contextually relevant insights that leadership can act upon.
3. Continually evolve the analytic framework as it begins to yield richer information on trends, emerging threats, vulnerabilities and opportunities, predicted conditions and root cause analysis across a broader and more granular array of domains and topics.
4. Collaborate with the board, senior management and business operators to ensure two way communication and action on findings. Engage stakeholders from adjacent GRC processes to drive more value from your GRC capabilities.



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Types of Internal Controls

By factoring automated solutions into the up-front design of event, risk & control monitoring processes, companies are able to identify and monitor key controls more cost-effectively. Automated controls and monitoring systems build controls into daily business processes. Standardized rules and reports streamline internal and external audits and allow faster implementation of changes to policies and procedures. Once validated, independent monitoring systems can be used as a baseline for subsequent audits.

FINANCIAL CONTROLS

Financial controls protect the integrity and accuracy of financial statements which shareholders rely on and ensure that transactions are entered in the general ledger are authorized and legitimate. For this reason they are typically a major focus of most audits. Some of the most common challenges include revenue recognition, accruals, procurement, payroll management, capitalization, and inter-company eliminations. Automated controls can flag sensitive, unauthorized and unusual transactions as they happen so that errors do not unexpectedly make their way into financial statements.

OPERATIONAL CONTROLS

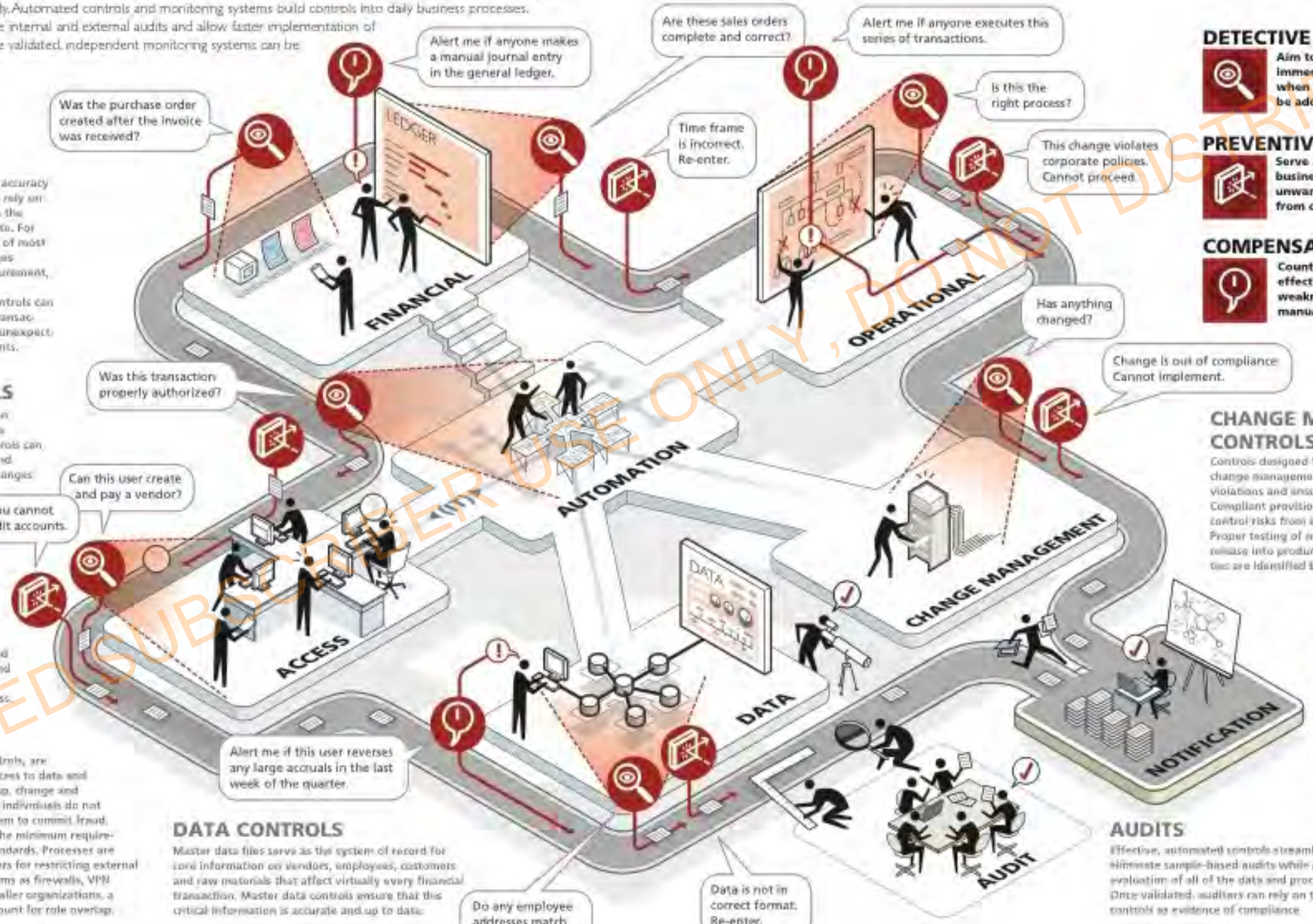
Controls in place throughout the organization ensure that business processes and corporate policies are being followed. Automated controls can provide visibility into process breakdowns and identify improvements such as training or changes to processes and policy.

GENERAL COMPUTING CONTROLS

General computing controls include controls over basic system settings, password policies, system development and deployment, incident management, data backup and recovery, third party vendor management and physical security controls that are critical to the integrity of the financial reporting process.

ACCESS CONTROLS

Access controls, or segregation of duties controls, are implemented to identify roles and related access to data and programs. Controls ensure that account set-up, change and termination standards are followed and that individuals do not possess access rights which would enable them to commit fraud. Controls may also be established regarding the minimum requirements for unique user ID's and password standards. Processes are monitored to confirm access rights. Parameters for restricting external connectivity to the system via such mechanisms as firewalls, VPN connections, and dial-up are reviewed. In smaller organizations, a compensating control may be in place to account for role overlap.



DETECTIVE

Aim to detect problems and immediately alert control owners when exceptions occur so they can be addressed or remediated.

PREVENTIVE

Serve as brakes on day-to-day business processes by preventing unwanted activity and actions from occurring.

COMPENSATING

Counterbalance the potential effect of an internal control weakness, usually through a manual process or review.

CHANGE MANAGEMENT CONTROLS

Controls designed to automate and document change management processes prevent new control violations and ensure proper audit trails exist. Compliant provisioning processes prevent access control risks from entering application environments. Proper testing of new applications prior to their release into production ensures security vulnerabilities are identified before they lead to new risks.

NOTIFICATION

Continuous monitoring & alerts ensure that control violations are identified immediately so that control owners can take action immediately and eliminate the need for time-consuming investigations that take place when exceptions are identified weeks or months after the fact.

DATA CONTROLS

Master data files serve as the system of record for core information on vendors, employees, customers and raw materials that affect virtually every financial transaction. Master data controls ensure that this critical information is accurate and up to date.

AUDITS

Effective, automated controls streamline the audit process. They eliminate sample-based audits while providing a comprehensive evaluation of all of the data and processes within an organization. Once validated, auditors can rely on the existence of automated controls as evidence of compliance.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Internal Controls & Business Processes

Effective operational controls add value by ensuring that the people, processes and technology which drive the organization's core functions remain aligned. In addition to flagging potential risks as they occur operational controls can identify misalignments that arise from inefficient business processes, poor training, improperly configured IT systems and fraud.

TYPES OF CONTROLS

TRANSACTION LEVEL CONTROLS

As individuals perform day-to-day business processes, key steps and milestones are recorded as transactions and can take the form of entries in the financial system, e-mails or even conversations. Transaction-level controls serve to prevent, identify and/or detect inappropriate, inaccurate or unauthorized transactions.

