Cybersecurity Forum and Workshop 2.0:

Enterprise Risk Management (ERM) Workshop

(Frameworks, Plans, Strategy & Best Practices)

Dr. Nathaniel Atansuyi,
FIIM, MNCS, MCPN (C.itp)
Managing Consultant
Dataplus Global Services Limited

https://www.linkedin.com/in/naths/
natansuyi@dataplusgs.com.ng/
nathansuyi@gmail.com

nigeria computer society

Nigeria records 147% increase in password-stealing malware in three months— Report

Kapersky in its findings published on Monday said small businesses in Nigeria are still in danger of exposure to malware and face an 89 per cent increase in Remote Desktop Protocol attacks in 2022.

https://www.premiumtimesng.com/news/more-news/533691-nigeria-records-147-increase-in-password-stealing-malware-in-three-months-report.html May 30, 2022

Scope

1. Enterprise Risk Management (ERM) Overview
2. Enterprise Risk Management (ERM) Strategy
3. Cyber Security and Enterprise Risk Management (ERM) Integration
4. Governance, Risk Management and Compliance (GRC)
5. Cyber Security Tools

Workshop Objective

Value creation through an appropriate development of frameworks, plans, strategy and best practices of Enterprise Risk Management with tools that mitigate cyber risks and securing data assets by prioritizing investments and maximizing the impact of each kobo spent on cybersecurity.

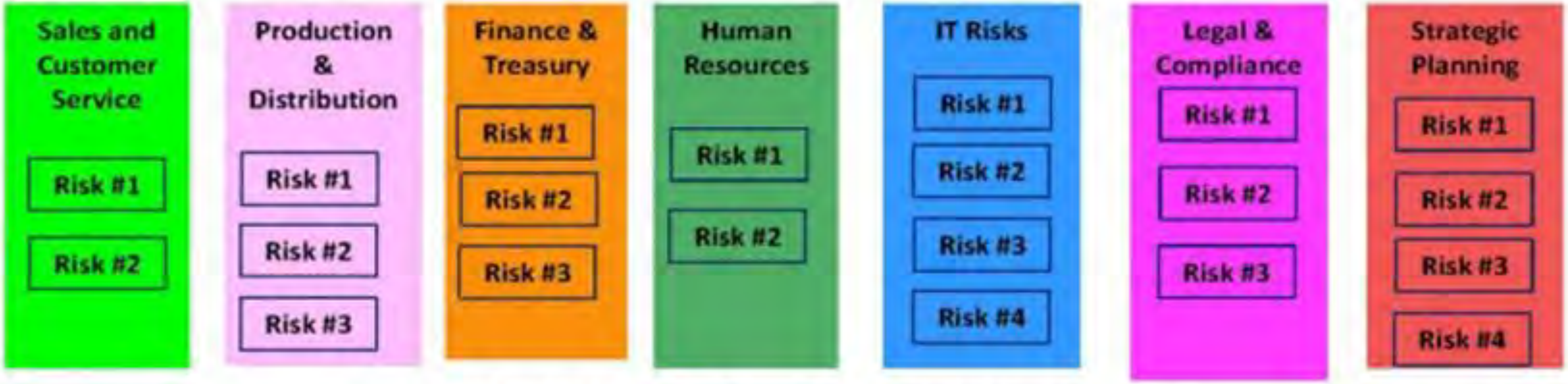
Enterprise Risk Management (ERM) Overview

1

What is Enterprise Risk Management (ERM)?

Enterprise Risk Management (ERM) is the process of identifying and understanding the risks that threaten standard business operations and it involves risk prioritization, as well as the planning and preparation necessary for responding to those risks.

