grc 20/20
Bringing GRC into Focus

WORKSHOP

UK Corporate Governance Code by Design

Michael Rasmussen, The GRC Pundit & Analyst

The Baseline Is Instability

Weak Links Expose the Organization

> The more we study the major problems of our time, the more we come to realise that they cannot be understood in isolation. They are systemic problems, which means that they are interconnected and interdependent.
>
> - Physicist Fritjof Capra

Are you truly aware of your risks?

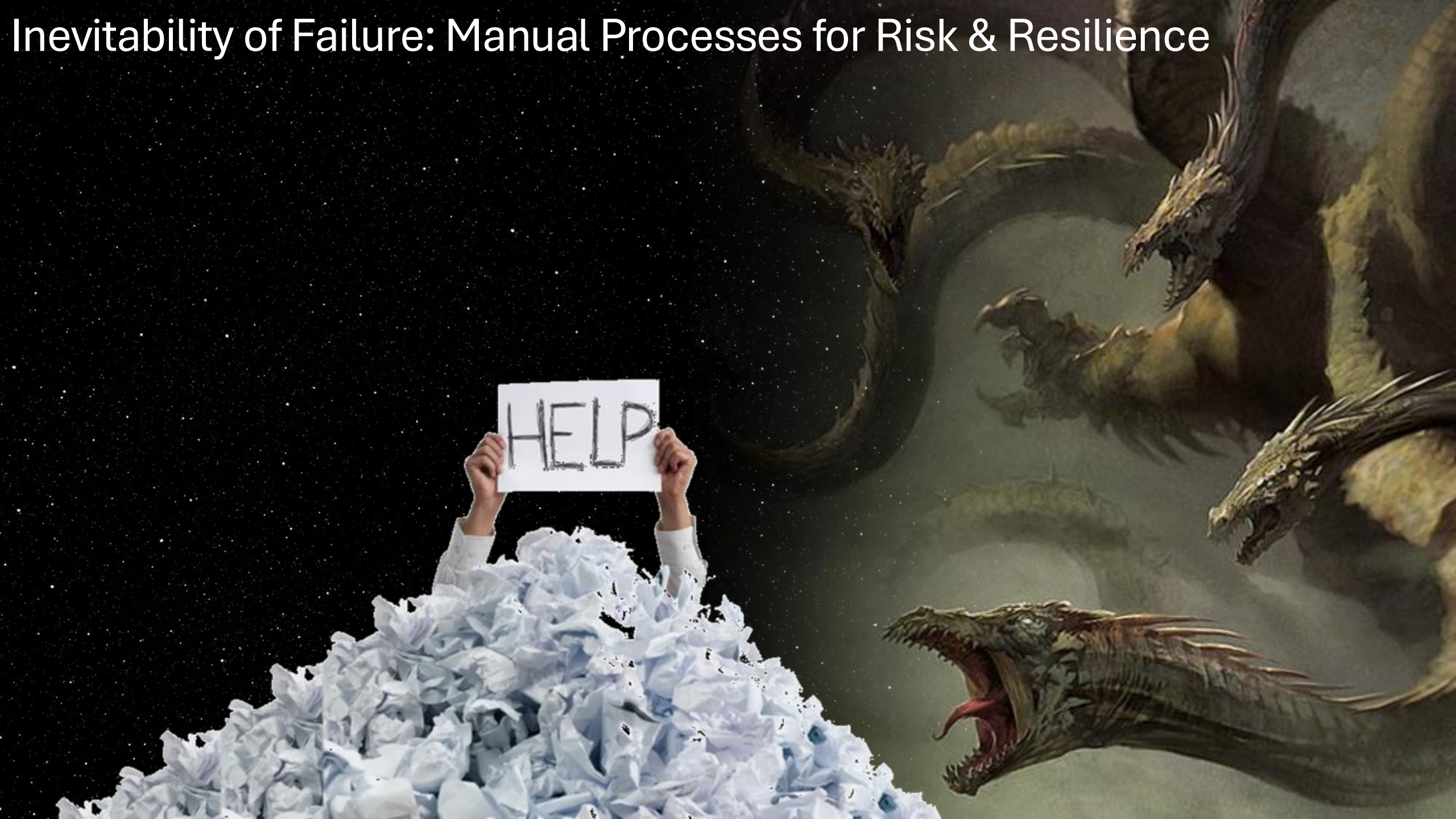
“I never saw a wreck and never have been wrecked, nor was I ever in a predicament that threatened to end in a disaster. I cannot conceive of any vital disaster happening to this vessel.”

E.J. Smith,
Captain of the Titanic

Risk & Internal Control

Too Often Looking in the Rearview Mirror

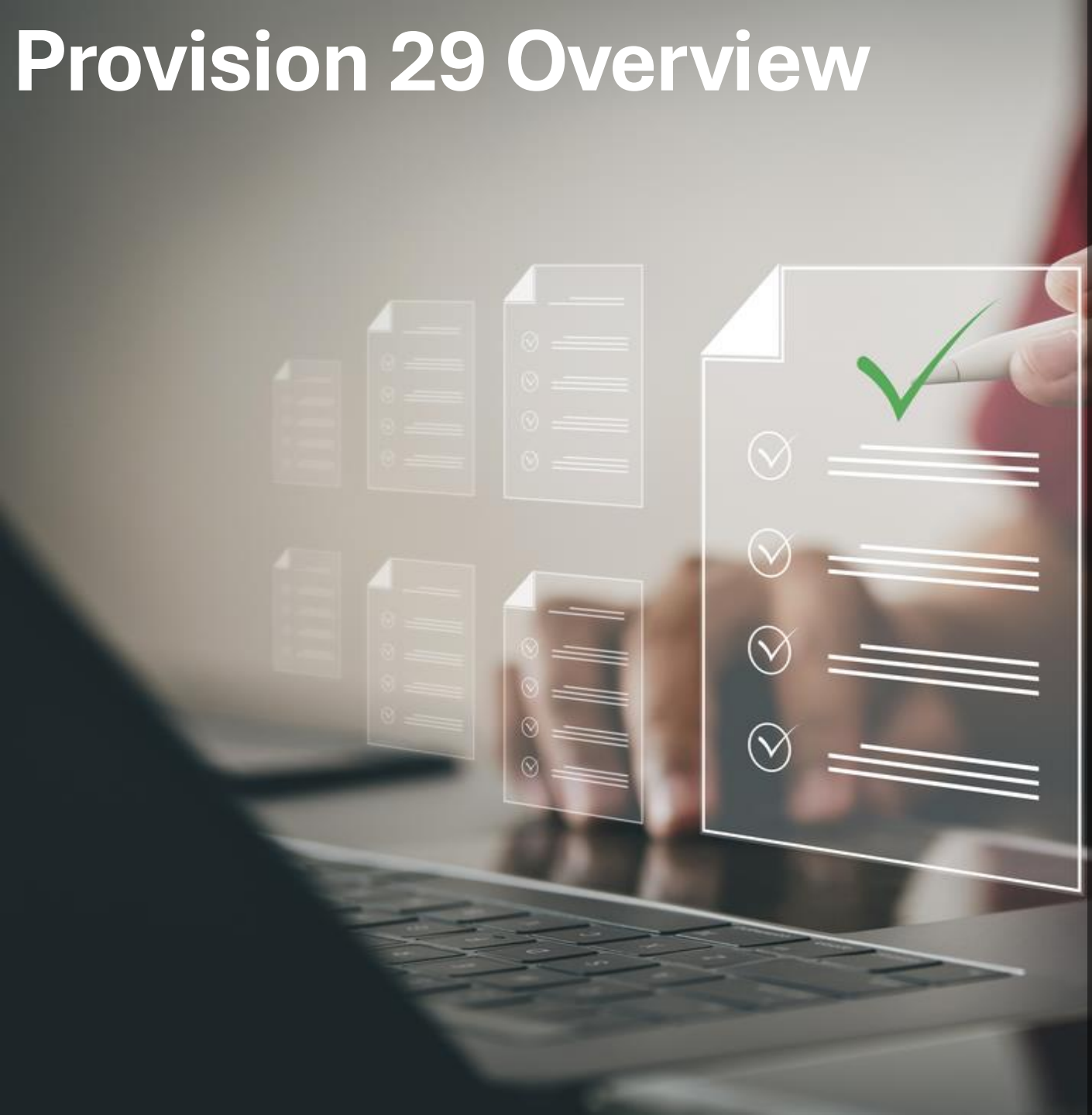
Inevitability of Failure: Manual Processes for Risk & Resilience



Risk & Control Mystery House

- 160 rooms
- 47 fireplaces
- 6 kitchens
- 10,000 windows
- 65 doors to blank walls
- 13 staircases abandoned
- 25 skylights – in floors
- 147 builders/no architects
- Built without a blueprint
- $5.5 million over 38 years

Provision 29 Overview



In Provision 29 mandates that company boards must:

- Actively monitor and review the effectiveness of their company's risk management and internal control framework, including all material controls (financial, operational, reporting, and compliance),

- Provide a declaration regarding their effectiveness in the annual report, signifying a heightened focus on internal control oversight.

Provision 29 Key Implications

- **Accountability:** Boards are now directly accountable for the ongoing effectiveness of risk management and internal controls.

- **Transparency:** The requirement promotes greater transparency, enabling stakeholders to have increased confidence in the organization's governance practices.

- **Monitoring:** Organizations must implement processes for continuous assessment rather than relying solely on periodic reviews.

Key Changes to Corporate Governance Code

1. **Outcomes-Based Reporting.** Outcomes-based reporting is a crucial aspect of board governance. Boards should use this reporting mechanism to clearly demonstrate how their actions and observable outcomes align with the company's strategy and objectives.

2. **Embedding Culture.** In addition to setting the company's culture from the top down, boards should now also actively work to ensure that culture is manifested throughout the organization.

3. **Effectiveness of Risk Management & Internal Controls. B**oards are expected to monitor the company's risk management and internal control framework. They should provide an annual report declaring the effectiveness of material controls.

Outcome/Principle-Based Compliance

The Financial Reporting Council (FRC) promotes an outcomes-focused approach to corporate governance reporting, encouraging companies to explain instances of non-compliance.

This approach is flexible and considers stakeholder expectations, avoiding rigid definitions.

The FRC acknowledges that applying Code provisions should be tailored to each company's strategy, maturity, and complexity.