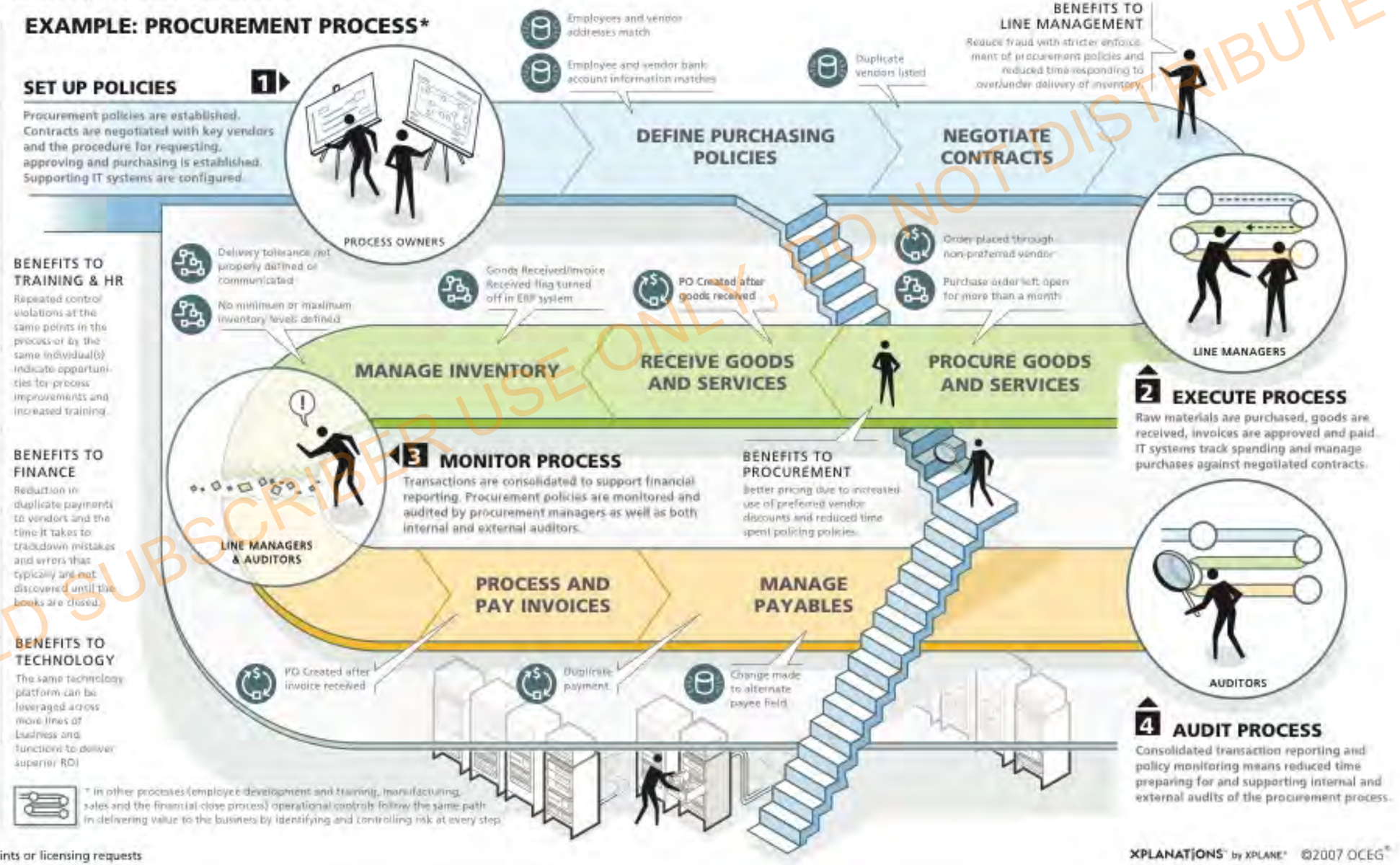
CONFIGURABLE CONTROLS

Business processes and corporate policies are comprised of a prescribed sequence of tasks, events and transactions. Configurable controls ensure that processes are executed as intended. When business processes are highly automated, configurable controls ensure that the workflow which drives key processes is never circumvented.

MASTER DATA CONTROLS

Master data is the core information about an organization's customers, vendors, employees, raw materials and chart of accounts that is fundamental to the execution of mission-critical business processes. Master data controls ensure the integrity of this data so that mistakes are not compounded as transactions reference the data when business processes are executed.

EXAMPLE: PROCUREMENT PROCESS*



* In other processes (employee development and training, manufacturing, sales and the financial close process) operational controls follow the same path in delivering value to the business by identifying and controlling risk at every step.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

COSO Internal Control Management Principles

CONTROL ENVIRONMENT

1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority, and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

RISK ASSESSMENT

6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

CONTROL ACTIVITIES

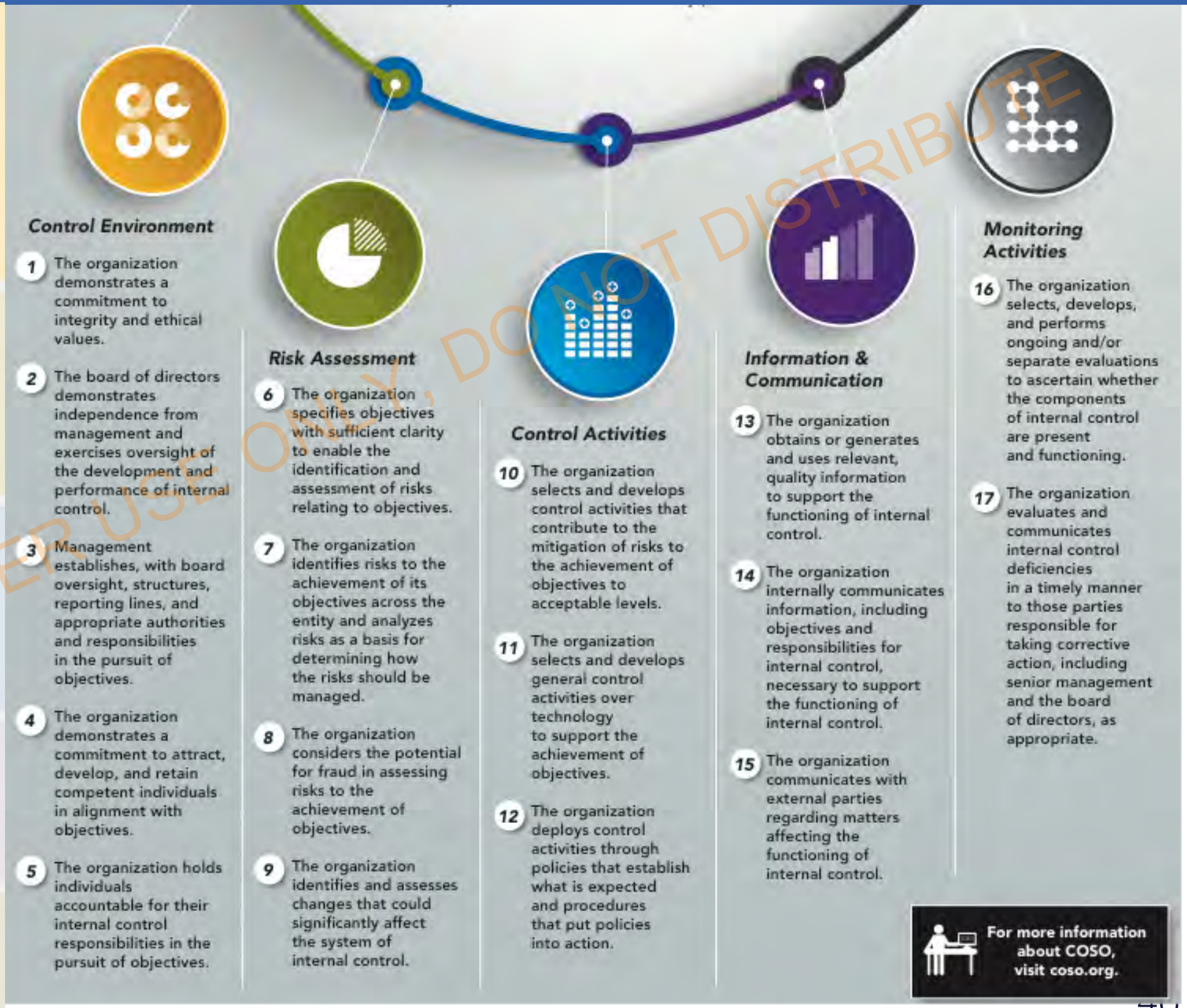
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

INFORMATION & COMMUNICATION

13. Uses relevant information
14. Communicates internally
15. Communicates externally

MONITORING

16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

C 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Internal Control Management

Solution Area Definition

Internal Control Management solutions provide the capability to manage, define, document, map, monitor, test, assess, and report on internal controls of the organization.:

- **Internal control management process** of control identification, assessment, monitoring, and reporting activities, including the overall management of the continual, cyclic, as well as dynamic processes of internal control assessment, analysis, decision making, and response.
- **Internal control monitoring** to alert the organization to conditions that point to control issues, failure and weaknesses.
- **Internal control evaluation** to identify specific causes and evaluate review, simulation, interpretation and projection of impacts on an objectives and assets.