Traditional Risk Management Approach



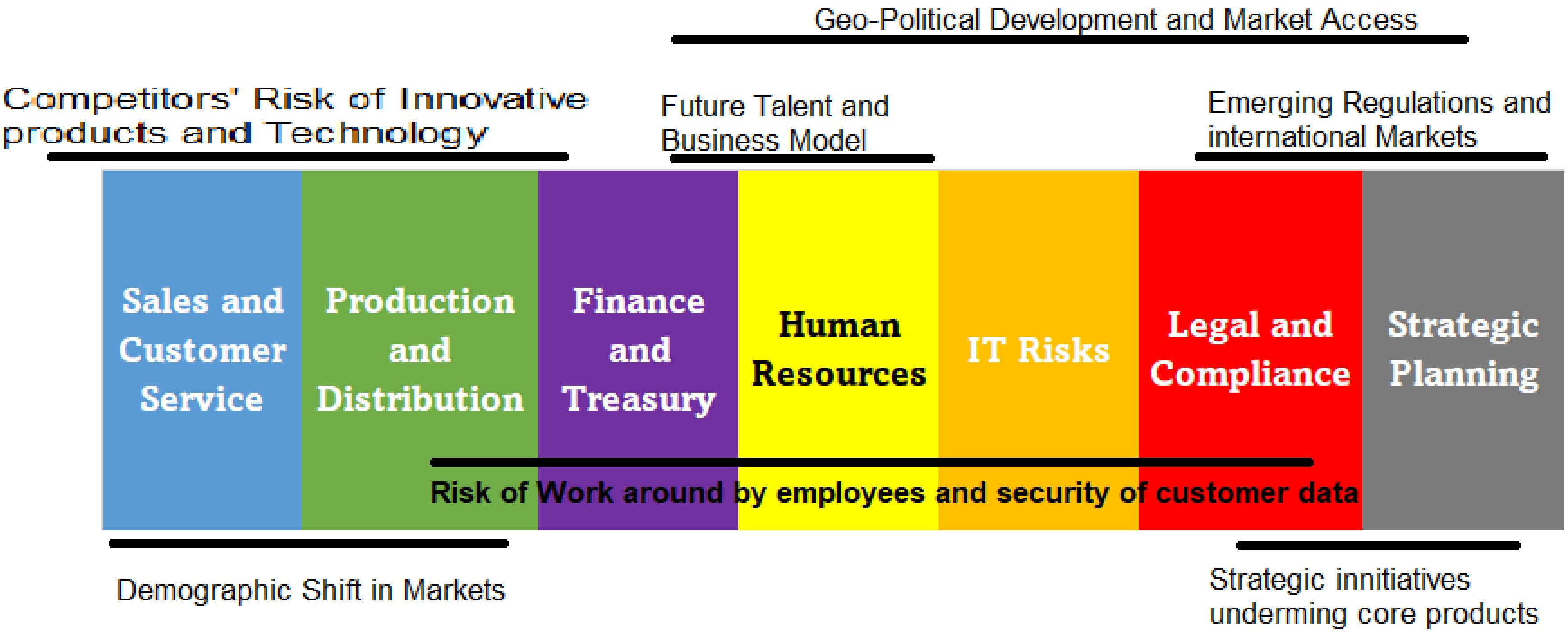
"Silo" or "Stove-Pipe" Risk Management

Limitations:

1. There may be risks that "fall between the siloes" that none of siloes leaders can see.
2. Some risks affect multiple siloes in different ways
3. Individual silo owners may not understand how an individual respond to particular task that might impact the business.
4. In most cases, it focus on internal risk only
5. This approach struggles to connect efforts in risk management to strategic planning

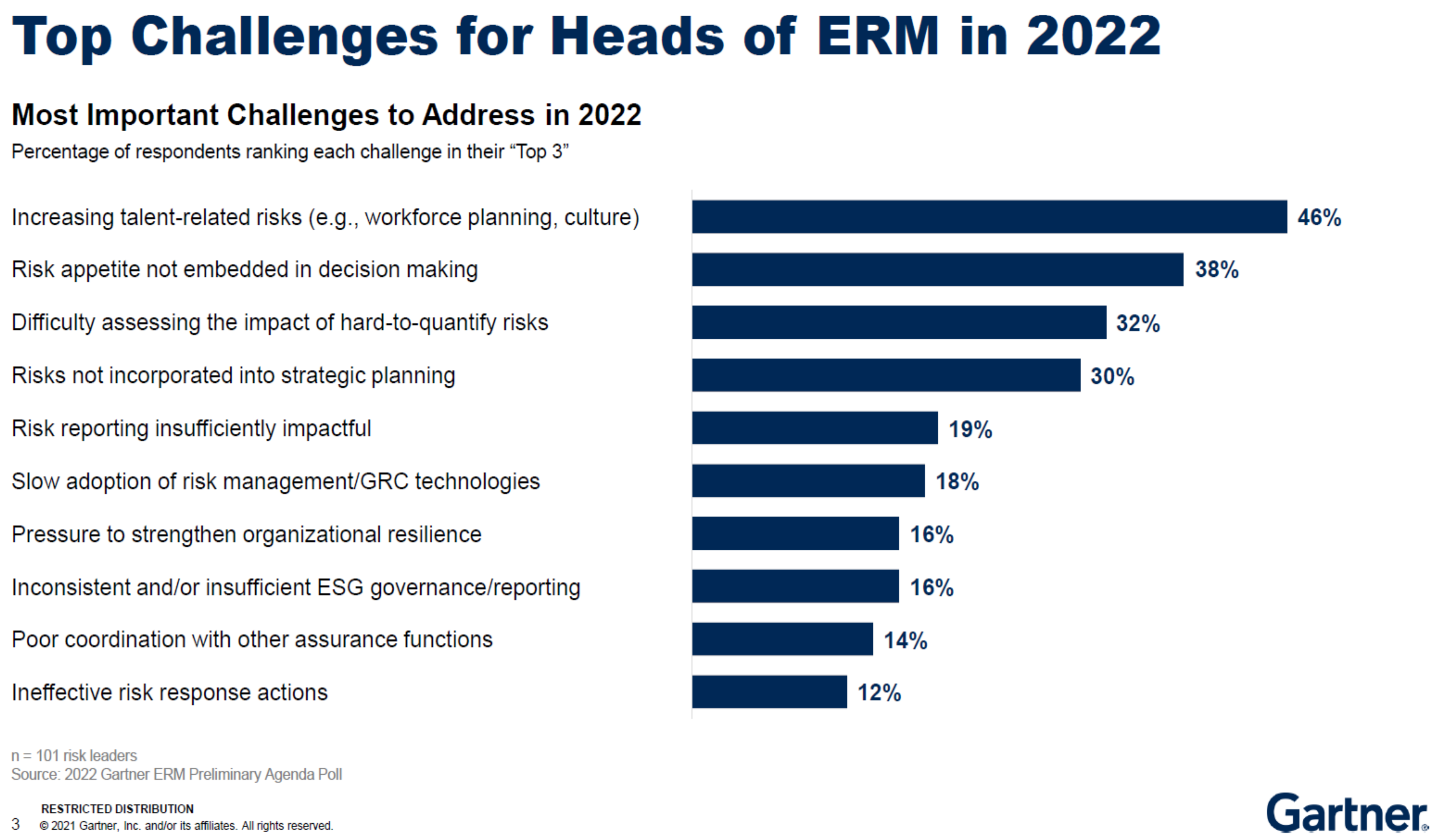
Autnhive
Automating Data Security & Privacy

Embracing Enterprise Risk Management (ERM)


Geo-Political Development and Market Access
Competitors' Risk of Innovative products and Technology
Future Talent and Business Model
Emerging Regulations and international Markets
Sales and Customer Service
Production and Distribution
Finance and Treasury
Human Resources
IT Risks
Legal and Compliance
Strategic Planning
Risk of Work around by employees and security of customer data
Demographic Shift in Markets
Strategic innitiatives underming core products