Audit, Risk & Internal Control Changes

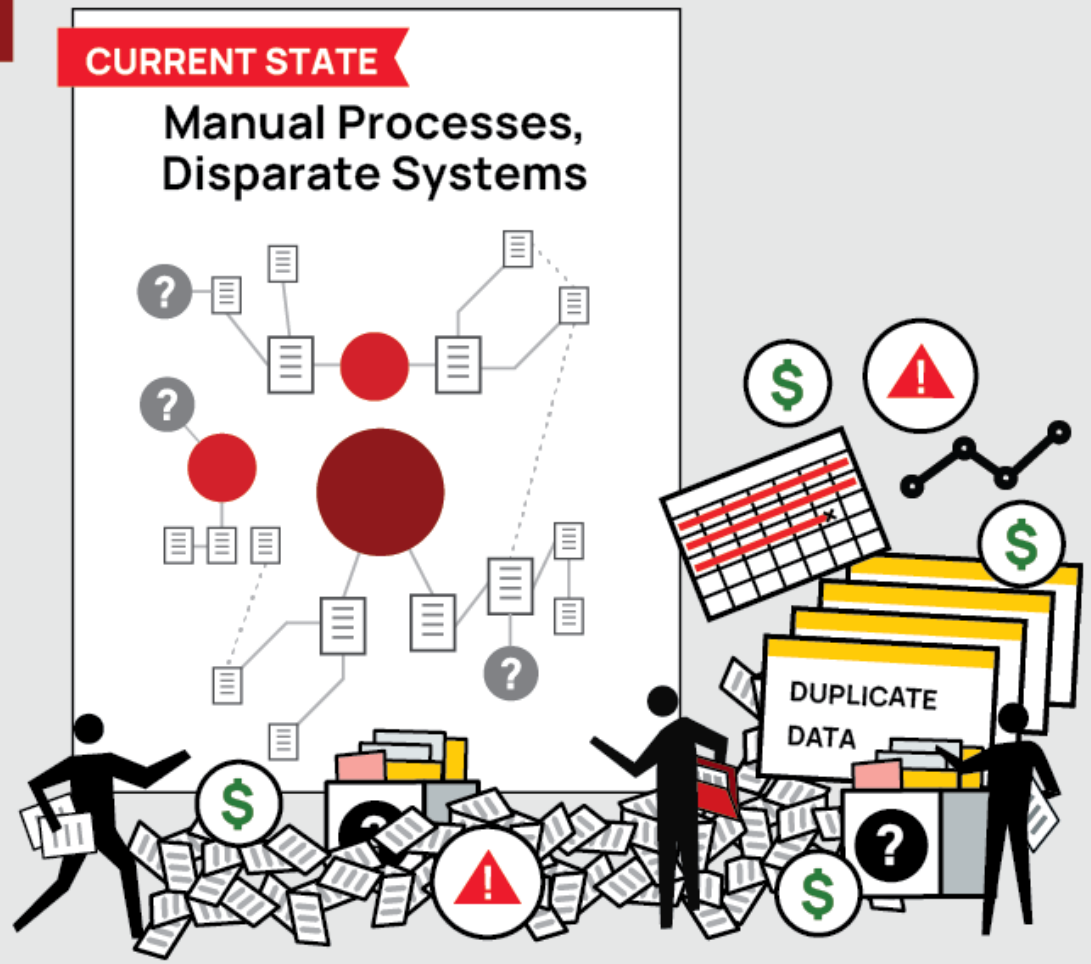
Principle O has been amended to make the board responsible not only for establishing, but also for maintaining the effectiveness of, the risk management and internal control framework.	1 January 2025
Provision 25 and Provision 26 have been updated to reflect the Minimum Standard: Audit Committees and the External Audit, and duplicative language has been removed.	1 January 2025
New: **Provision 29.** The board should monitor the company's risk management and internal control framework and, at least annually, carry out a review of its effectiveness. The monitoring and review should cover all material controls, including financial, operational, reporting and compliance controls. The board should provide in the annual report: • A description of how the board has monitored and reviewed the effectiveness of the framework; • A declaration of effectiveness of the material controls as at the balance sheet date; and • A description of any material controls which have not operated effectively as at the balance sheet date, the action taken, or proposed, to improve them and any action taken to address previously reported issues.	1 January 2026

SOURCE: https://media.frc.org.uk/documents/UK_Corporate_Governance_Code_2024_Key_Changes.pdf

Top 10 Challenges Companies Face

Managing risk and resilience in manual processes poses many challenges for companies:

- Lack of Risk Agility
- Fragmented & Inaccurate Data
- Limited Visibility
- Inefficient Workflows
- Inadequate Risk Reporting
- Limited Scalability
- Resource Intensiveness
- Ineffective Collaboration
- Resilience Planning Gaps
- Difficulties in Change Management



Address these challenges by transitioning to an integrated risk and resilience management solution that provides a unified view of data, streamline workflows, and deliver greater efficiency, effectiveness, resilience, and agility to the organization.

Success Requires Risk Taking, But Risk Must Be Managed

Business is the undertaking of risk for reward.

Judge Mervyn King, South Africa

King I, II, III, IV Report on Corporate Governance

Risk & Internal Control= NO SURPRISES!

Risk & Internal Control

Navigating Uncertainty on the Road Ahead

The questions organizations need to ask:

- ✓ Does the organization have enough information to make decisions about the future of the company, when they don't have a clear view of risks that impact critical business operations and processes?
- ✓ Does the organization know its risk exposure at the enterprise, business process, and technology levels and how they interrelate?
- ✓ How does the organization know it is managing and mitigating risk effectively in the context of the business to achieve business goals?
- ✓ Can the organization accurately gauge the impact of risk on business strategy, objectives, and operations?
- ✓ Does the organization get the information it needs to take timely action to risk exposure to avoid or mitigate loss and situations of non-compliance?
- ✓ Does the organization monitor key risk indicators across key objectives, systems, processes, and information?
- ✓ Does the organization optimally measure and model risk in a business context?

Risk & Resilience Management by Design: Federated Risk Management Architecture

What is Your Approach to Risk & Internal Control Management?

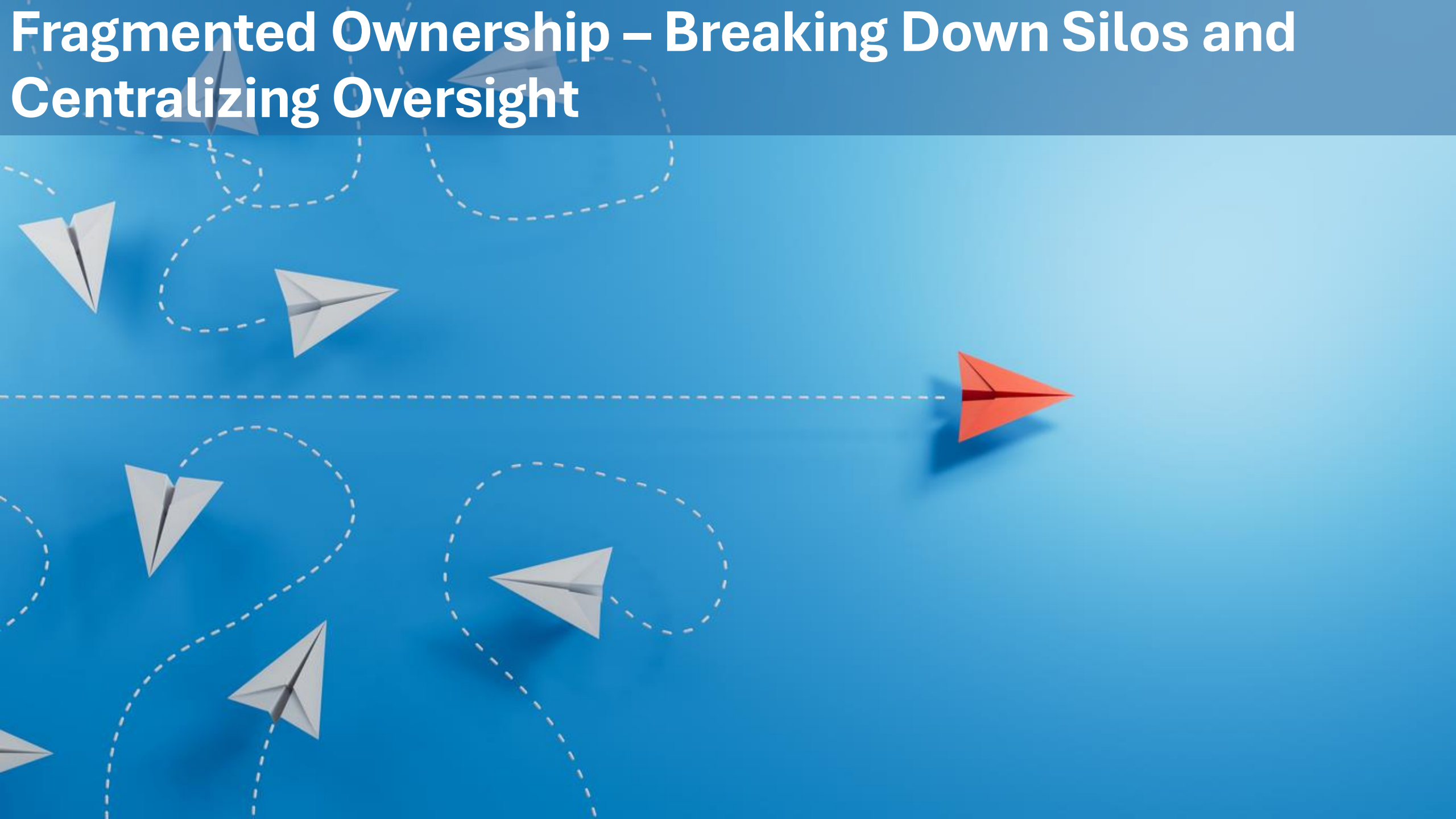
Distributed Risk & Control Management

- Disconnected departments managing risk in different ways with little or no collaboration with other departments