Critical Capabilities

- ❑ Manage overall internal control management program planning, staff, projects/assessments, and activities
- ❑ Support for multiple GRC management frameworks, methodologies, and analysis techniques
- ❑ Set and map objectives and context of internal controls
- ❑ Enable the organization to identify, categorize, map, and show control relationships in registers
- ❑ Enable the organization to gather information and assessment of controls in a variety of approaches
- ❑ Analyze internal control from different perspectives and implement risk treatment
- ❑ Provide monitoring and reporting on internal controls
- ❑ Ability to analyze scenarios and evaluate impacts and events, and revise models as necessary
- ❑ Dashboarding and metrics on internal controls

LICENSED SUBSCRIBER USE ONLY. DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Technology Market: Internal Control Management

Internal Control Management

- *Internal Control Management Platforms*
- *Financial Close & Reporting Solutions*
- *Internal Control Reporting Solutions*
- *Miscellaneous Internal Control Tools*

Internal Control Management technologies provide the ability to define, document, map, monitor, test, assess, and report on controls within the organization, including process and systems documentation. These solutions document internal controls, provide control assessments/self-assessments, and manage this through workflow, tasks, and reporting.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Internal Control Content & Intelligence Providers

- ✓ Avior
- ✓ Bloomberg BNA
- ✓ C2C Smart Compliance
- ✓ Deloitte RCCS
- ✓ Greenlight Technologies
- ✓ LexisNexis
- ✓ Unified Compliance Framework
- ✓ Protiviti Knowledge Leader
- ✓ Risk Spotlight
- ✓ Segmantics

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

IT GRC Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

IT GRC Pressures

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC 20/20 Market Definition of IT GRC . . .

IT GRC Management technologies are used to govern and direct information and technology (IT) strategies in the context of business.

The governance function of IT is the alignment, strategy, and direction of IT to support the business.

A core component of IT GRC Solutions is the ability to manage and monitor security, risk, and compliance across IT systems throughout the organization and across significant business relationships.

Critical Capabilities that Define an IT GRC Platform

Four Critical Capability Areas that Define an IT GRC Platform:

IT Asset Mgmt

Ability to catalog and manage IT physical and logical assets in context of IT and the business.

IT Vulnerability Mgmt

Ability to discover and remediate vulnerabilities and related threats across IT physical and logical assets, often through integration into security tools/architecture.

IT GRC

IT Risk Mgmt

Ability to assess and manage IT risks in context of the business, and present risk exposure to risk owner for acceptance or mitigation.

IT Control Mgmt

Ability to document, assses, and provide an evidence trail of IT controls and compliance to standards and regulations impacting IT and manage compliance in context of changing obilgations and a changing IT environment.

Additional Capabilities Often Are:

- IT Incident Management
- IT Policy Management
- Vendor Risk Management (3rd Party)
- Business Continuity & Disaster Recovery
- IT Audit Management
- Security Architecture Integration

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

The scope of capabilities in the components of IT GRC will depend if your strategy is focused on IT security management or a broader understanding of IT GRC.

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Anatomy of an IT GRC RFP

IT Risk Management Functionality

- ❑ Alignment of IT governance objectives and risks to business
- ❑ Risk methodologies supported
- ❑ Risk registers and taxonomies
- ❑ Risk ownership and acceptance
- ❑ Risk reporting, modeling & analytics
- ❑ Risk assessments
- ❑ Risk workshops
- ❑ Mapping of risks to controls

IT Threat & Vulnerability Management

- ❑ Integration with vulnerability scanners, service desks, threat databases, SIEM, configuration management
- ❑ Alerts & notification
- ❑ Remediation workflow based on risk exposure to business
- ❑ Threat & vulnerability intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

NOTE: these are just a summary of some common elements from GRC 20/20's RFP template containing over 300 requirements for IT GRC Platforms

© GRC 20/20 Research, LLC, all rights reserved, www.GRC202

IT GRC Management Content & Intelligence Providers

- ✓ AlienVault
- ✓ C2C Smart Compliance
- ✓ CERTStation
- ✓ Cloud Security Alliance
- ✓ Cyveillance
- ✓ Dell SecureWorks
- ✓ Exodus Intelligence
- ✓ Exploit Database
- ✓ FireEye
- ✓ IBM X-Force
- ✓ IID ActiveTrust
- ✓ InfoArmor
- ✓ InformationShield
- ✓ iSIGHT Partners
- ✓ McAfee
- ✓ Unified Compliance Framework
- ✓ Open Security Foundation
- ✓ Orange Business Services
- ✓ Recorded Future
- ✓ Risk Based Security
- ✓ SANS Institute
- ✓ Secunia
- ✓ Security Database
- ✓ SecurityGlobal.net
- ✓ SecurityScorecard
- ✓ Sûnnet Beskerming
- ✓ Symantec
- ✓ Threat Intelligence Pty Ltd
- ✓ ThreatConnect

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

IT GRC Management Content & Intelligence Providers, continued

- ✓ ToolsWatch
- ✓ UCF
- ✓ VeriSign

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Legal Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Legal Content & Intelligence Providers

- ✓ Bloomberg BNA
- ✓ LexisNexis
- ✓ StateScape
- ✓ Thomson Reuters
- ✓ Wolters Kluwer Financial Services
- ✓ Wolters Kluwer Law & Business

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

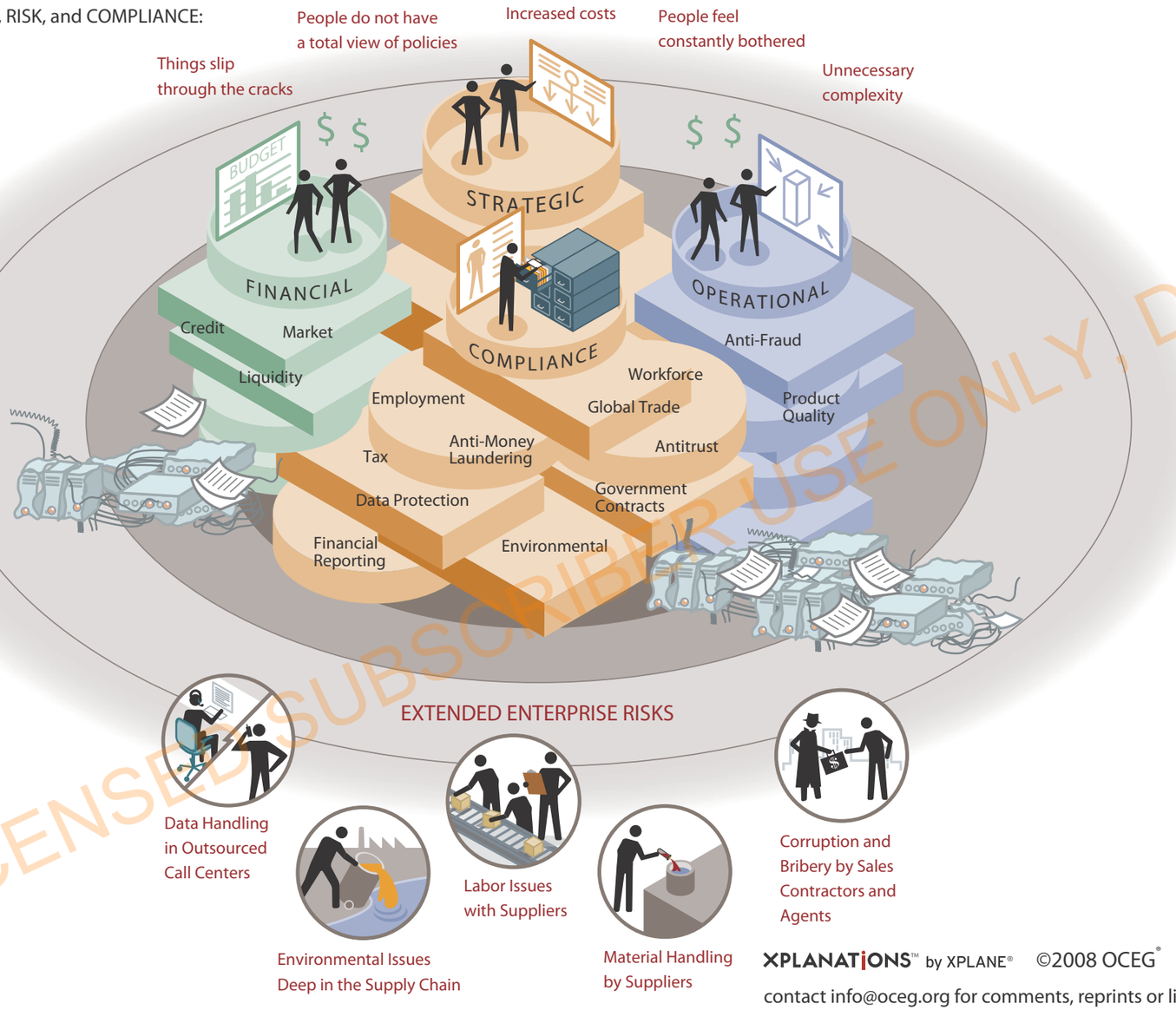
Policy & Training Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