- ❑ This approach solve the potential shortcomings of the traditional approach by embracing the concept of ERM
- ❑ The concept of ERM as a way to strengthens organization's risk oversight.
- ❑ The key objective of ERM is to develop a holistic, portfolio view of the most significant risks to the achievement of the entity's most important objectives

Understanding the role of ERM



Top Challenges for Heads of ERM in 2022

Most Important Challenges to Address in 2022

Percentage of respondents ranking each challenge in their “Top 3”

Increasing talent-related risks (e.g., workforce planning, culture)	46%
Risk appetite not embedded in decision making	38%
Difficulty assessing the impact of hard-to-quantify risks	32%
Risks not incorporated into strategic planning	30%
Risk reporting insufficiently impactful	19%
Slow adoption of risk management/GRC technologies	18%
Pressure to strengthen organizational resilience	16%
Inconsistent and/or insufficient ESG governance/reporting	16%
Poor coordination with other assurance functions	14%
Ineffective risk response actions	12%

n = 101 risk leaders
Source: 2022 Gartner ERM Preliminary Agenda Poll

RESTRICTED DISTRIBUTION

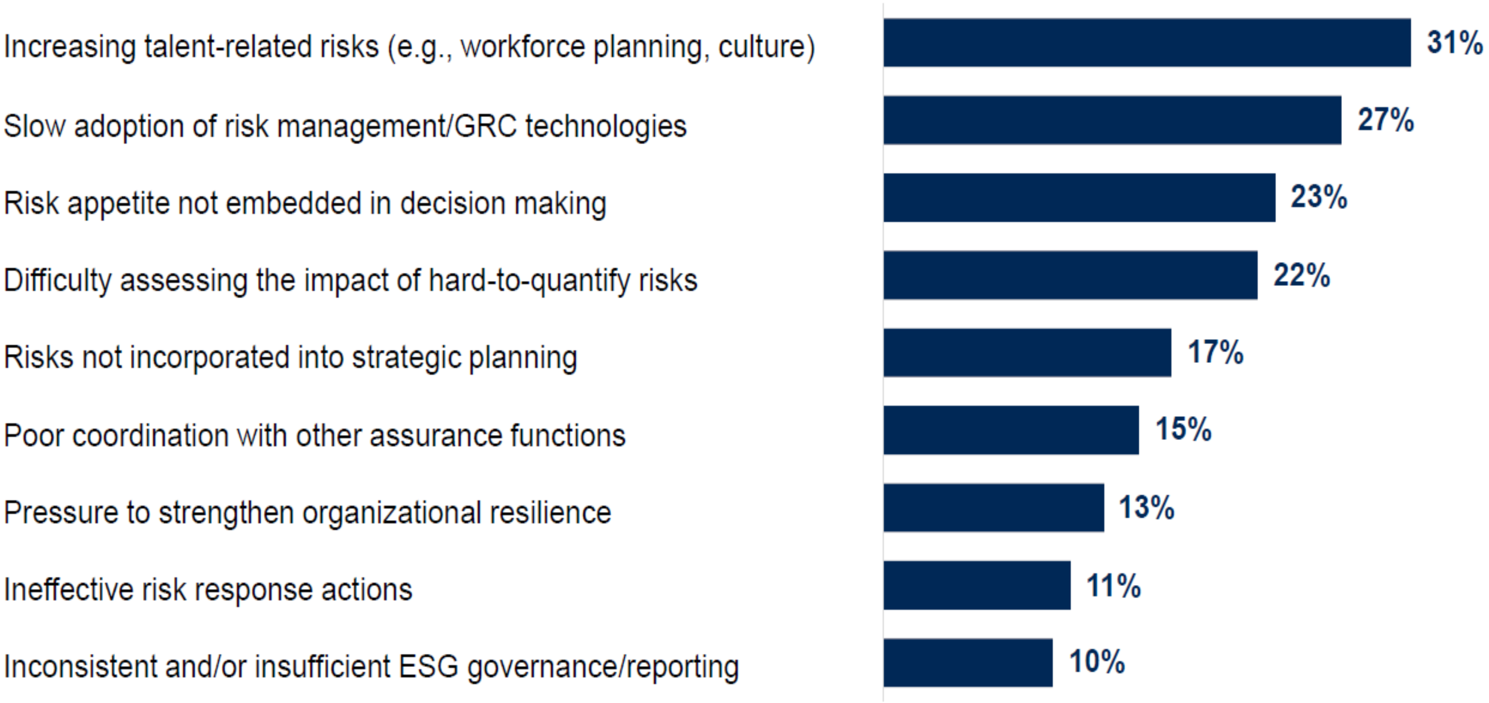
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner.

Areas of Low Confidence for Heads of ERM

Least Confidence in ERM's Current Approach to Solving the Challenge

Percentage of respondents ranking each challenge in their "Top 3"



n = 101 risk leaders
Source: 2022 Gartner ERM Preliminary Agenda Poll

RESTRICTED DISTRIBUTION
© 2021 Gartner, Inc. and/or its affiliates. All rights reserved.

ERM Drivers

The Fundamental Elements of ERM:

❑Assessment of significant risks

❑Implementation of suitable risk responses.

Risk Responses include:

❑Acceptance or tolerance of a risk;

❑Avoidance or termination of a risk;

❑Risk transfer or sharing via insurance,

❑A joint venture or other arrangement; and

❑Reduction or mitigation of risk via internal control procedures or other risk prevention activities.