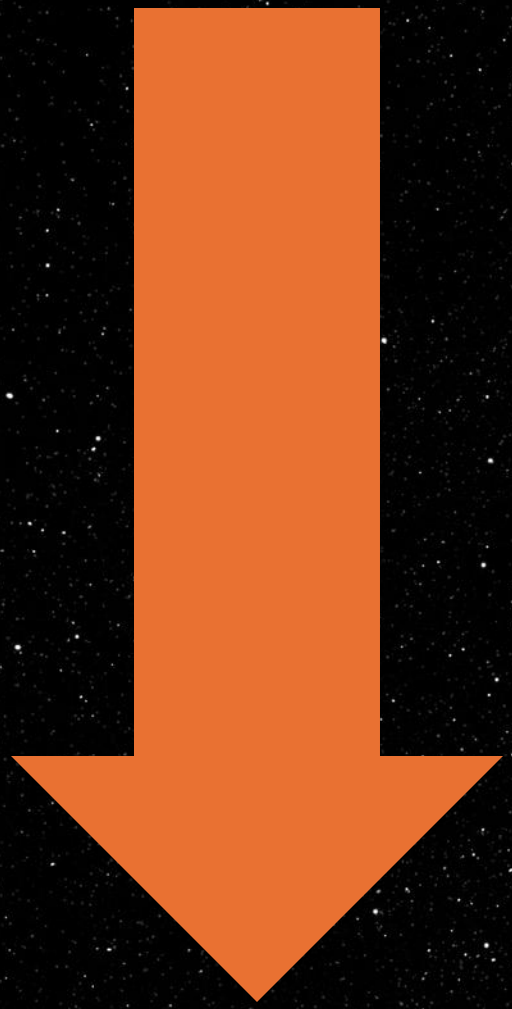
Federated Risk & Control Management

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

Fragmented Ownership – Breaking Down Silos and Centralizing Oversight

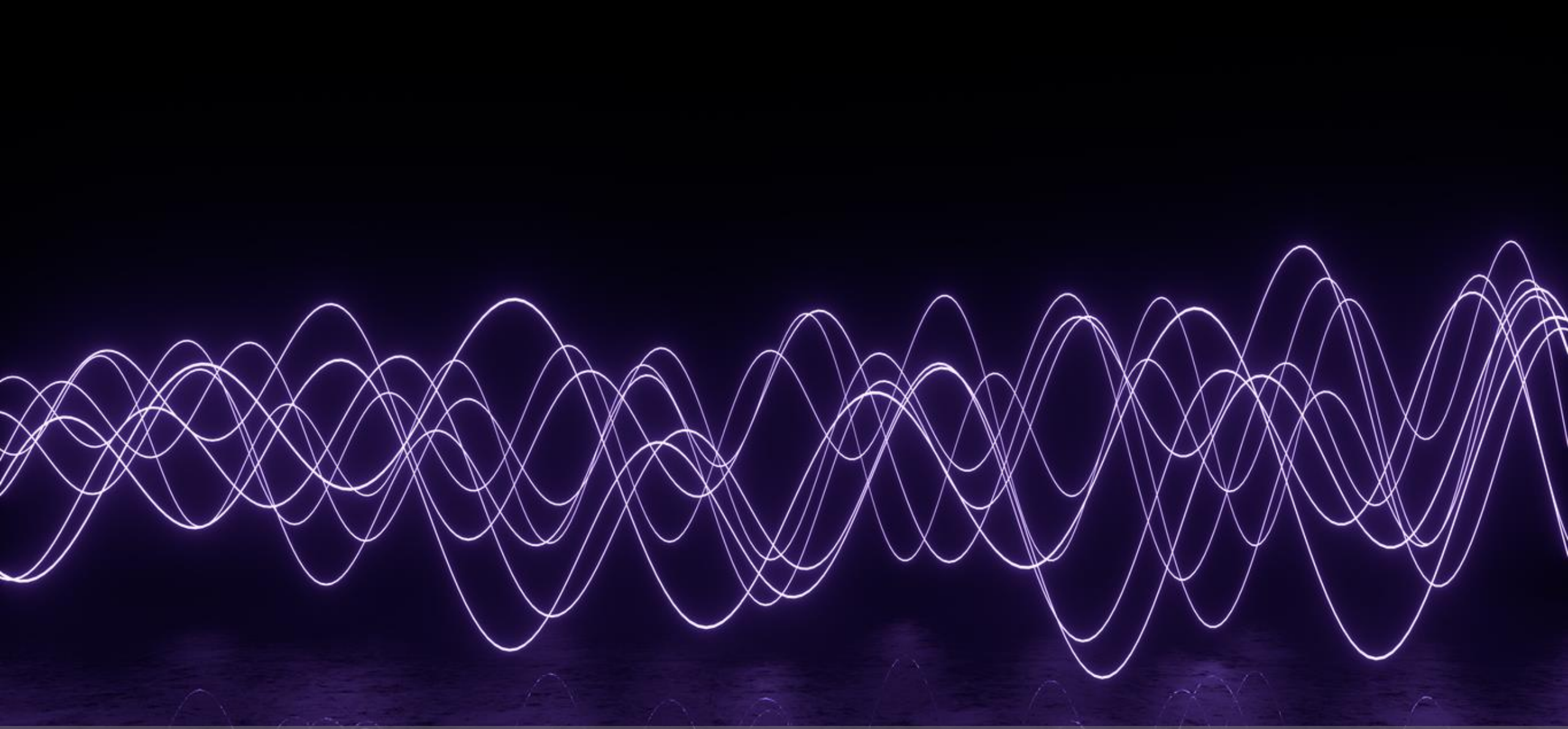


Risk & Control Management: a Top-Down Approach



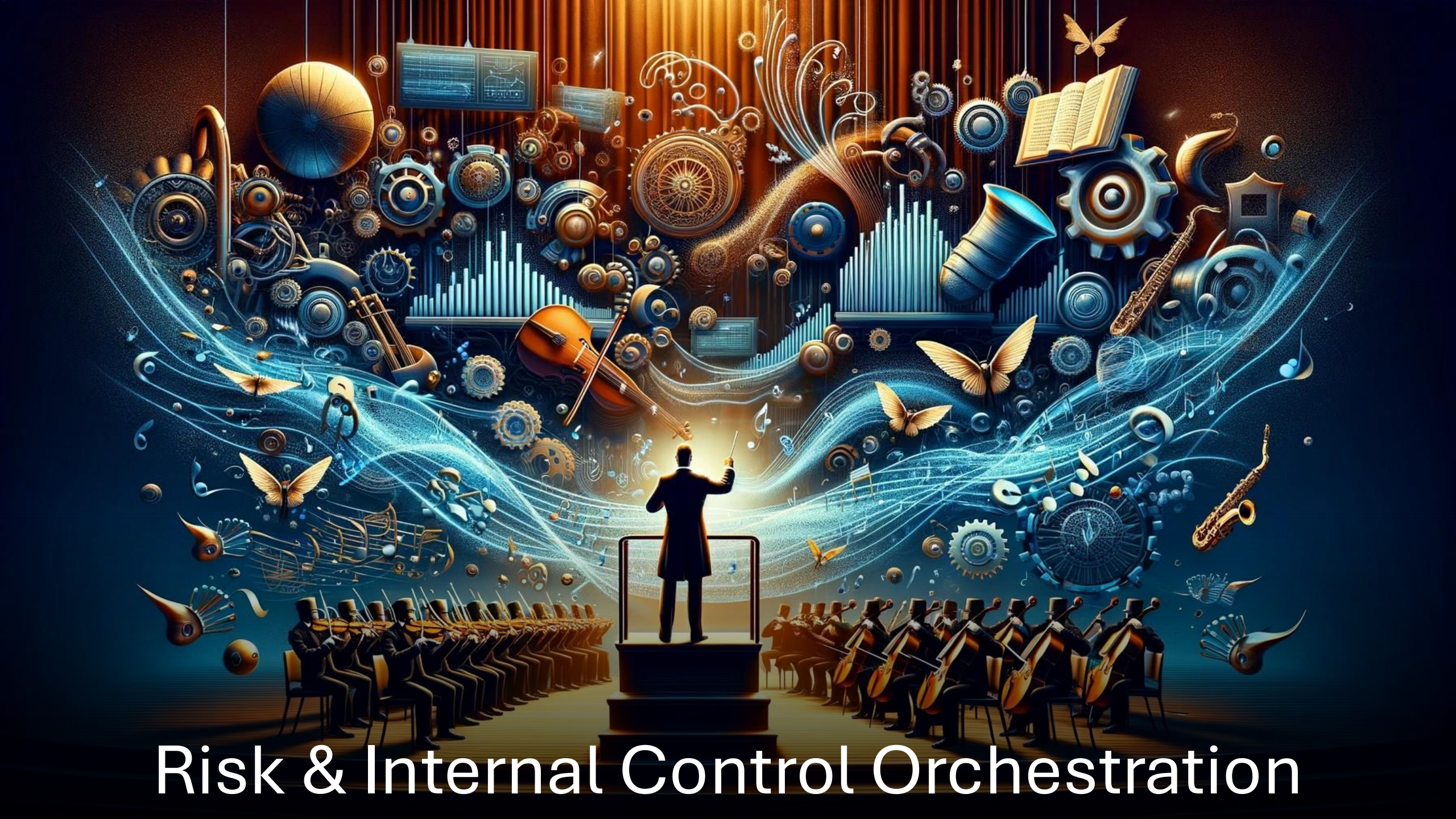
- Risk & Control Management Strategy
- Risk & Control Management Process
- Risk & Control Management Information
- Risk & Control Management Technology

Risk & Internal Control: Strategic to operational



The Rhythm of Risk & Control

Managing Risk in the Cycles & Patterns of Business


Risk & Internal Control Orchestration

Three Levels of Risk & Resilience Management

Strategic Risk & Resilience Management (Decisions)

This level of risk management is forward-looking, deeply integrated with all levels of management in making decisions that lead to establishment of objectives. It's not just about protecting strategy: it is about shaping strategy through risk-informed intelligence. It's where risk becomes a strategic asset.

Objective-Centric Risk & Resilience Management (ERM)

This is the level where risk management becomes proactive, integrated, and performance-aligned. Risk is not managed in a vacuum but is directly linked to the organization's ability to achieve objectives.

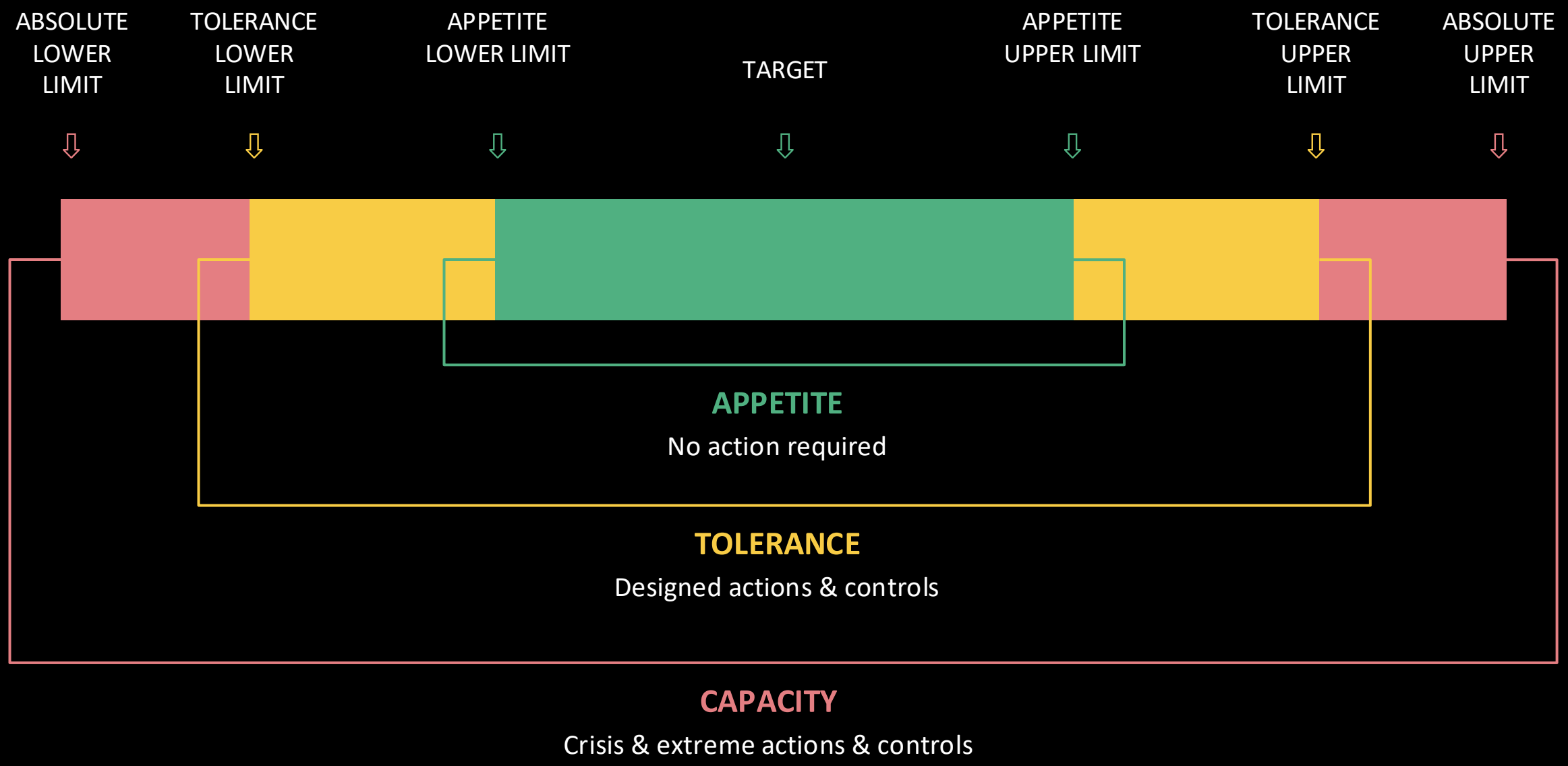
Operational Risk & Resilience Management (ORM)

Operational risk and resilience provides the foundation that enables strategy and objectives to succeed by ensuring reliable, efficient, and adaptable day-to-day operations. Far from being purely defensive, it strengthens confidence in execution, safeguards stakeholders, and creates the stability needed for the organization to perform today while preparing for tomorrow.