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

SILOS OF GOVERNANCE, RISK, and COMPLIANCE:



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

XPLANATIONS™ by XPLANE® ©2008 OCEG®

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

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Case Study in Effective Policy Management

Morgan Stanley: Case Study in Effective GRC Engagement

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

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

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

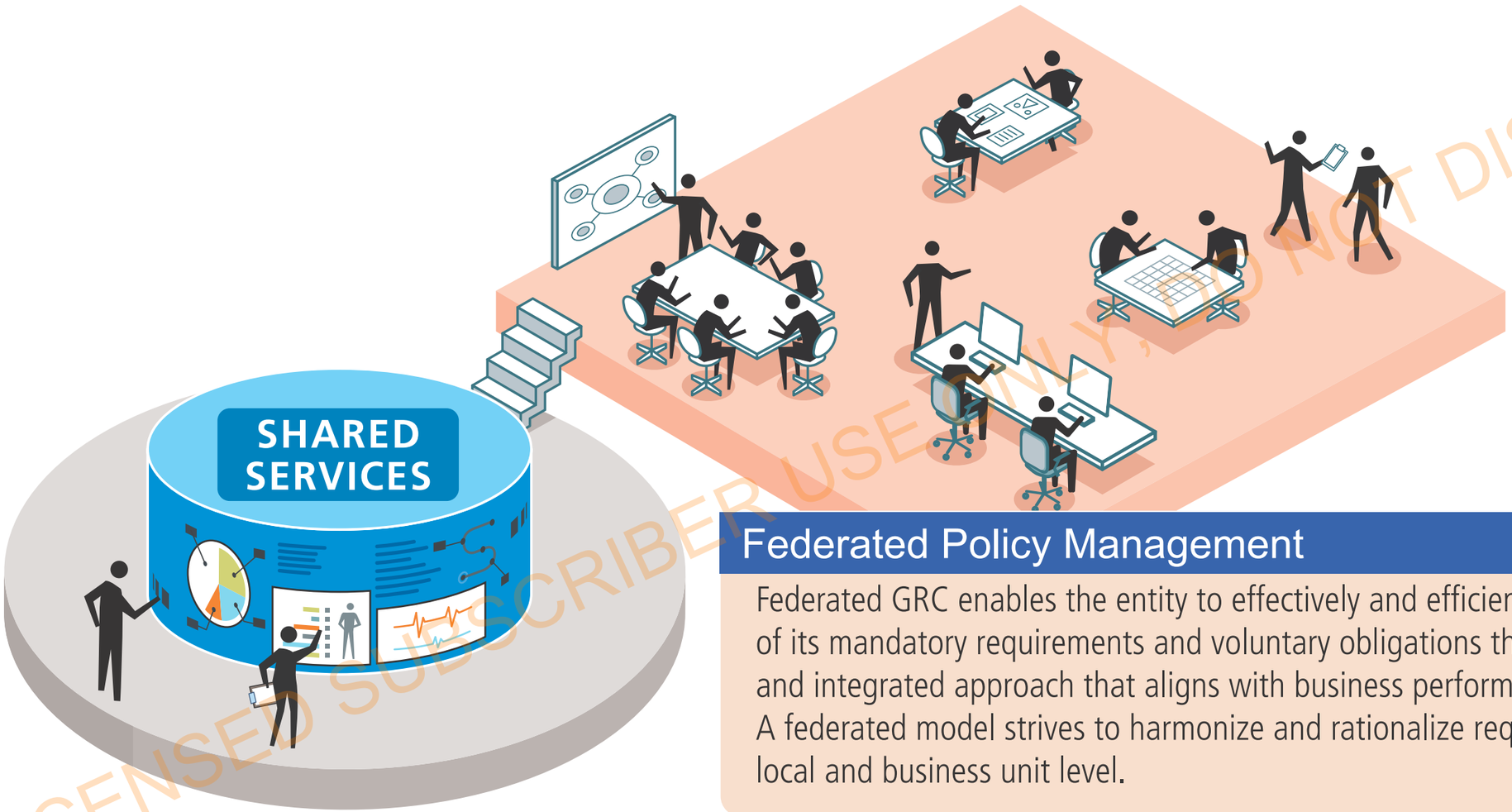
> "have often encountered companies with compliance programs that are strong on paper but that nevertheless have significant . . . violations because management has failed to effectively implement the program even in the face of obvious signs of corruption."

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

LICENSED SUBSCRIBER USE ONLY - DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Federated Policy Management



Federated Policy Management

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

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

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

We have a lot of improper gift incidents clustered in areas where we only train the salesforce once a year. It looks like we need to train more often.

Other countries get the same training but they are more compliant. Let's see if the hot spots have different salary incentives that might need to be changed, or if local management isn't enforcing the policy.

We've got 98% completion overall, but only 77% in the marketing group, which is the worst in the whole company. Why?

Our operations in Italy are number one in reducing injuries on the plant floor from last year to this one. The new policies seem to be working.

I see 22 changes in regulations that affect our policies but no revisions. We might need to change how often policy owners are notified of changes.

We have a lot of improper gift incidents clustered in areas where we only train the salesforce once a year. It looks like we need to train more often.

Other countries get the same training but they are more compliant. Let's see if the hot spots have different salary incentives that might need to be changed, or if local management isn't enforcing the policy.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

An Engaging User Experience for Policy Management

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

UNIFIED

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

RELEVANT

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

INTERACTIVE

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

SOCIAL, YET PERSONAL

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

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

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Policy Content & Intelligence Providers

- ✓ Awareity
- ✓ Compliance Mentor
- ✓ Information Shield
- ✓ Protiviti Knowledge Leader
- ✓ SANS Institute
- ✓ Thompson Information Services
- ✓ Wolters Kluwer Law & Business

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Training Content & Intelligence Providers

- ✓ 360training
- ✓ Click 4 Compliance
- ✓ Compliance Gateway
- ✓ Compliance Online
- ✓ Compliance Publishing Corporation
- ✓ ComplianceWave
- ✓ ComplyArena
- ✓ GRC Solutions
- ✓ Littler
- ✓ LRN
- ✓ MSDSonline
- ✓ NAVEX Global
- ✓ NYSE Governance Services
- ✓ Quest CE
- ✓ Second City
- ✓ SkillCast
- ✓ SkillSoft
- ✓ Thomson Reuters
- ✓ Compliance4All