Other Important ERM Concepts:

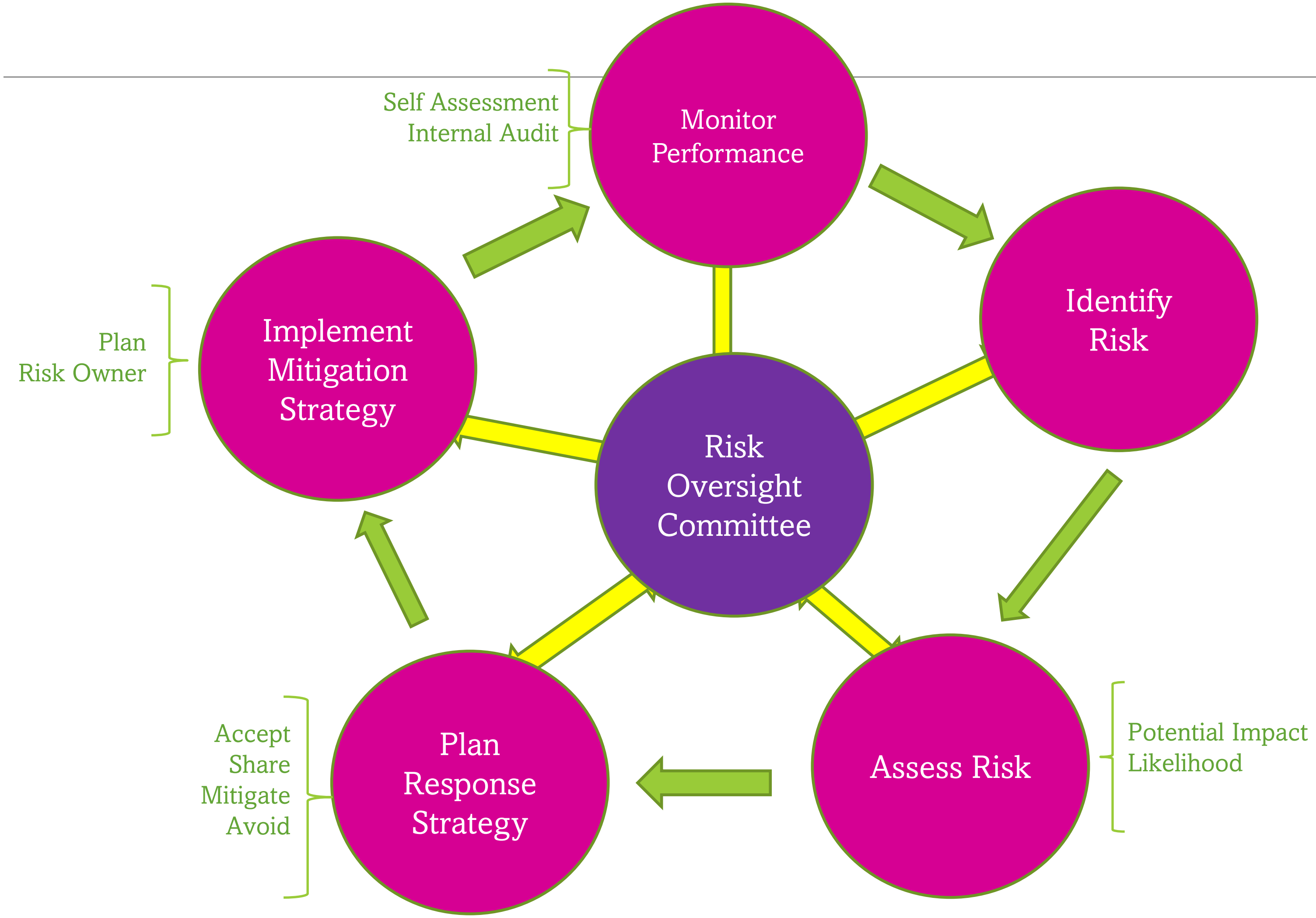
- Risk Philosophy or Risk Strategy,
- Risk Culture and
- Risk Appetite.

These are expressions of the attitude to risk in the organisation, and of the amount of risk that the organisation is willing to take. These are important elements of governance responsibility.

Management Responsibilities:

- Risk Architecture or Infrastructure
- Documentation of Procedures or Risk Management Protocols
- Training
- Monitoring and Reporting on Risks and
- Risk Management Activities.

Risk Management Life Cycle



Monitor Performance

Self Assessment
Internal Audit

Identify Risk

Assess Risk

Potential Impact
Likelihood

Plan Response Strategy

Accept
Share
Mitigate
Avoid

Implement Mitigation Strategy

Plan
Risk Owner

Risk Oversight Committee

Questions before ERM Implementation

- ❑What are the main components or drivers of our business strategy?
- ❑What internal factors or events could impede or derail each of these components?
- ❑What external events could impede or derail each of the components?
- ❑Do we have the right systems and processes in place to address these internal and external risks?

Strategy and business objectives
Risks

Action to take (Dos)

- Gain support of top management and the board
- Engage a broad base of managers and employees in the process
- Start with a few key risks and build ERM incrementally
- Use existing knowledge, skills and resources in management, internal audit, compliance etc.
- Embed ERM into the fabric of the organisation
- Take a holistic, portfolio view of risks across the enterprise

Action to avoid (Don’ts)

- ❑ Never treat ERM as a project – ERM is a process
- ❑ Don’t get bogged down in details and history – ERM should be strategic and forward-looking
- ❑ Avoid relying only on a few key staff – make ERM everyone’s job
- ❑ Don’t take a silo or stove-pipe approach to risks.
- ❑ Don’t ignore how risks might impact on other parts of the business
- ❑ Avoid obsessing too much about categorizing risks – rather than ensuring that the key risks have been identified and mitigation plans developed
- ❑ Never assume that the risk register is complete – there will always be ‘unknown unknowns’ and the biggest enemy of effective ERM is complacency