Strategic Risk & Resilience Management (Decisions)

Objective-Centric Risk & Resilience Management

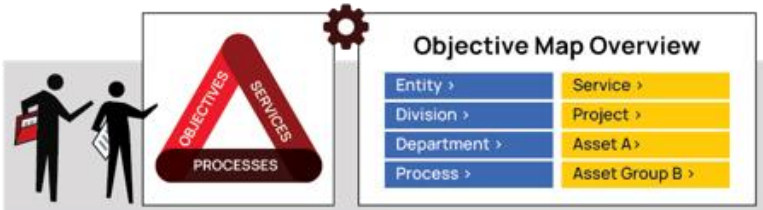
Operational Risk & Resilience Management


ABSOLUTE LOWER LIMIT
TOLERANCE LOWER LIMIT
APPETITE LOWER LIMIT
TARGET
APPETITE UPPER LIMIT
TOLERANCE UPPER LIMIT
ABSOLUTE UPPER LIMIT
APPETITE
No action required
TOLERANCE
Designed actions & controls
CAPACITY
Crisis & extreme actions & controls

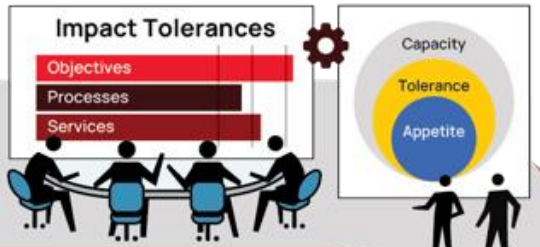
Source: OCEG

What Risk & Resilience Solutions Deliver

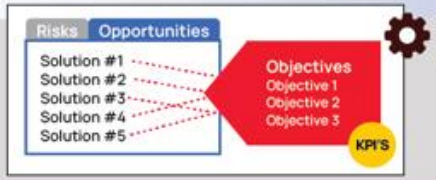
1 Objective, Process & Service Identification
Risk is the measure of the negative, unfavorable effect of uncertainty on objectives. Fully define, map and model its business processes and services to understand risk and resiliency in the organization's operations.



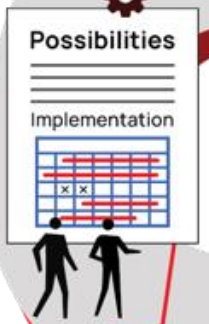
2 Establish Impact Tolerances
Clearly define impact tolerances for objectives, processes, and services. Determine the level and type of risk the organization is willing to address given the level and type of reward it pursues.



3 Risk Identification
Automate a standard, objective approach to identifying opportunities and risks that are evolving and impact the overall objectives and performance of the organization.

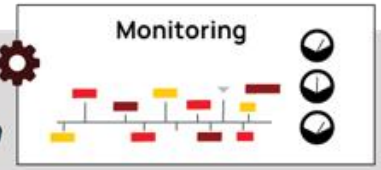


4 Risk Assessment
Identify the possibilities of outcomes possible impact on achievement of objectives. This includes a variety of risk analysis and assessment techniques (e.g., bow-tie risk assessments, scenario analysis, monte carlo).

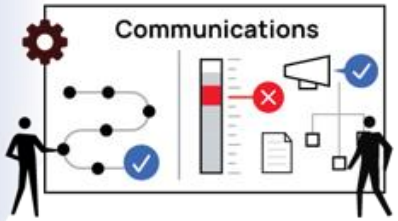


5 Risk Treatment
Drive activities to understand inherent and residual risk while looking at strategies for risk acceptance, risk transfer (insurance), risk avoidance, or risk mitigation (controls). The goal is to optimize value and return while keeping risk within acceptable tolerance and appetite levels.

6 Risk and Resilience Monitoring
Apply a range of processes to monitor risks continuously in the organization. These activities are the ones typically done within the organization to monitor and assess risks on an ongoing basis.

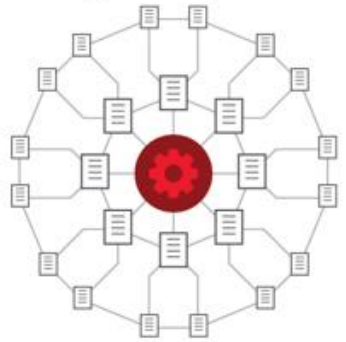


7 Risk and Resilience Communications & Attestations
Run ongoing processes to manage communication and interactions with risk owners. These are done periodically, or when certain risk conditions are triggered.



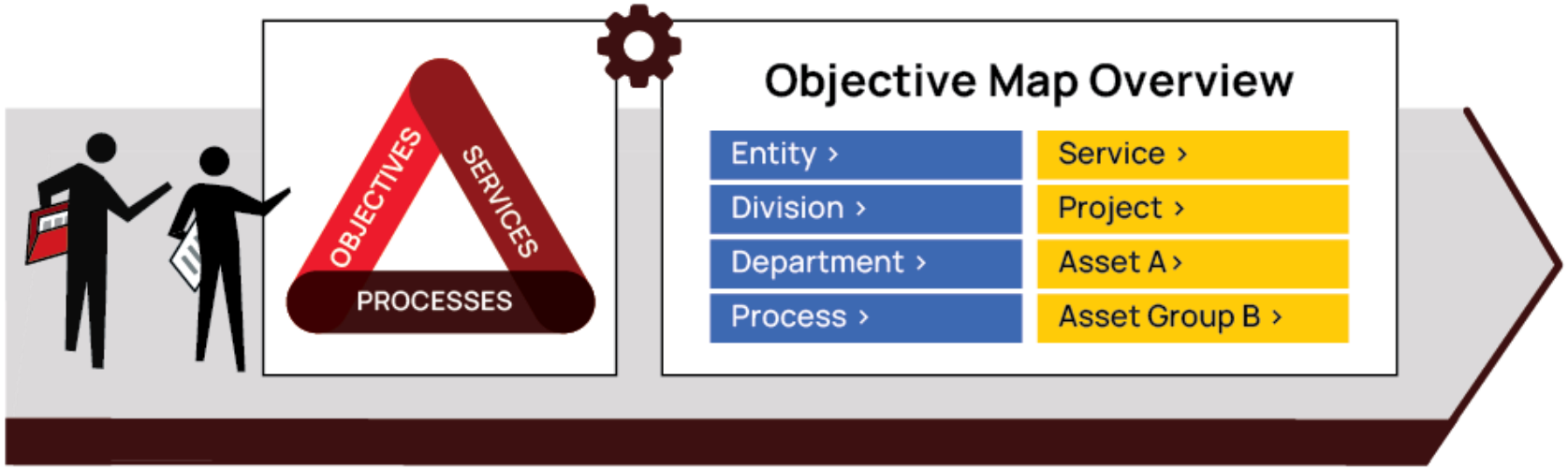
FUTURE STATE

Automated Processes, Integrated Systems



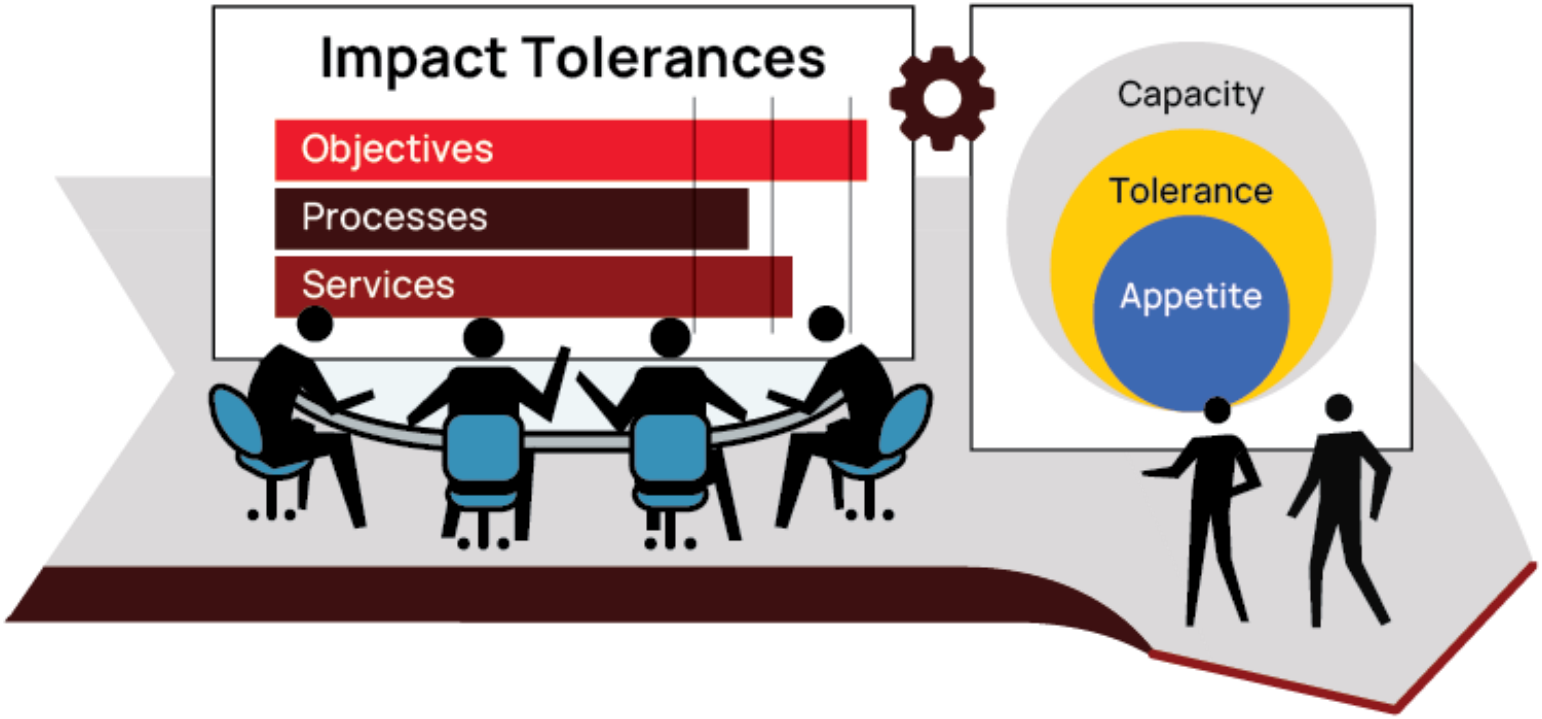
1 Objective, Process & Service Identification

Risk is the measure of the negative, unfavorable effect of uncertainty on objectives. Fully define, map and model its business processes and services to understand risk and resiliency in the organization's operations.