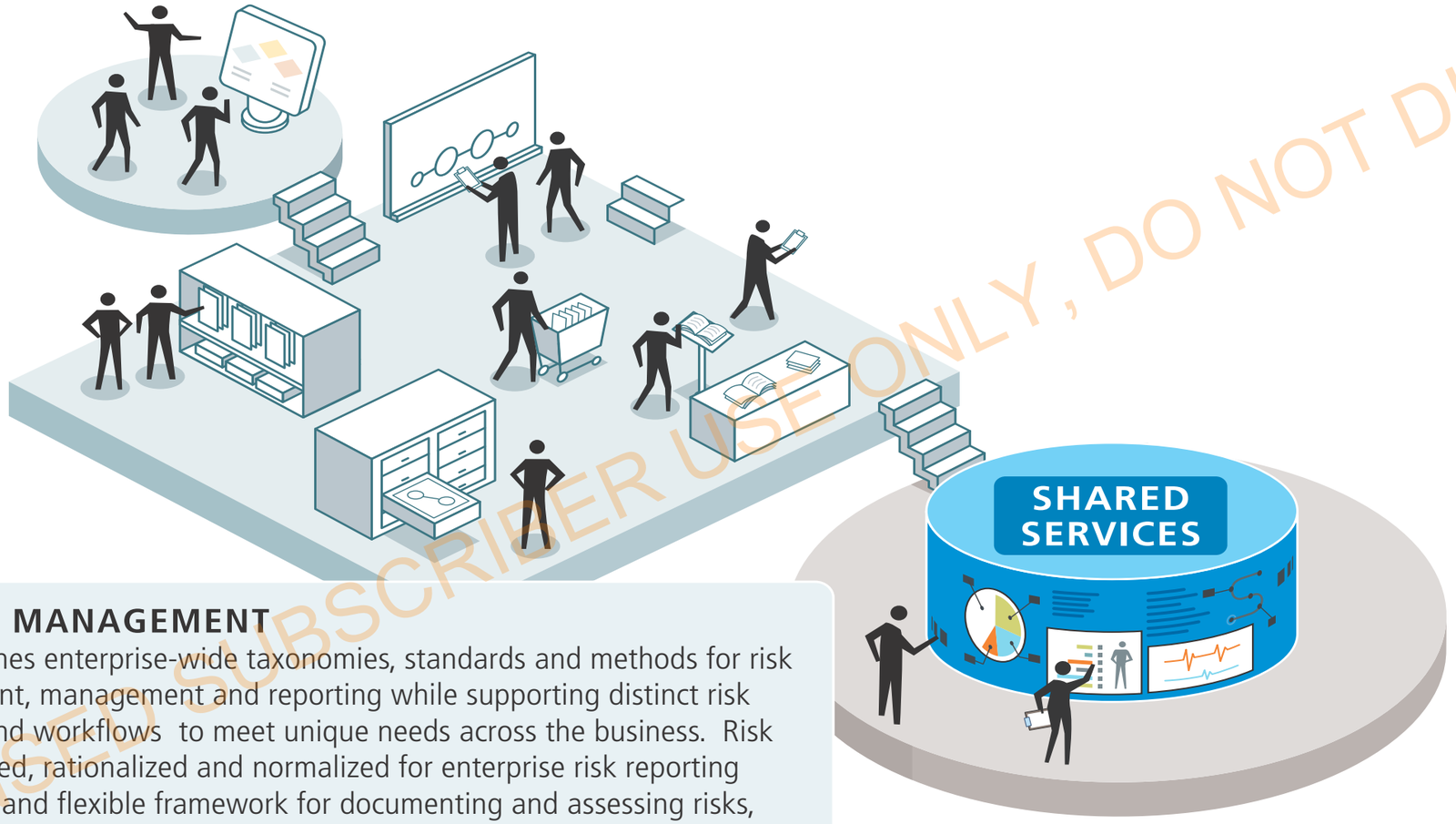
LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

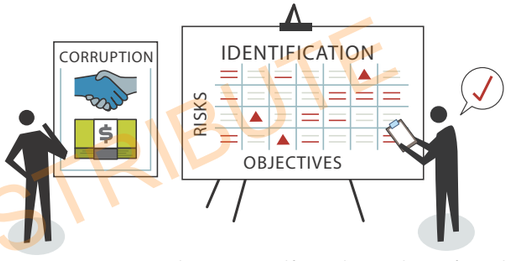
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Risk Management Content & Intelligence

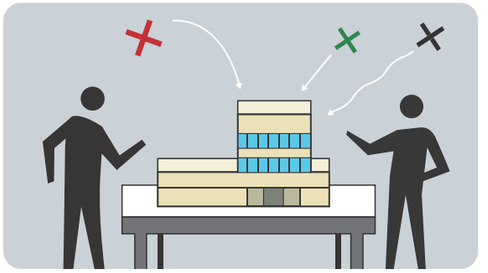
LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Federated Risk Management: Layered Approach to Risk Governance

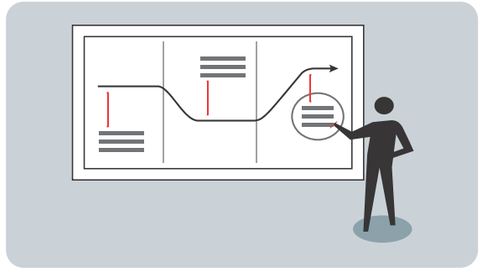




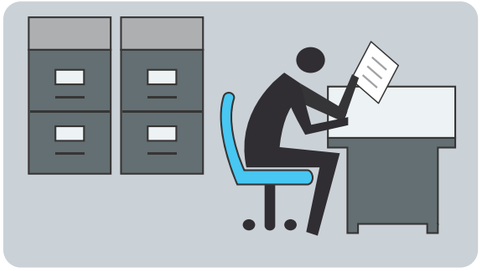
ANALYZE RISKS



UNDERSTAND HISTORY



REVIEW EXISTING POLICIES



FEDERATED RISK MANAGEMENT

Federated GRC establishes enterprise-wide taxonomies, standards and methods for risk identification, assessment, management and reporting while supporting distinct risk methods, taxonomies and workflows to meet unique needs across the business. Risk information is aggregated, rationalized and normalized for enterprise risk reporting based on an integrated and flexible framework for documenting and assessing risks, defining controls, managing assessments, identifying issues, and implementing recommendations and remediation plans.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

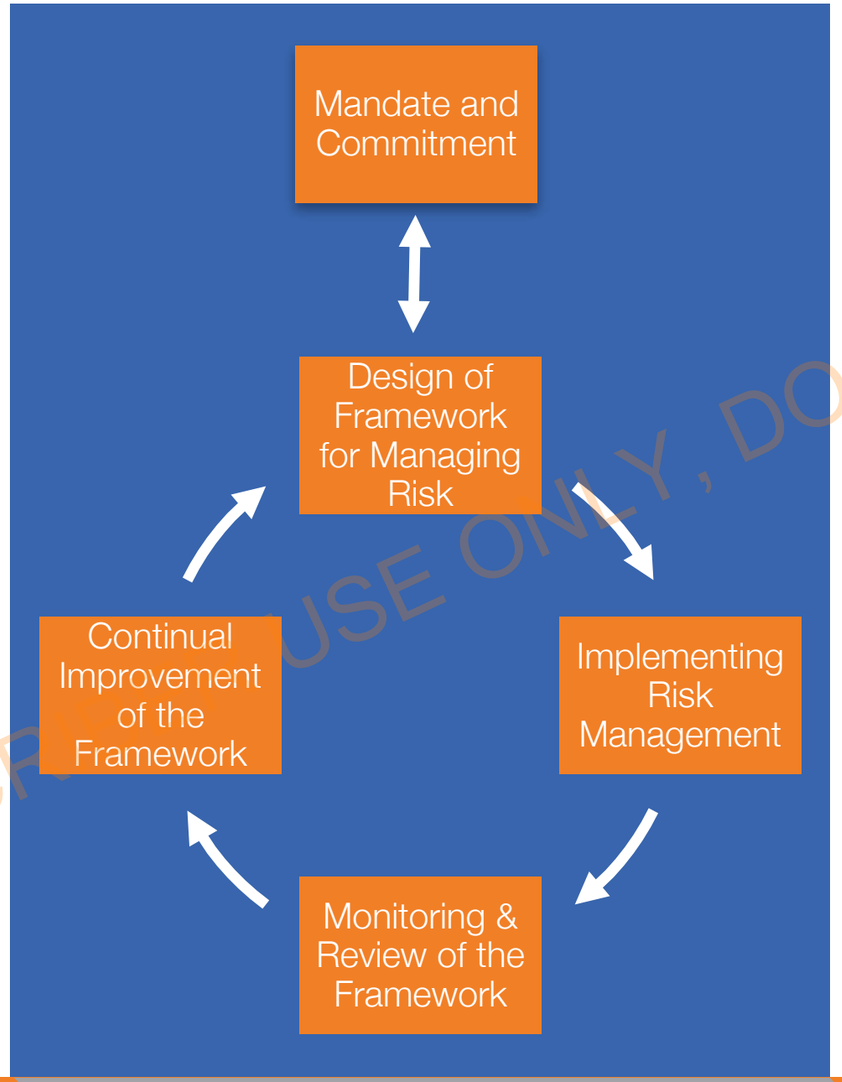
contact Carole S. Switzer, cswitzer@oceg.org for comments, reprints or licensing requests