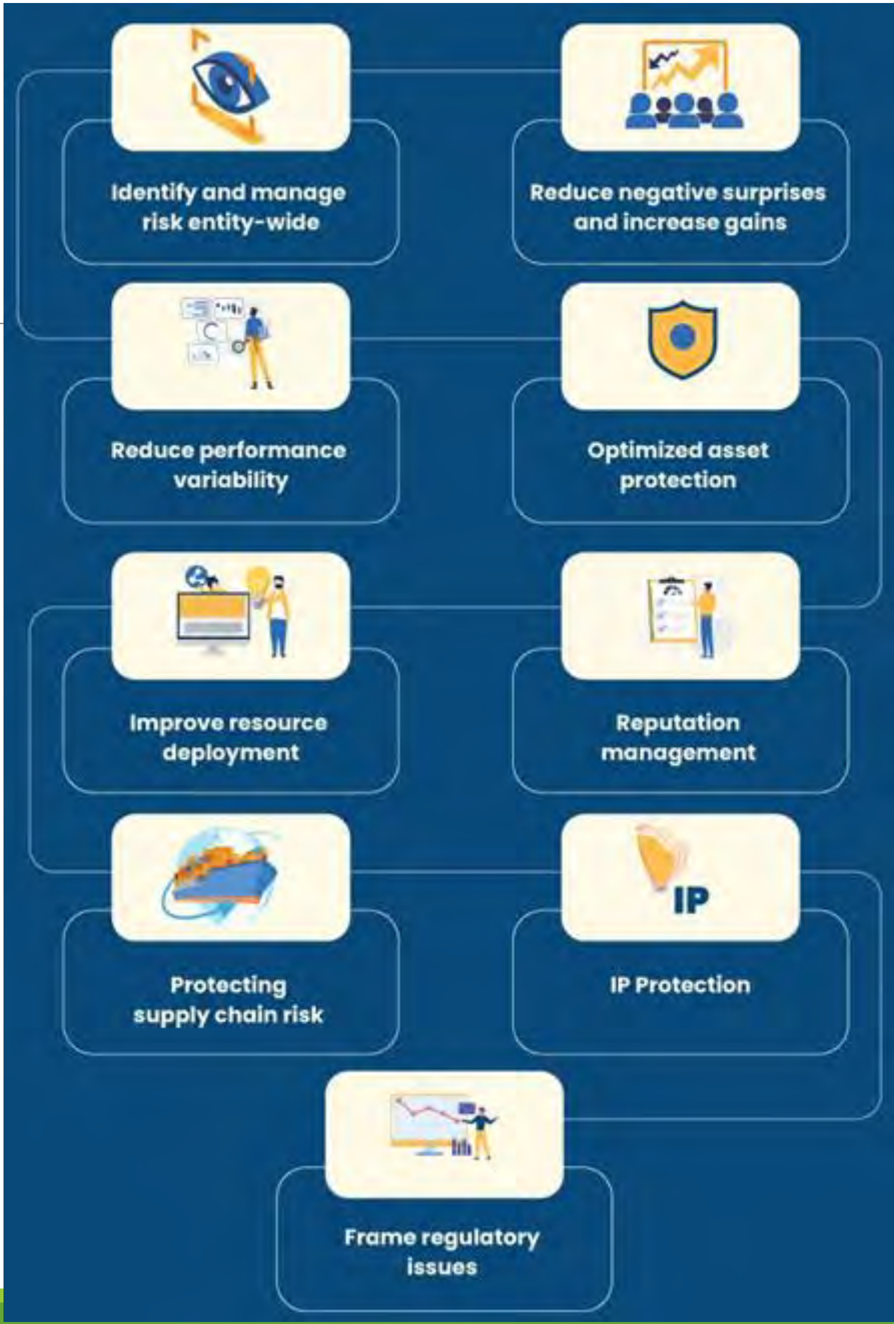
ERM Benefits

❑Greater awareness about the risks facing the organisation and the ability to respond effectively

❑Enhanced confidence about the achievement of strategic objectives

❑Improved compliance with legal, regulatory and reporting requirements

❑Increased efficiency and effectiveness of operations


Identify and manage risk entity-wide
Reduce negative surprises and increase gains
Reduce performance variability
Optimized asset protection
Improve resource deployment
Reputation management
Protecting supply chain risk
IP
IP Protection
Frame regulatory issues

Popular ERM Frameworks by Industry

	Healthcare	IT	Finance	Insurance	Government
ISO 31000	⊕	⊕	⊕	⊕	⊕
COSO	⊕	⊕	⊕	⊕	⊕
J & J ERM	⊕	⊕			
COBIT		⊕			
SOC 2 Type 2		⊕			
CAS		⊕	⊕	⊕	
RIMS				⊕	⊕

Enterprises of all types and sizes face external and internal risks, regardless of industry. However, some ERM frameworks are more prevalent across specific industries due to privacy laws, financial transactions, the regulatory environment, and governance requirements for technology and infrastructure.

ERM Standards and Frameworks (ISO 31000, COSO)