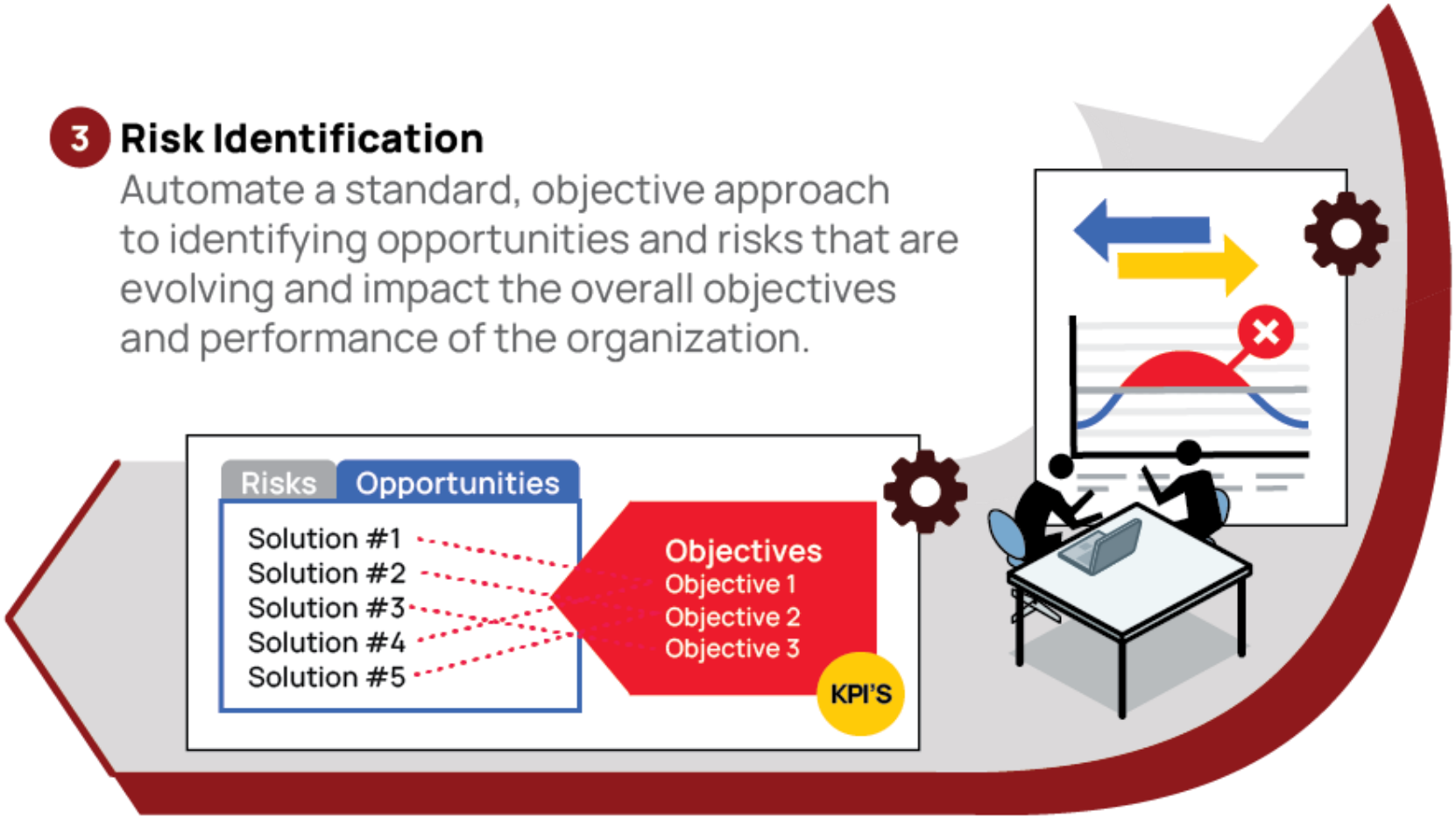
2 Establish Impact Tolerances

Clearly define impact tolerances for objectives, processes, and services. Determine the level and type of risk the organization is willing to address given the level and type of reward it pursues.



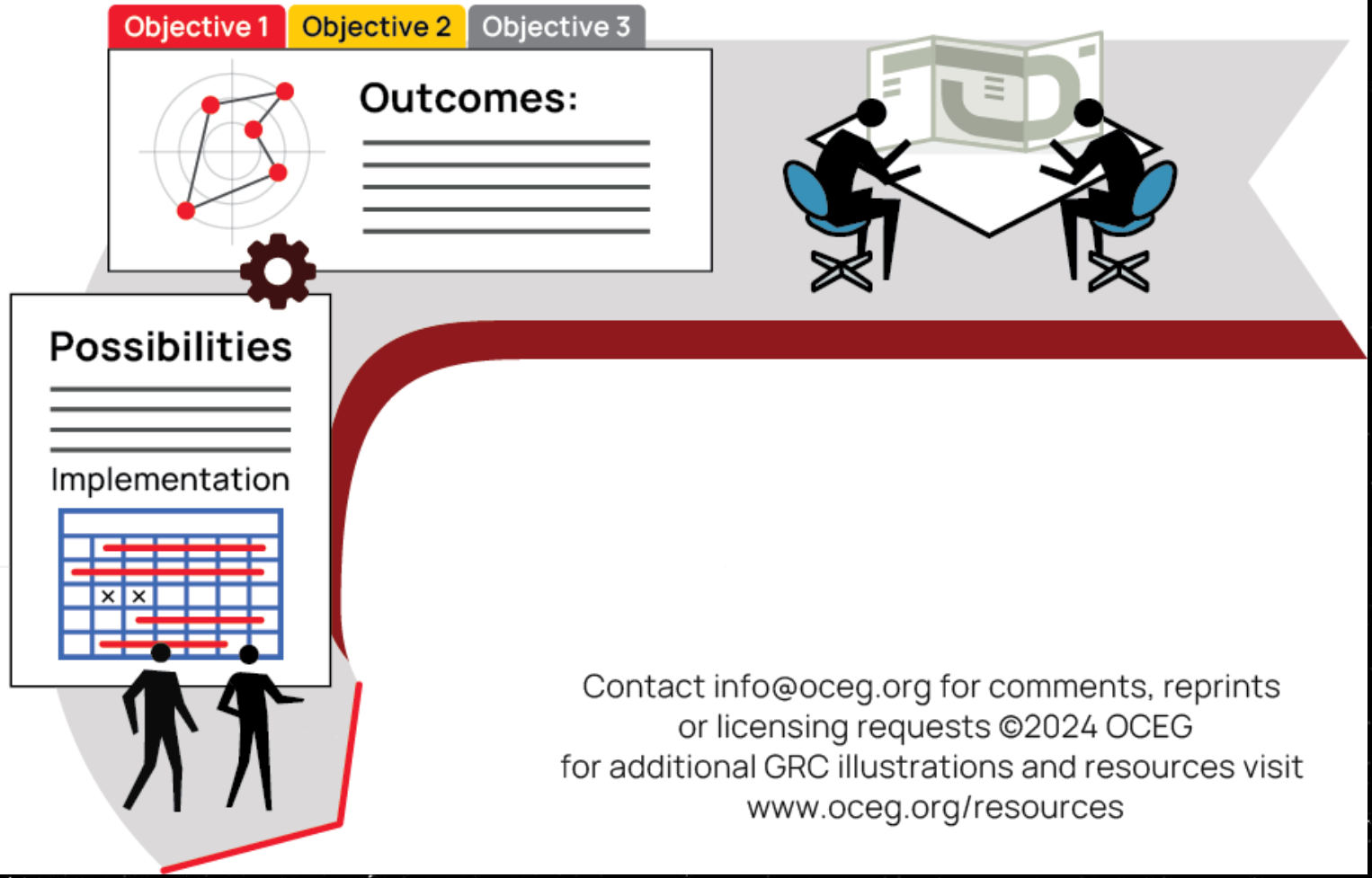
3 Risk Identification

Automate a standard, objective approach to identifying opportunities and risks that are evolving and impact the overall objectives and performance of the organization.



4 Risk Assessment

Identify the possibilities of outcomes possible impact on achievement of objectives. This includes a variety of risk analysis and assessment techniques (e.g., bow-tie risk assessments, scenario analysis, monte carlo).

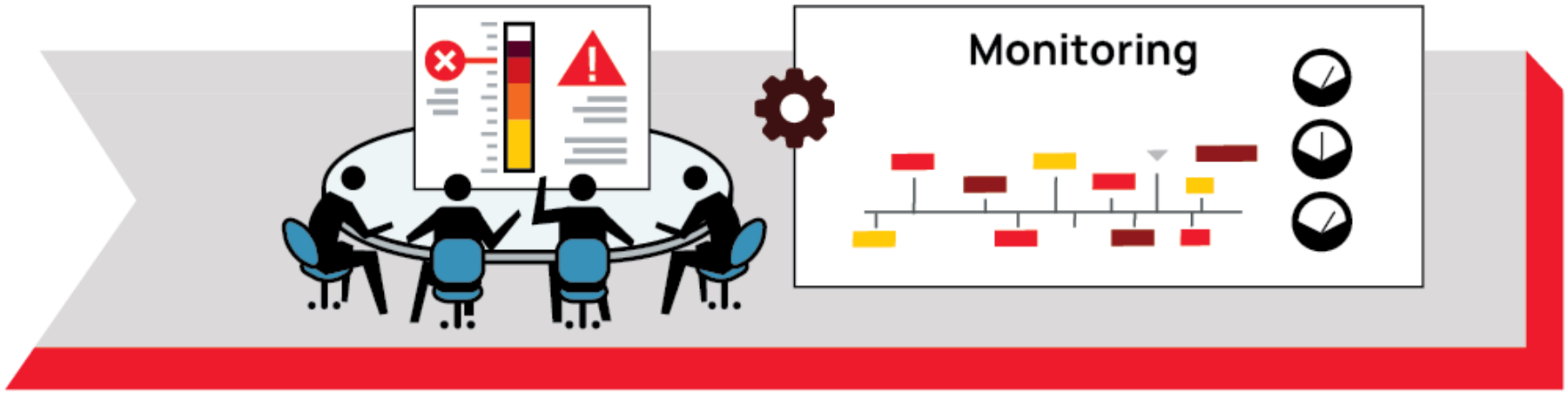


5 Risk Treatment

Drive activities to understand inherent and residual risk while looking at strategies for risk acceptance, risk transfer (insurance), risk avoidance, or risk mitigation (controls). The goal is to optimize value and return while keeping risk within acceptable tolerance and appetite levels.

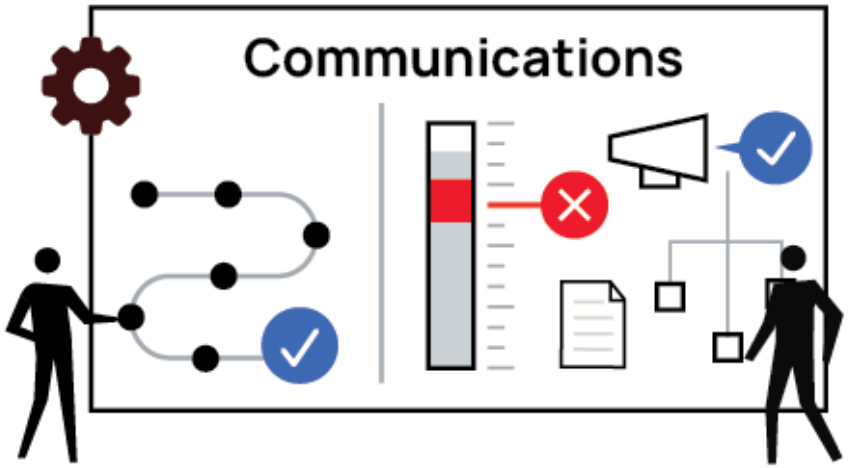
6 Risk and Resilience Monitoring

Apply a range of processes to monitor risks continuously in the organization. These activities are the ones typically done within the organization to monitor and assess risks on an ongoing basis.



7 Risk and Resilience Communications & Attestations

Run ongoing processes to manage communication and interactions with risk owners. These are done periodically, or when certain risk conditions are triggered.



GRC Technology Illustrated Series

Internal Control Management, Monitoring & Automation Solutions

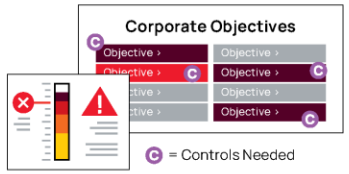
Internal Control Management, Monitoring & Automation Solutions streamline an organization's GRC management by automating the definition, documentation, and continuous monitoring of internal controls across processes and systems. These tools simplify assessments and reporting, and enable real-time enforcement and testing of controls, ensuring effectiveness and compliance.