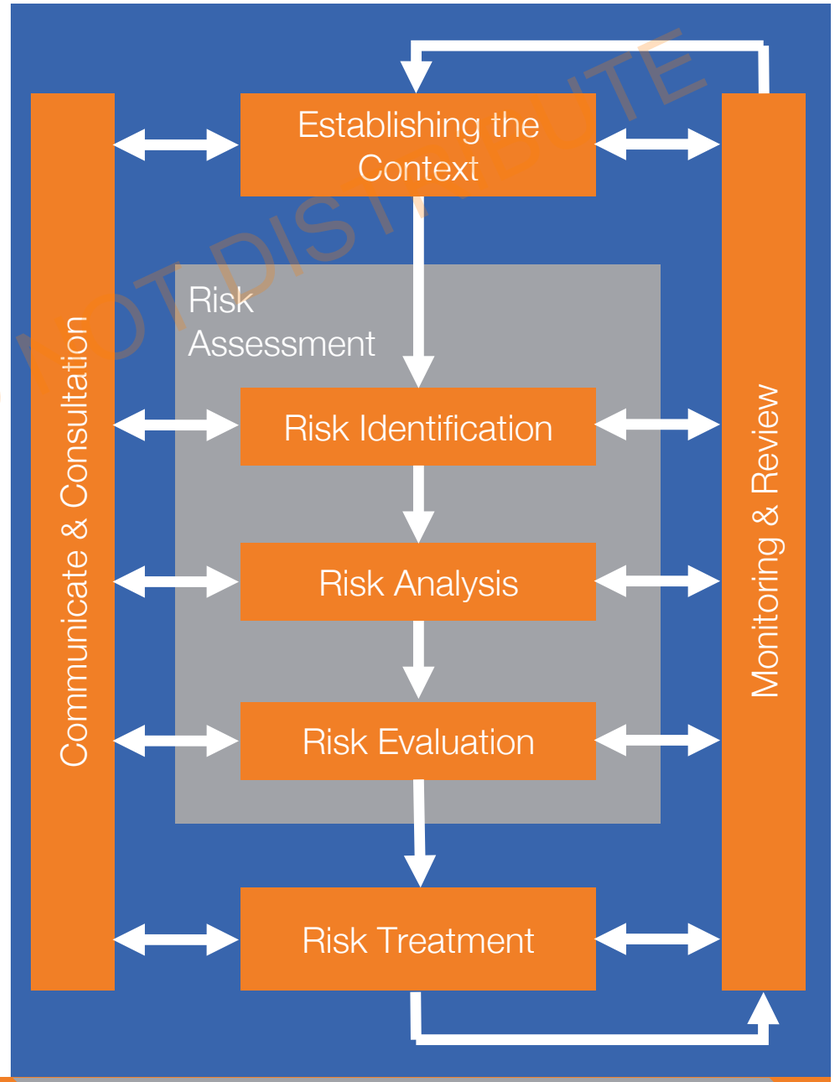
©2013 OCEG visit www.oceg.org for other installments in the GRC Illustrated Series

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

ISO 31000:2009 Risk Management

- ✓ Creates value
- ✓ Integral part of organizational processes
- ✓ Part of decision making
- ✓ Explicitly addresses uncertainty
- ✓ Systematic, structured and timely
- ✓ Based on the best available information
- ✓ Tailored
- ✓ Takes human and cultural factors into account
- ✓ Transparent and inclusive
- ✓ Dynamic, iterative and responsive to change
- ✓ Facilitates continual improvement and enhancement of the organization





1) Risk Management Principles

2) Risk Management Framework

3) Risk Management Process

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Technology Market: Risk Management

Risk Management

- *Enterprise & Operational Risk Mgmt Platforms*
- *Risk Assessment Solutions*
- *Finance & Treasury Risk Management Solutions*
- *Insurance Risk & Claims Management Solutions*
- *Risk Analytics & Modeling Solutions*
- *Model Risk Management Solutions*
- *Project Risk Management Solutions*
- *Loss Collection & Analytic Solutions*
- *Miscellaneous Risk Management Tools*

Risk Intelligence & Content

- *Risk Libraries*
- *Loss Data*
- *Loss Scenarios & Case Studies*
- *Control Libraries*
- *Geo-Political Risk*

Risk Management technologies support the identification, assessment, evaluation and response, and monitoring of risks and opportunities of risk across the organization.

This includes the ability to monitor changes in the external and internal contexts to alert an organization to changing risk conditions (e.g., geo-political, economic, competitor, technology, and natural disaster) that can impact business. These systems help identify specific causes and execute historical review, simulation, interpretation and projection of impacts on an organization's operations or assets given the potential consequences of events and the likelihood of events occurring sequentially or simultaneously.

This category includes enterprise risk management systems, operational risk management systems, as well as specialized risk applications.

Finance/Treasury Risk Management - involves an array of applications and systems used to identify and manage the risk factors, causes and response procedures in an organization's financial and treasury management. These include risk technology focused on specific areas such as liquidity, credit, market, and commodity risk management that help identify risk and execute historical review, simulation, interpretation and projection of impacts on an organization's financial assets given the potential consequences of events and the likelihood of events occurring sequentially or simultaneously.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Risk Management Content & Intelligence Providers

- ✓ Accuity
- ✓ Bloomberg Finance L.P.
- ✓ Dow Jones
- ✓ Dunn & Bradstreet
- ✓ Economist Intelligence Unit
- ✓ Eurasia Group
- ✓ IBM Algo FIRST
- ✓ iJet
- ✓ LexisNexis
- ✓ MapleCroft
- ✓ Radar Risk
- ✓ RiskBusiness
- ✓ RiskSpotlight
- ✓ SAS
- ✓ Segmantics
- ✓ Standard & Poors
- ✓ VeRisk
- ✓ Enlight Research

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Third Party Management Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Who is a 3rd Party?

LICENSED SUBSCRIBER ONLY. DO NOT DISTRIBUTE

©2014 OCEG®

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

3rd Party Risk Bearing Down on Organizations

The issues organizations face in managing risk and compliance across extended business relationships include:

- ❑ Bribery & corruption
- ❑ Business continuity
- ❑ Code of conduct and ethics
- ❑ Conflict minerals
- ❑ Corporate social responsibility
- ❑ Environmental
- ❑ Geo-political risk
- ❑ Health and safety
- ❑ Human rights, trafficking & slavery
- ❑ Import and export compliance
- ❑ Information security
- ❑ Labor standards
- ❑ Operational risk
- ❑ Privacy
- ❑ Quality
- ❑ Regulatory compliance
- ❑ Physical security
- ❑ Supply-chain risks

You cannot outsource liability

- ➢ You "stand in the shoes" of your business relationships
- ➢ Their problems are your problems
- ➢ Their problems directly impact your brand and reputation

Increasing regulatory focus

- ➢ Can you attest to an "in-compliance" status?

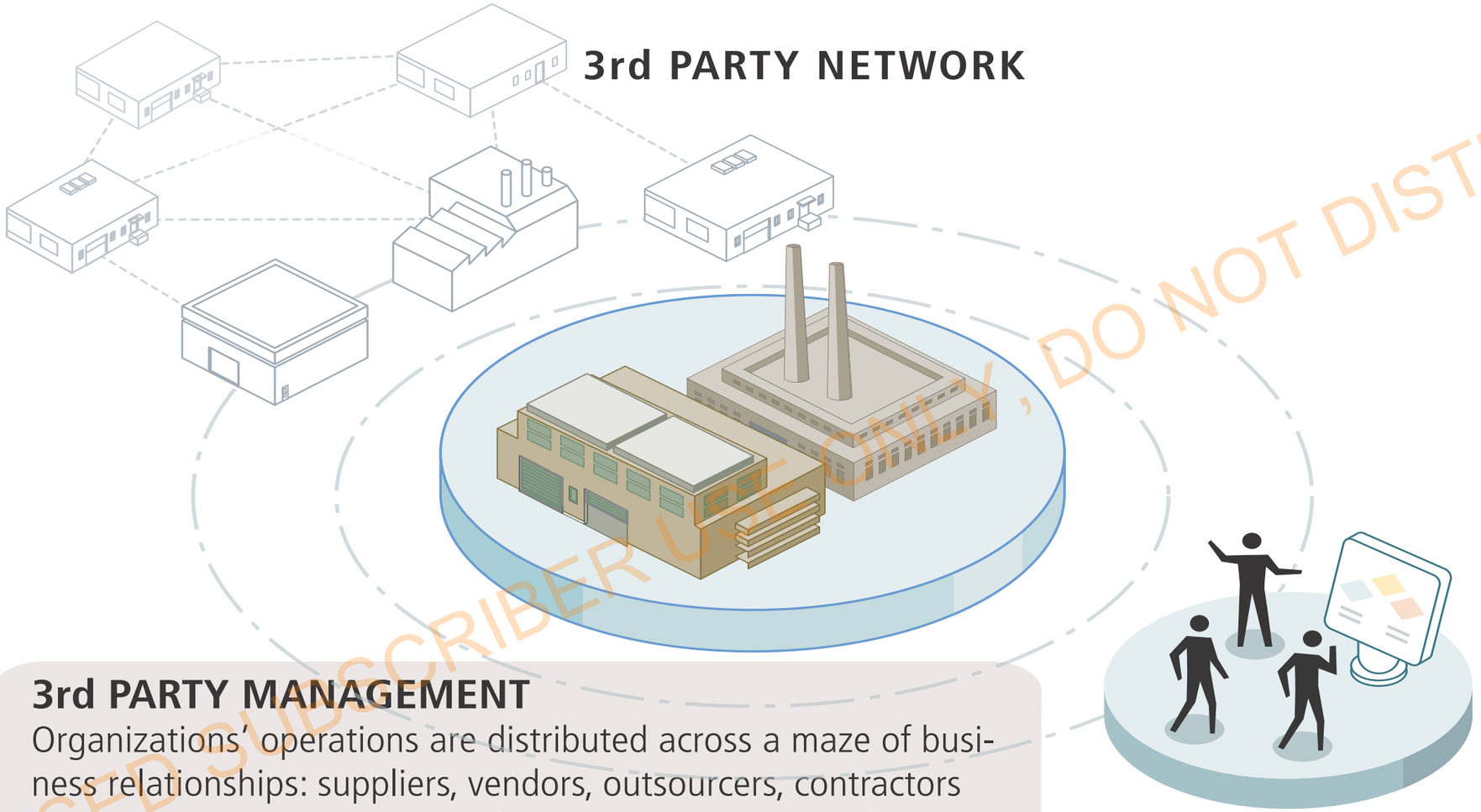
Many companies focus on the on-boarding process…

- ➢ Most risk is incurred over the life of the relationship
- ➢ Who owns on-going third party risk?
- ➢ How is third party risk assessed and reported to the board?