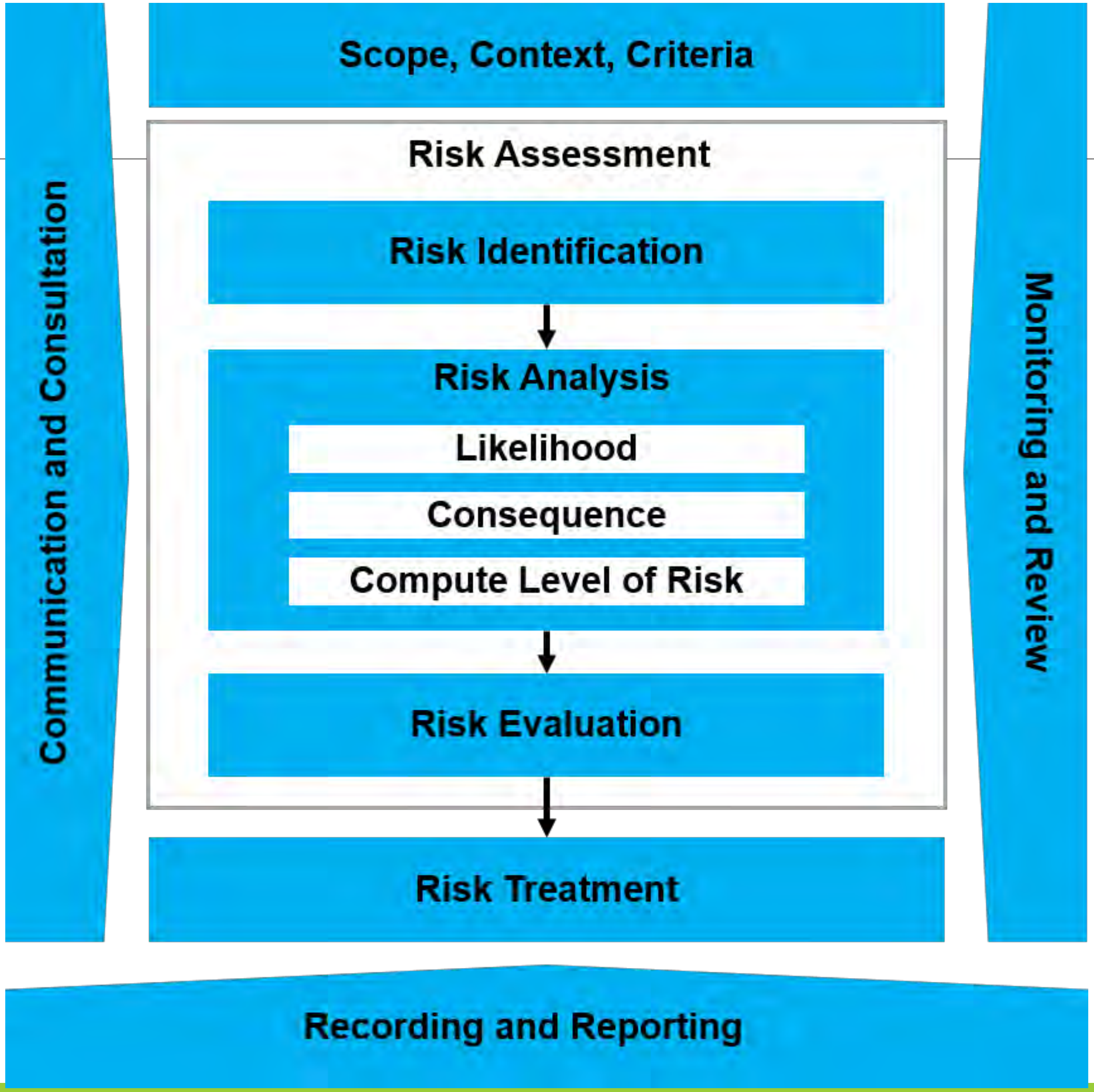
Two widely referenced frameworks:

- ISO 31000: Risk management – Guidelines, provides principles, a framework and a process for managing risk.
- COSO (Committee of Sponsoring Organizations): is to help organizations improve performance by developing thought leadership that enhances internal control, risk management, governance and fraud deterrence.

ISO 31000 Model

The ISO 31000 framework covers various risks and is customizable for organizations, regardless of size, industry, or sector and it is model is reviewed every five years for market evolution and changes to business complexity.