DEVELOPED BY oceg

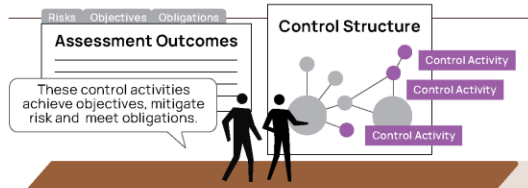
WITH CONTRIBUTIONS FROM grc 2020 Diligent

What Internal Control Management, Monitoring & Automation Solutions Deliver

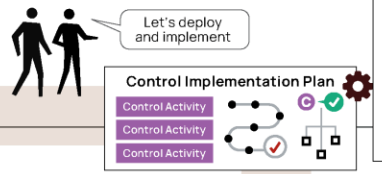
1 Objective, Risk & Obligation Assessment
Identify and prioritize corporate objectives and areas of highest risk that impact where controls are needed to reliably achieve objectives, address uncertainty, and act with integrity.

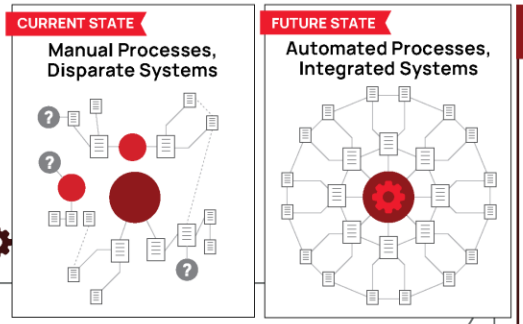


2 Control Environment Establishment
Define and document the control structure aligned with the Objective, Risk & Obligation Assessment outcomes. Develop specific control activities to effectively meet objectives, mitigate risks/uncertainty, and meet obligations.



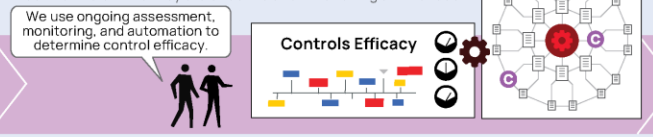
3 Control Implementation
Deploy the designed control activities into the operational environment.



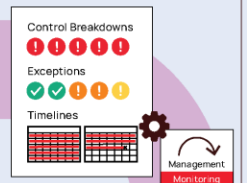


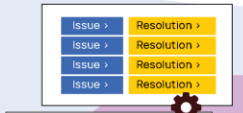
OPERATIONAL ENVIRONMENT

4 Control Automation
Integrate monitoring and automation tools with existing systems and processes. Continuously and periodically test the controls to ensure they are effective and functioning as intended.

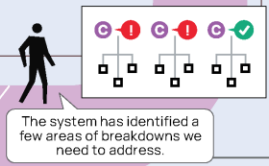


5 Data Analysis and Review
Utilize automated tools to analyze data for signs of control breakdowns or exceptions.

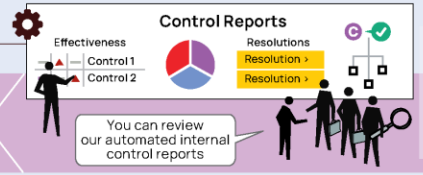




6 Reporting
Generate and review internal control reports on the effectiveness of internal controls for management and external parties.



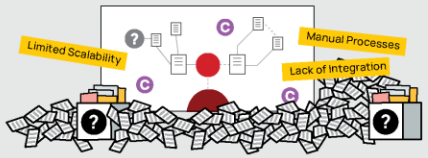
7 Issue Identification and Resolution
Detect and address any control failures or weaknesses through automated alerts.



8 Continuous Improvement
Regularly update and refine internal controls and monitoring systems in response to changes in objective, risk, and obligation assessment and technological advancements.

Top Challenges

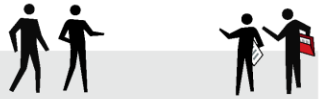
- Scattered Silos of Internal Control Management
- Manual Processes with Documents & Emails
- Manual Testing
- Manual Control Updates from Control Owners
- Failure to Have Enterprise Visibility of Controls
- Lack of Automated Control Monitoring & Enforcement
- Complexity of Regulatory Compliance
- Integration with Existing Systems
- Data Quality & Accuracy
- Change Management Impact on Controls
- Limited Scalability
- Evolving Technology



Address these challenges by transitioning to an integrated internal control management, monitoring, and automation solution that provides a unified view of controls, streamlines workflows and automation, and delivers greater efficiency, effectiveness, resilience, and agility to the organization.

Critical Capabilities

- Enterprise visibility of controls
- Business process and service view of controls
- Controls in context of objectives, risk, obligations
- Real-time control identification
- Automated and continuous control monitoring and enforcement
- Advanced control data analytics
- Seamless business system integration
- Scalability and flexibility
- Robust audit trail creation
- Customizable reporting and dashboards
- Control issue/incident management
- Workflow and task management with automated notifications
- Predictive control modeling
- Control effectiveness testing
- Business portal to collaborate on controls



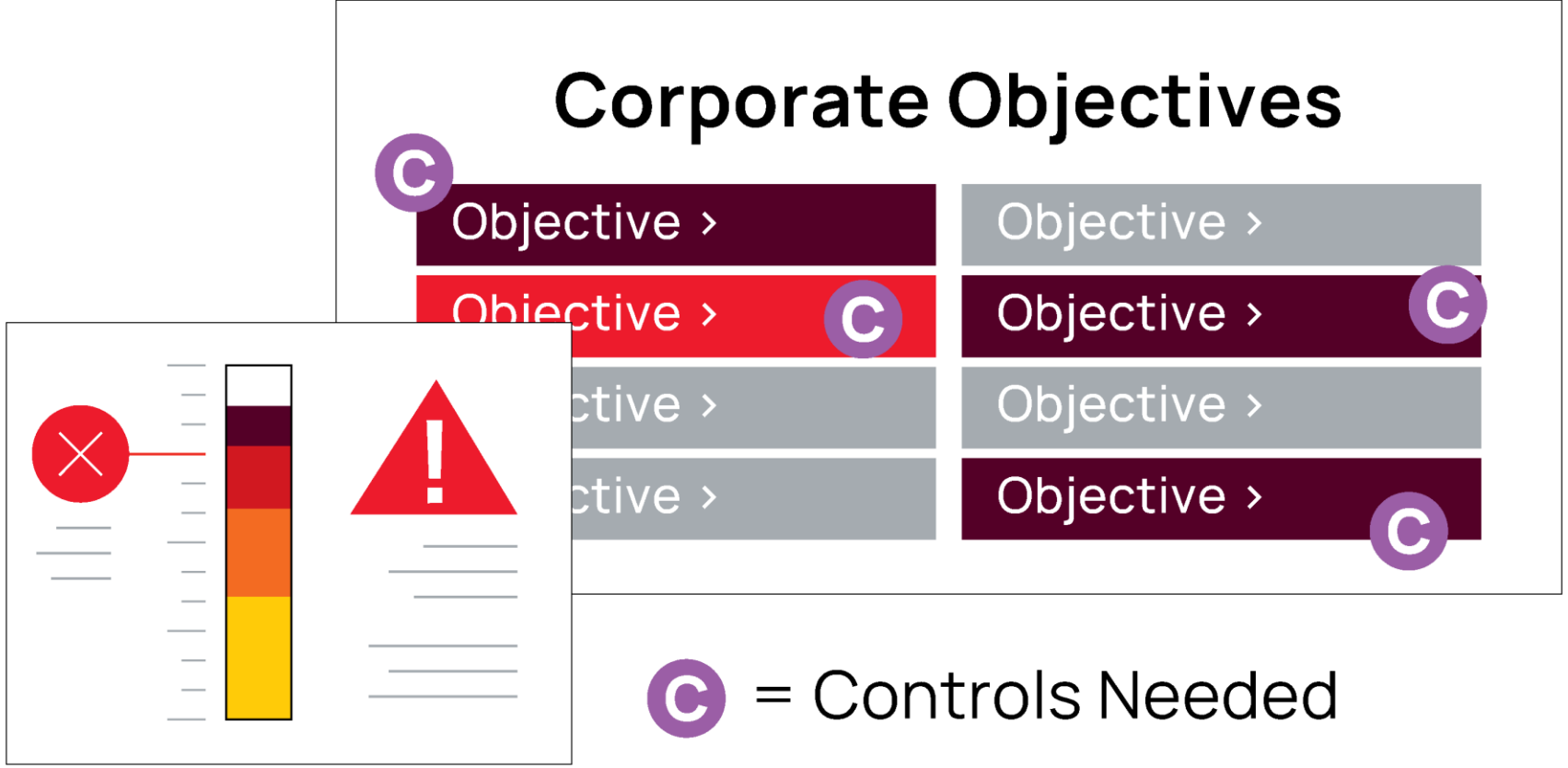
Building Your Business Case for Internal Control Management, Monitoring & Automation Solutions

Efficiency
The right internal control management, monitoring, and automation solution will save time and money (human capital and financial capital costs).

Effectiveness
The right internal control management, monitoring, and automation solution will see fewer things slipping through the cracks and greater management and accountability of internal controls.

Resilience
The right internal control management, monitoring, and automation solution will enable the organization to identify and contain control issues, minimizing exposure to the organization.

Agility
The right internal control management, monitoring, and automation solutions will enable the organization to keep controls current in the context of changing obligations, risks, and business objectives and processes.



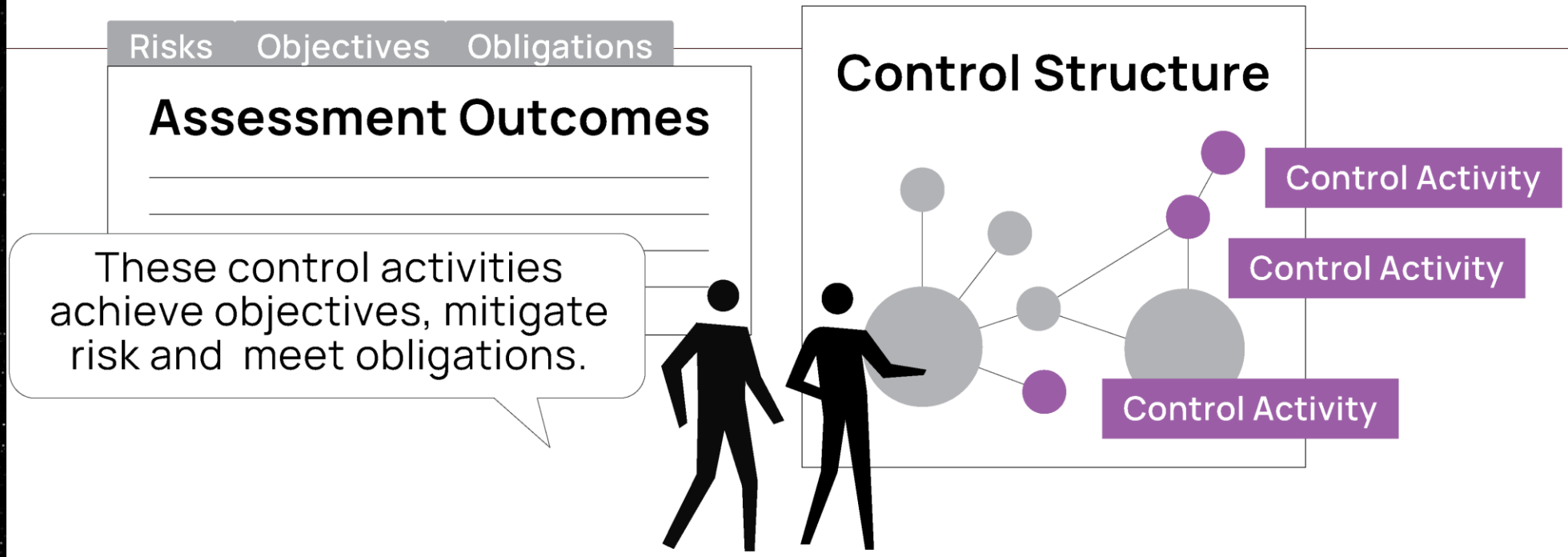
C = Controls Needed

1 Objective, Risk & Obligation Assessment

Identify and prioritize corporate objectives and areas of highest risk that impact where controls are needed to reliably achieve objectives, address uncertainty, and act with integrity.