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Federated 3rd Party Management



3rd PARTY MANAGEMENT

Organizations' operations are distributed across a maze of business relationships: suppliers, vendors, outsourcers, contractors and agents. Federated GRC includes the integration and oversight of performance, risk, and compliance across the organization's third party relationships and transactions.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

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

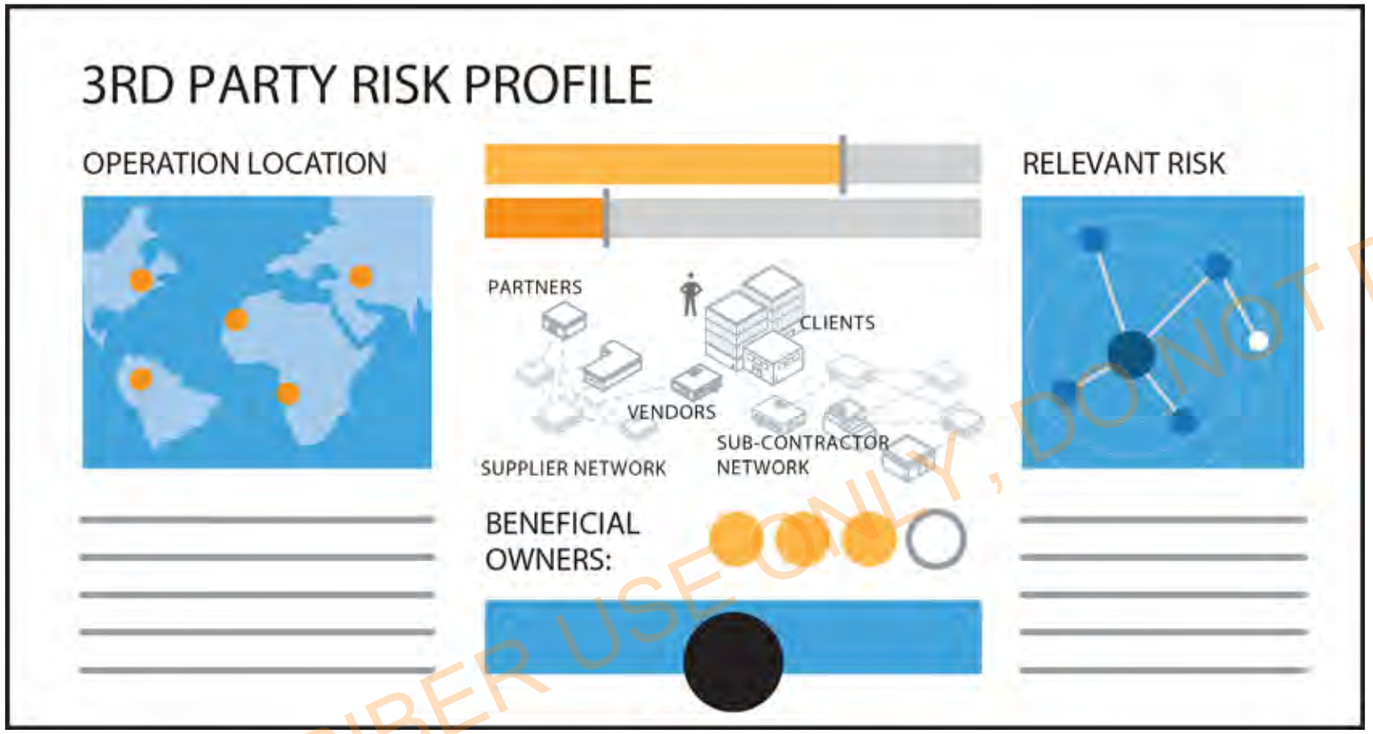
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

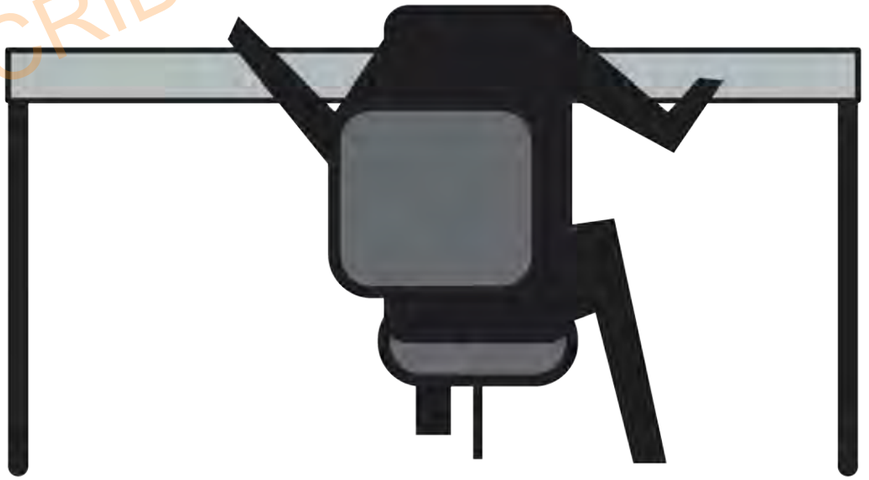
Overview of a 3rd Party Management Process

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

3rd Party Risk Profile





LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Contact info@oceg.org for comments, reprints or licensing requests ©2017 OCEG for additional resources visit www.oceg.org/resources
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Go Beyond Basic Due Diligence

GO BEYOND BASIC DUE DILIGENCE

Organizations often rely on the use of independent data sources to screen and validate self-reported information from third party questionnaires collected through the on-boarding process. This helps them establish a foundational workflow that takes in third-party data and screens it against various separate sanctions and watch lists, country risk databases and other public records. This provides greater confidence in their risk mitigation program. However there are limitations to what this linear and siloed screening workflow can accomplish. It is now possible, and essential, to develop a more holistic, integrated approach to due diligence.

RISKS & DRAWBACKS:

- Incomplete View of Risk
- Disconnected Data Sources
- Time and Resource Intensive
- Manual Remediation of False Positives

LICENSED SUBSCRIBER USE ONLY DO NOT DISTRIBUTE

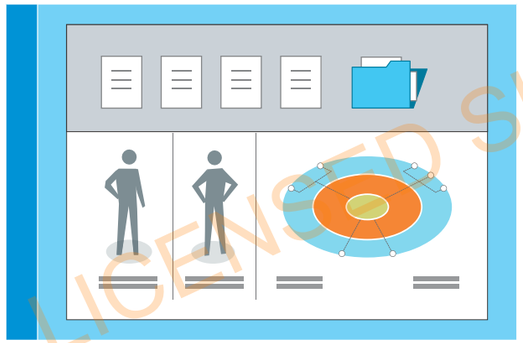
Contact info@oceg.org for comments, reprints or licensing requests ©2017 OCEG for additional resources visit www.oceg.org/resources

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

GRC Market: Third Party Management

Third Party Management Technology

- *Third Party Management Platforms*
- *Third Party Risk Management Solutions*
- *Procurement & ERP Third Party Solutions*
- *Screening & Due Diligence Solutions*
- *Miscellaneous Third Party Management Tools*



AUTOMATION AND TRACKING

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

Third Party Intelligence & Content

- *Third Party Forms & Templates*
- *PEP/Sanction/Watch Lists*
- *Negative News*
- *Organization/Corporate Ratings*
- *Geo-Political Risk*
- *Reputation & Brand Lists & Monitoring*
- *Sourcing Information*
- *Vessels Data*
- *Controlled Goods & Substances*
- *IT Security Ratings*