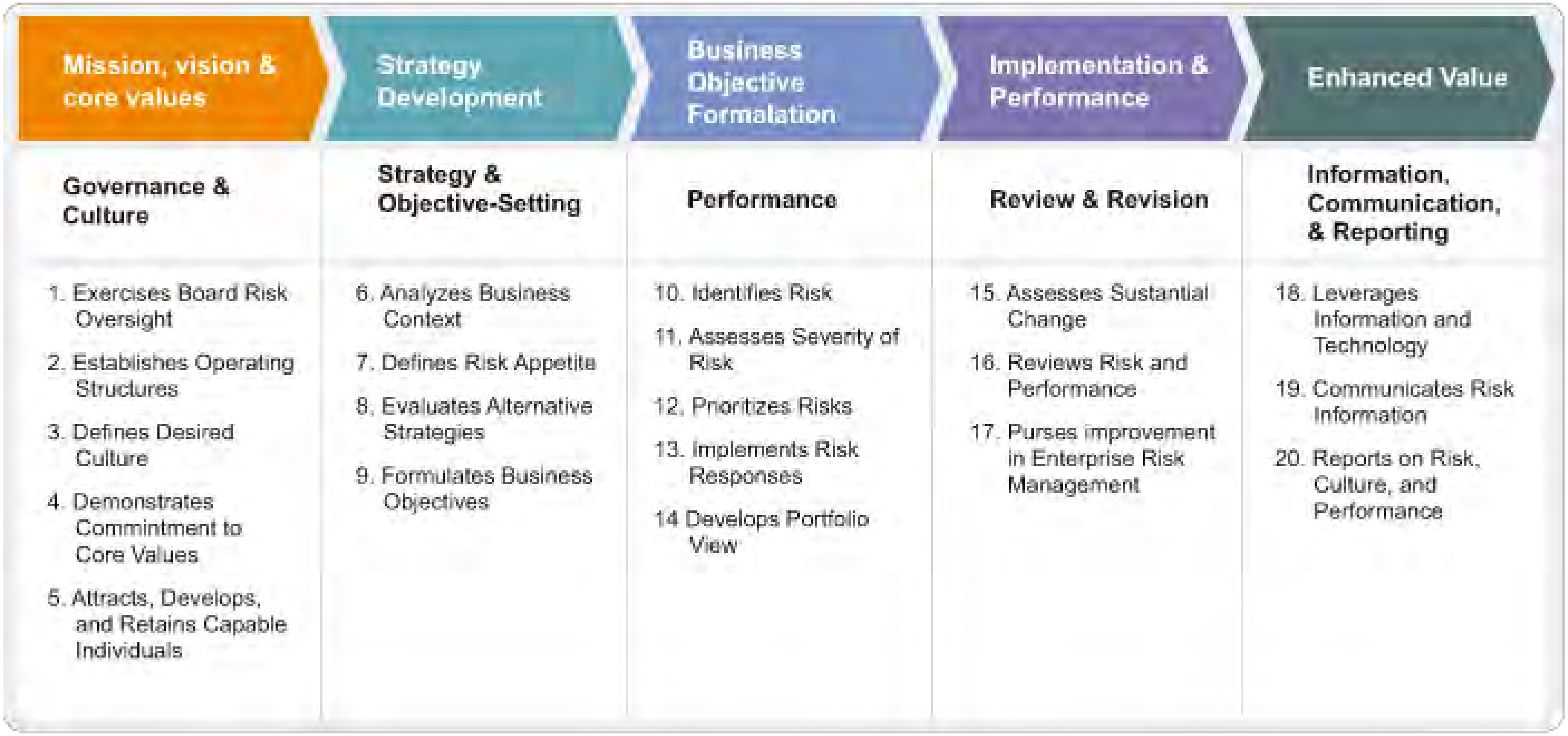
ISO 31000 ERM Framework



ISO 31000: 2018 Framework

- ❑**Communication and Consultation:** Emphasizes the importance of promoting awareness and understanding of risk across key stakeholders.
- ❑**Scope, Context, and Criteria:** Highlights the importance of customizing the risk management process to the organization.
- ❑**Risk Assessment:** Describes that the risk assessment consists of risk identification, risk analysis, and risk evaluation.
- ❑**Risk Treatment:** Reminds business leaders of the importance of selecting and implementing responses to manage risks.
- ❑**Monitoring and Review:** Emphasizes the importance of improving the effectiveness of the risk management process.
- ❑**Recording and Reporting:** Highlights the importance of effective communication of risk information for decision-making.

COSO ERM Framework



Mission, vision & core values	Strategy Development	Business Objective Formalation	Implementation & Performance	Enhanced Value
Governance & Culture	**Strategy & Objective-Setting**	**Performance**	**Review & Revision**	**Information, Communication, & Reporting**
1. Exercises Board Risk Oversight 2. Establishes Operating Structures 3. Defines Desired Culture 4. Demonstrates Commintment to Core Values 5. Attracts, Develops, and Retains Capable Individuals	6. Analyzes Business Context 7. Defines Risk Appetite 8. Evaluates Alternative Strategies 9. Formulates Business Objectives	10. Identifies Risk 11. Assesses Severity of Risk 12. Prioritizes Risks 13. Implements Risk Responses 14 Develops Portfolio View	15. Assesses Sustantial Change 16. Reviews Risk and Performance 17. Purses improvement in Enterprise Risk Management	18. Leverages Information and Technology 19. Communicates Risk Information 20. Reports on Risk, Culture, and Performance

COSO ERM framework is one of the two widely accepted standards for identifying, assessing, and managing risks for the enterprise, and it comprises of five interrelated enterprise risk management components.

Customizing ERM Frameworks

❑The risk management frameworks out there are guides.

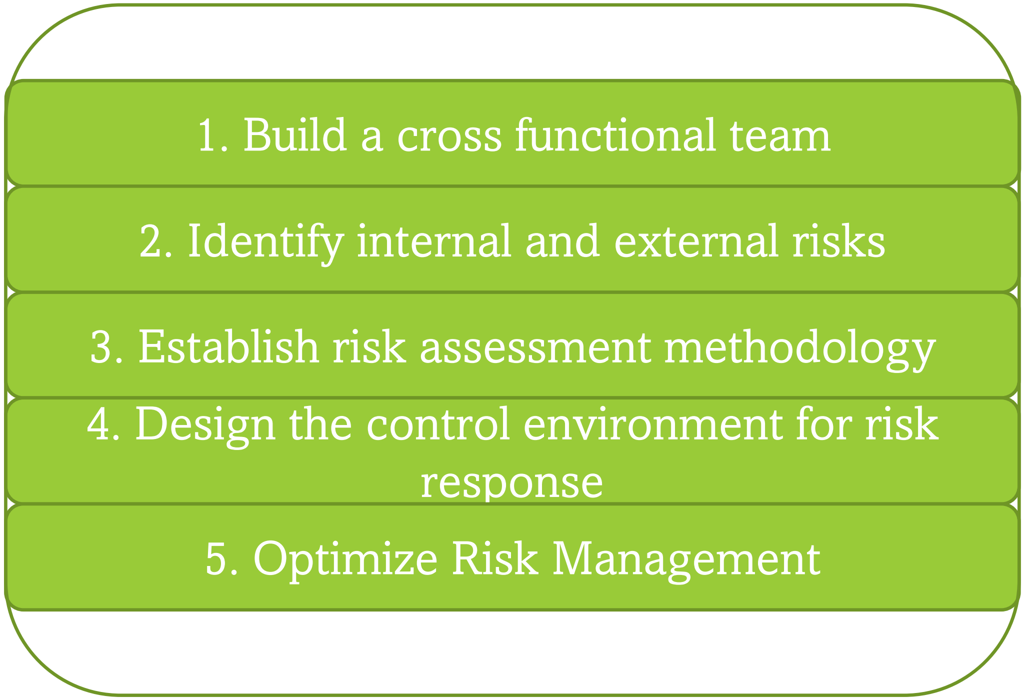
❑Consider the available framework if good enough for the organization .