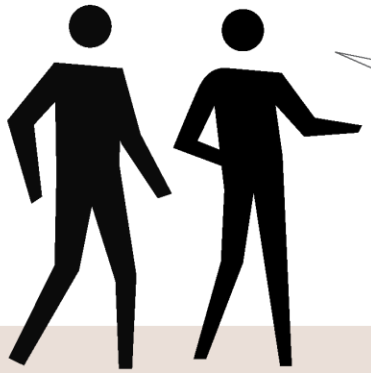
2 Control Environment Establishment

Define and document the control structure aligned with the Objective, Risk & Obligation Assessment outcomes. Develop specific control activities to effectively meet objectives, mitigate risks/uncertainty, and meet obligations.



3 Control Implementation

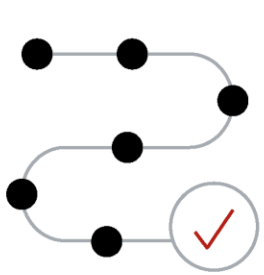
Deploy the designed control activities into the operational environment.

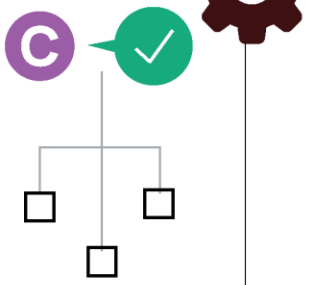


Let's deploy and implement

Control Implementation Plan

- Control Activity
- Control Activity
- Control Activity

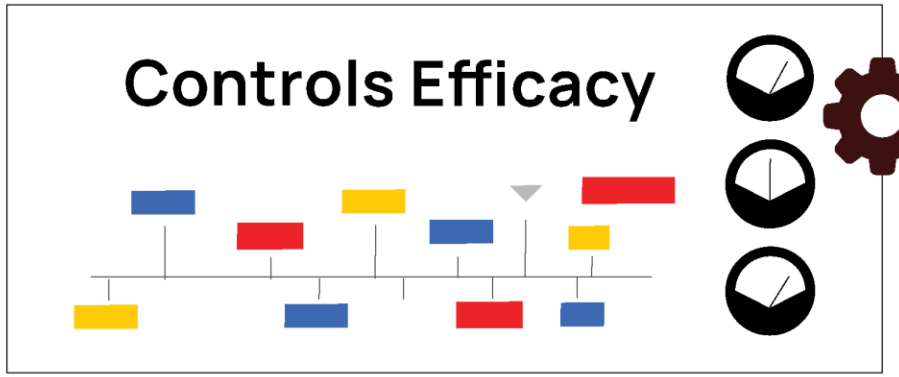


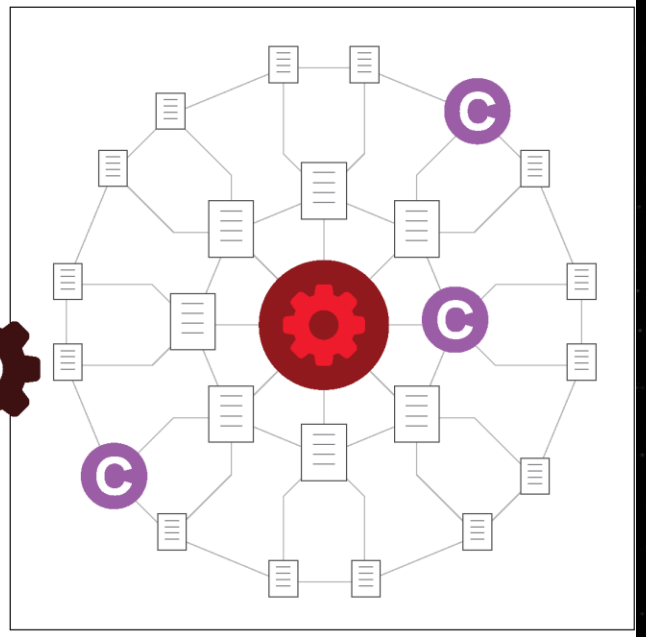


4 Control Automation

Integrate monitoring and automation tools with existing systems and processes. Continuously and periodically test the controls to ensure they are effective and functioning as intended.

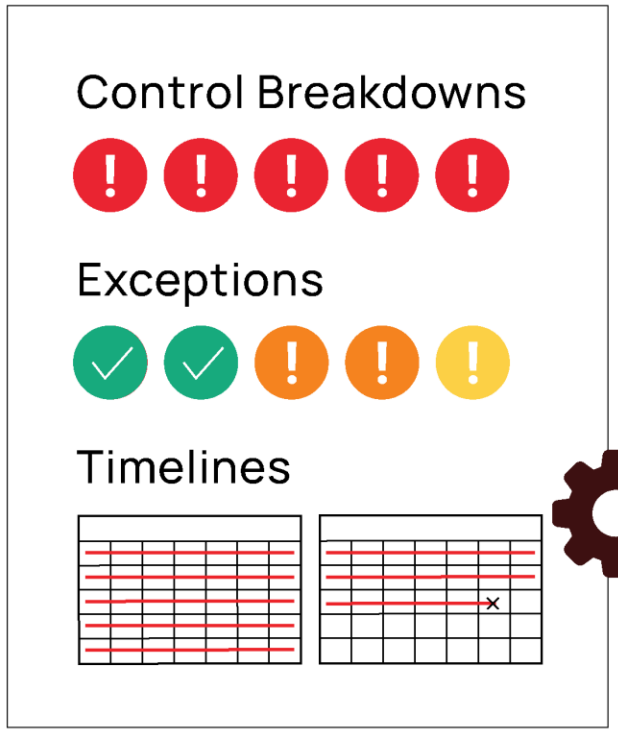
We use ongoing assessment, monitoring, and automation to determine control efficacy.

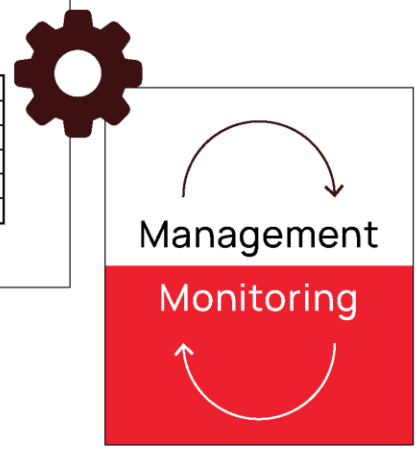


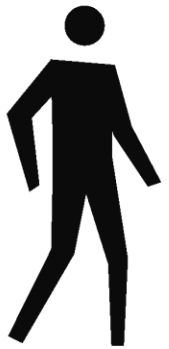


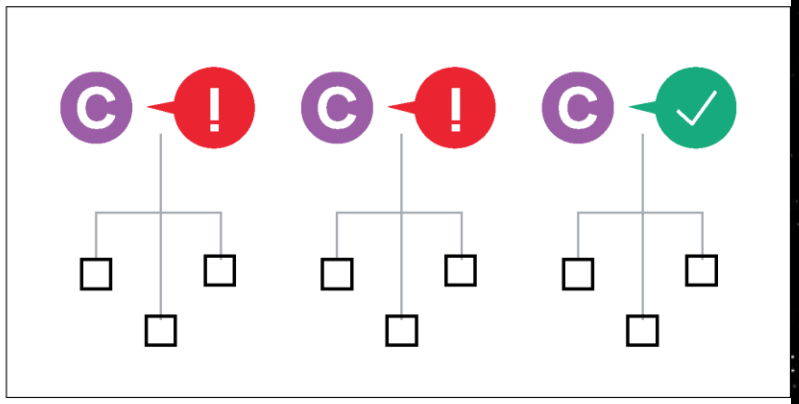
5 Data Analysis and Review

Utilize automated tools to analyze data for signs of control breakdowns or exceptions.









The system has identified a few areas of breakdowns we need to address.