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

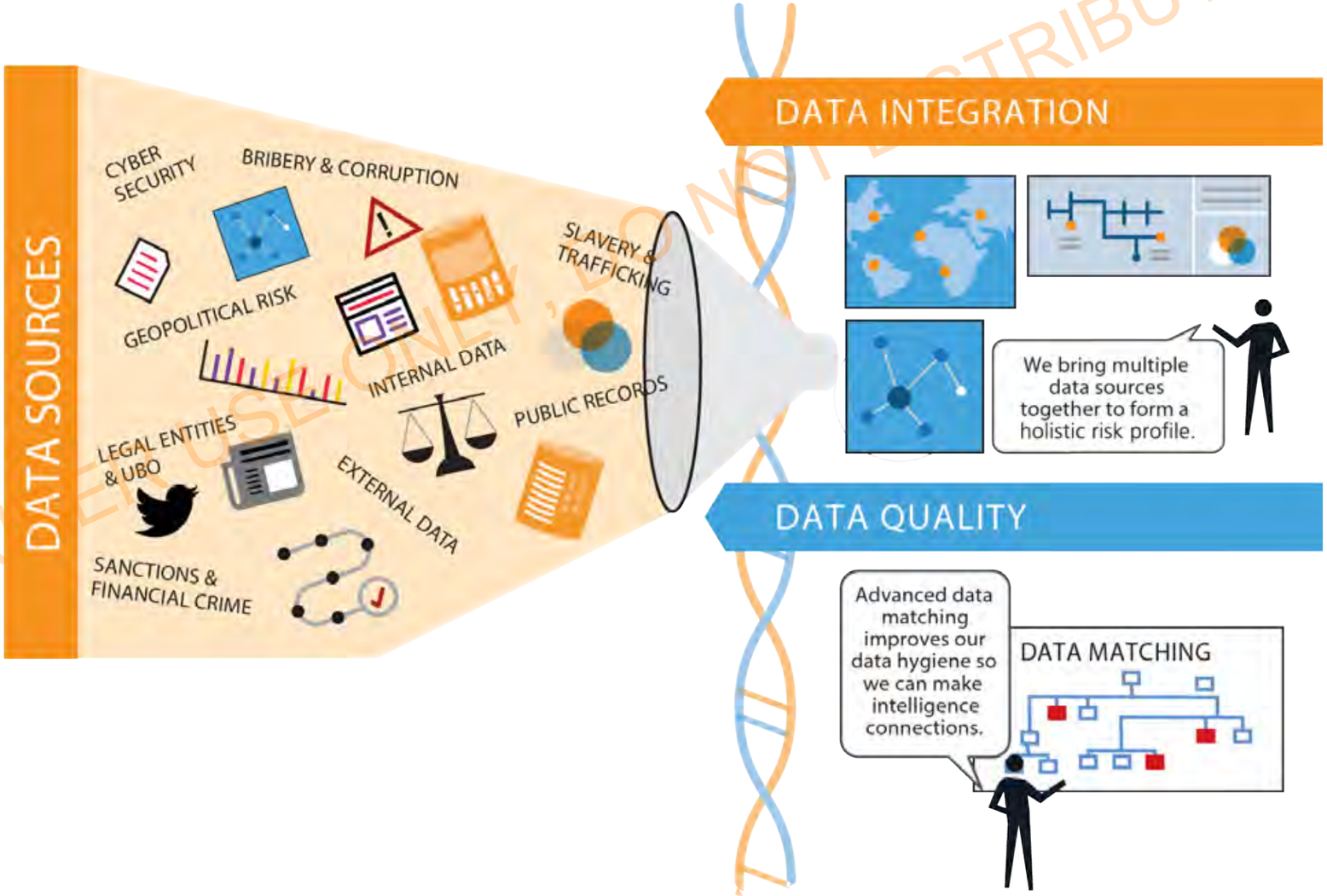
© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

3rd Party Data Integration

INTEGRATE, AUTOMATE & STREAMLINE

Cutting edge due diligence programs incorporate an array of internal and external data sources. These are mapped, integrated, and consumed in a technology powered workflow, enabling:

- Evaluation of a broad, holistic risk profile
- Deeper data mining and improved data hygiene
- Visibility of previously unseen connections and changes
- Ongoing monitoring with timely reports
- Streamlined workflow with less manual effort



LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Third Party Management Content & Intelligence Providers

- ✓ 3E
- ✓ Accuity
- ✓ Arachynys
- ✓ BitsightTech
- ✓ Blue Umbrella
- ✓ CFSI – Conflict-Free Sourcing Initiative
- ✓ Clear Market Practices
- ✓ Compliance Publishing Corporation
- ✓ CORL
- ✓ Exiger
- ✓ Fenergo
- ✓ Dow Jones
- ✓ Dunn & Bradstreet
- ✓ EcoDesk
- ✓ Economist Intelligence Unit
- ✓ Ecovadis
- ✓ EthixBase
- ✓ EurasiaGroup
- ✓ GreenPoint Law & Compliance iJet
- ✓ Kroll
- ✓ LexisNexis
- ✓ MapleCroft
- ✓ Monitor Global Outlook
- ✓ NASDAQ
- ✓ NAVEX Global
- ✓ Nomino Data
- ✓ Optiv
- ✓ Rapid Ratings
- ✓ Red Flag Group
- ✓ Regulatory Data Corp
- ✓ Resilinc

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Third Party Management Content & Intelligence Providers, continued

- ✓ RepRisk
- ✓ SecurityScorecard
- ✓ Shared Assessments
- ✓ Source Intelligence
- ✓ Standard & Poors
- ✓ Steele CIS
- ✓ Thomson Reuters
- ✓ TRACE International
- ✓ VeRisk

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Issue Specific Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Privacy Content & Intelligence Providers

- ✓ Bloomberg BNA
- ✓ Clearwater Compliance
- ✓ Littler
- ✓ TRUSTe

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Employment & Labor Content & Intelligence Providers

- ✓ Bloomberg BNA
- ✓ Littler
- ✓ Specialty Technical Publications
- ✓ Thompson Information Services
- ✓ Wolters Kluwer Law & Business

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Industry Specific Content & Intelligence

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Financial Services Content & Intelligence Providers

- ✓ Accurity
- ✓ Bloomberg BNA
- ✓ Clear Market Practices
- ✓ IBM Promontory
- ✓ JWG
- ✓ LexisNexis
- ✓ Propylon
- ✓ Quest CE
- ✓ Reg-Room
- ✓ RegEd
- ✓ Risk Spotlight
- ✓ Thompson Information Services
- ✓ Thomson Reuters
- ✓ Wolters Kluwer Financial Services
- ✓ Wolters Kluwer Law & Business
- ✓ Fenergo

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Healthcare & Life Sciences Content & Intelligence Providers

- ✓ Bloomberg BNA
- ✓ Clear Market Practices
- ✓ Clearwater Compliance LLC
- ✓ LexisNexis
- ✓ Littler
- ✓ RegScan
- ✓ Regulatory Consulting Limited
- ✓ Thompson Information Services
- ✓ Thomson Reuters
- ✓ Wolters Kluwer Law & Business

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Energy Content & Intelligence Providers

- ✓ Bloomberg Finance L.P.
- ✓ Thompson Information Services

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Two Things to Note . . .

Complimentary Inquiry

- Organizations evaluating or considering GRC solutions are free to ask GRC 20/20 on our understanding and comparison of solutions in the market to meet your GRC requirements.
- Inquiries are single focused questions that can be answered in under 30 minutes.
- Complimentary inquiry is only available to organizations evaluating or considering GRC solutions for their internal use.

RFP Development & Support

- GRC 20/20 has an extensive library of RFP requirements across a range of GRC capability areas presented in this presentation.
- GRC 20/20 can be engaged in RFP development and support projects to streamline your process, gain perspectives learned from other organizations, and to keep solution providers honest in their responses.

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

© GRC 20/20 Research, LLC, all rights reserved, www.GRC2020.com

Questions?

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

Subscribe GRC 20/20 Newsletter

LinkedIn: GRC 20/20

LinkedIn: Michael Rasmussen

Twitter: GRCPundit

Blog: GRC Pundit

LICENSED SUBSCRIBER USE ONLY, DO NOT DISTRIBUTE

Some of the content we have evaluated is OCEG content which GRC 20/20 has an established relationship to use. Please do not copy slides or graphics without permission. GRC 20/20 highly recommends you consider OCEG membership at www.OCEG.org.