Control Reports

Effectiveness

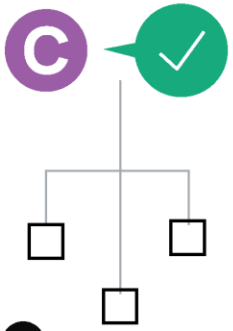
Control 1

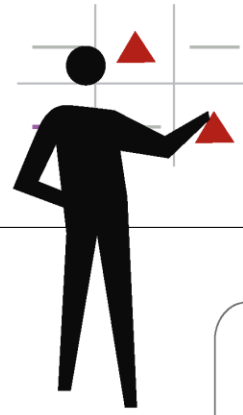
Control 2

Resolutions

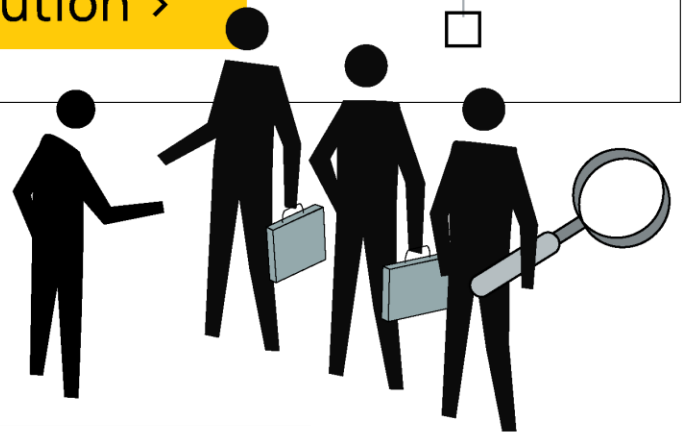
Resolution ›

Resolution ›



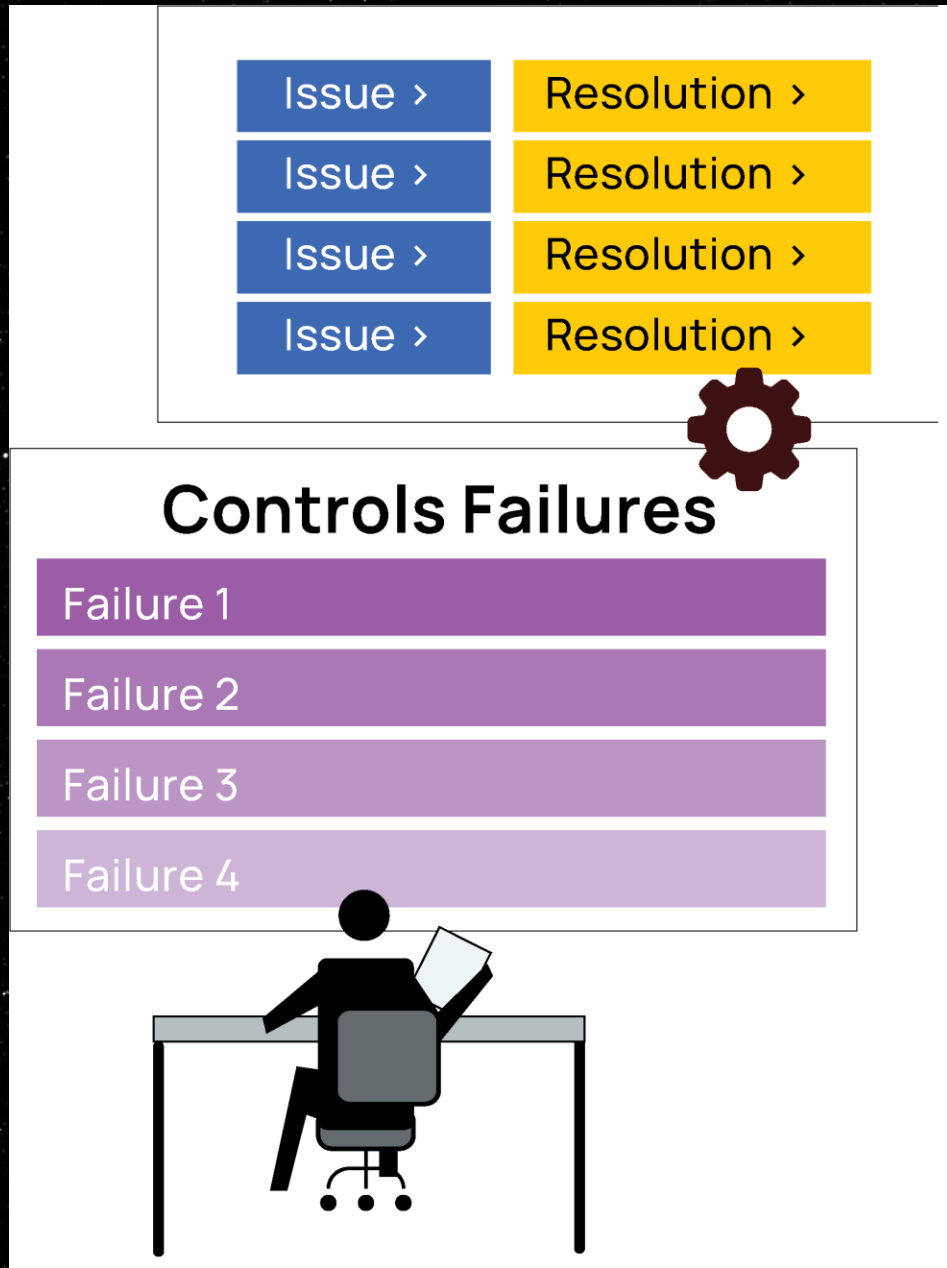


You can review our automated internal control reports



6 Reporting

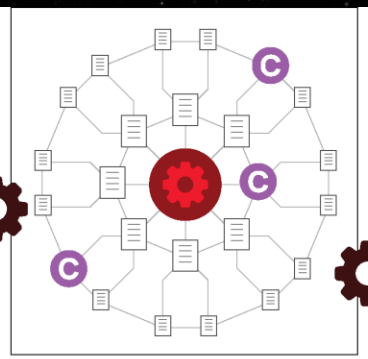
Generate and review internal control reports on the effectiveness of internal controls for management and external parties.

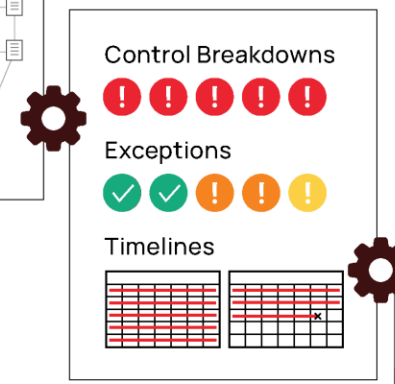


7 Issue Identification and Resolution

Detect and address any control failures or weaknesses through automated alerts.

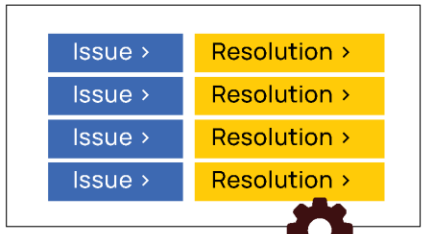
We use ongoing assessment, monitoring, and automation to determine control efficacy.

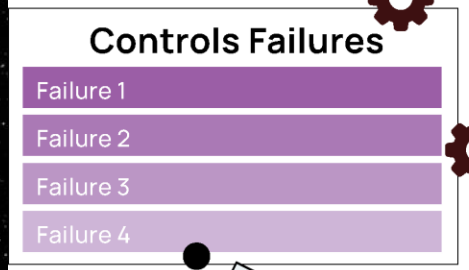


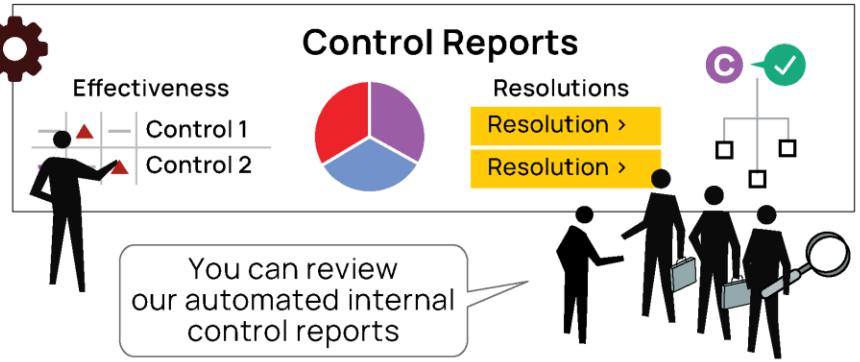


8 Continuous Improvement

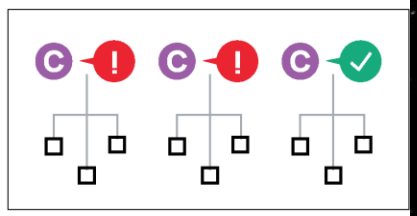
Regularly update and refine internal controls and monitoring systems in response to changes in objective, risk, and obligation assessment and technological advancements.







You can review our automated internal control reports

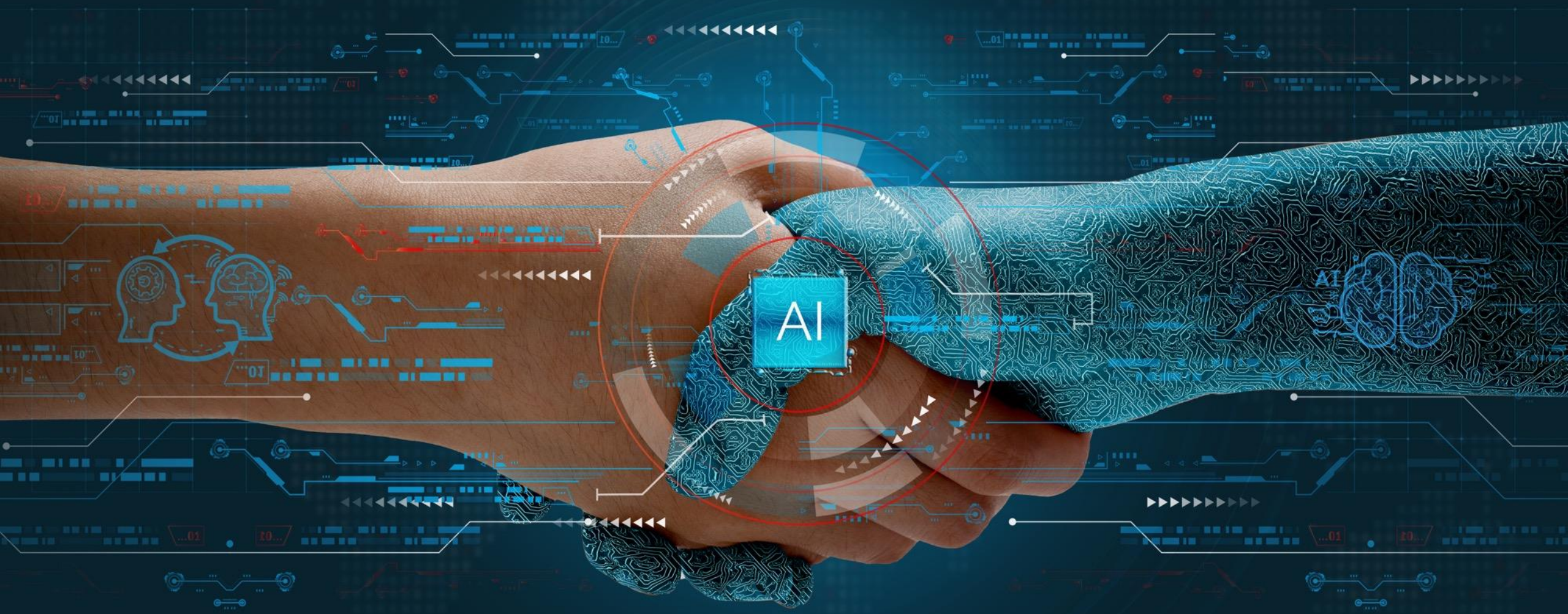


The system has identified a few areas of breakdowns we need to address.

360° Situational Awareness of Risk & Control


From System of Record to Homeostatic Risk & Control

AI Is Reshaping Risk & Control: But We Must Be Wise



Risk & Control Scenario Analysis & Stress Testing

Digital Twins in Risk & Control Management

Critical Capabilities

- Overall risk and resilience program management
- Support for strategic, enterprise, and operational risk and resilience
- 360° contextual awareness of risks to objectives
- Risk identification, analysis, treatment & monitoring
- Identify objectives, processes, services
- Understand & map risk relationships
- Establish impact tolerances and risk appetite
- Scenario & business impact analysis, risk forecasting, and planning
- Risk quantification, normalization & aggregation
- Allocate risk accountability
- Advanced risk reporting and trending
- Continuity & resilience plan management
- Corrective /Preventive Action Plans
- Crisis & Risk Event Management

Value: It’s More Than Just ROI

Efficiency = Traditional ROI (Time-Saved, Money-Saved)

Efficient risk and resilience is about doing things fast.

But effective risk and resilience is about doing the right things.

Effectiveness = Effectiveness is about actual/measurable risk reduction

If you cannot demonstrate that your risk and resilience program is measurably reducing risk to your objectives, then you are not being effective — just active, perhaps like a hamster on a wheel not truly getting anywhere.

Resilient = Ability to Anticipate and Recover from Incidents & Disruption

Resilience is what keeps a compliance issue from becoming a scandal.

A system failure from becoming a shutdown.

A risk exposure from becoming a crisis.

Agility = Navigating Uncertainty on the Road Ahead

Risk & Control End Game: Business Confidence

Risk & control management should not be the handbrake.

It should be the navigation system — helping the business steer safely through uncertainty toward its objectives.

grc 20/20
Bringing GRC into Focus

Thank You!
Questions?

Michael Rasmussen, The GRC Pundit & Analyst

RISK IS OUR BUSINESS
grc report

- GRC 20/20 Research • www.**GRC2020**.com
- News • The GRC Report • www.**GRCreport**.com
- Podcast • Risk Is Our Business Podcast
- Podcast • Hitchhiker's Guide to the GRC Technology Galaxy
- mkras@grc2020.com • www.linkedin.com/in/mkrasmussen/