❑Why do you need an enterprise risk management framework?

❑A lot of these risk frameworks are antiquated in what they talk about, hence the need to customize

Note: *Risk management is the overarching discipline in cybersecurity, and the focus tends to be on the technology aspects. But, for the enterprise, it's how to attract and retain profitable clients.*

ERM Framework Customization Steps


1. Build a cross functional team
2. Identify internal and external risks
3. Establish risk assessment methodology
4. Design the control environment for risk response
5. Optimize Risk Management

Developing a custom ERM framework helps implement a risk management strategy, align business objectives, and promote risk-based decision-making.

But, customizing an ERM framework to fit internal objectives, customer needs, industry regulations, IT governance, and internal audit standards doesn't have to be overwhelming.

Autnhive

Automating Data Security & Privacy

.... Empowering the planet with Data Security and Privacy

---

Protect Your Data and Privacy, Before it's Lost.

SCAN ME

DATAPLUS GLOBAL SERVICES

KEYMATIX

nathansuyi@gmail.co

...Work Securely Anywhere

....the reliable partner

DATAPLUS
GLOBAL SERVICES

KEYMATIX

natansuyi@dataplusgs.com.ng

nathansuyi@gmail.com

+234 803 255 4123

Workshop Activity 1: Gemini Motor Sports

A hypothetical illustration from a (Chartered Global Management Accountant) CGMA case study: How to evaluate enterprise risk management maturity.

Gemini Motor Sports (GMS), a public company headquartered in Brazil, manufactures on-road and off-road recreational vehicles for sale through a dealer network in Brazil and Canada. GMS Chief Financial Officer (CFO) David Cruz was charged with overseeing the development of the initial ERM framework for the company.

In the first year of implementation, the ERM team met with senior management, and identified and prioritized a number of crucial risks that had been disruptive to GMS. Their initial presentation to the audit committee was criticized for being a rehash of past problems, and not useful to the board as they discussed the strategic direction of GMS.

In the second year of the programme, after seeking ERM training for the team, Cruz focused more attention on potential events that managers thought might affect the business. He asked them to assess the likelihood and potential impact of the identified risks.

The resulting report was well received. However, the audit committee chair suggested that the next step be an evaluation of the risk management process and the degree of its integration with the strategic management process of the organization, leading to the use of the CGMA Risk Management Maturity tool.

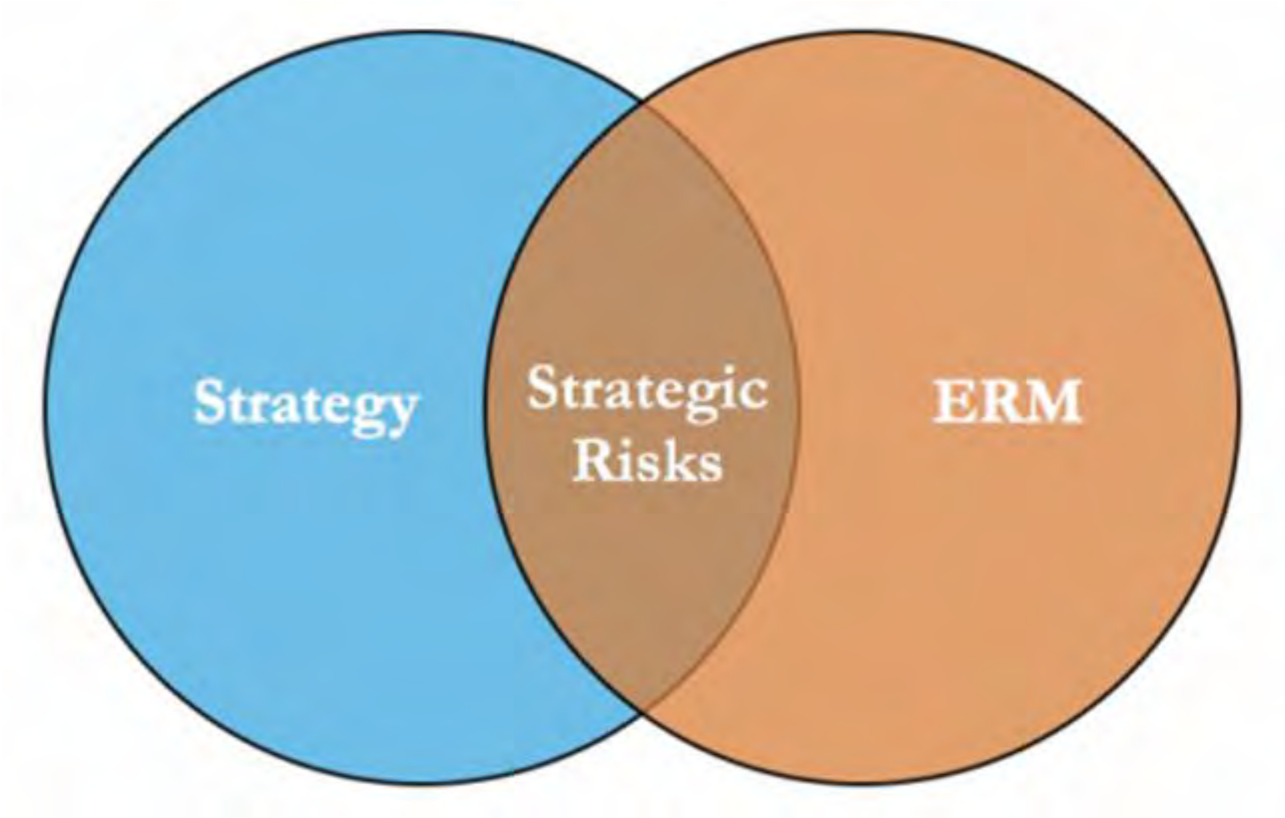
Practice

List three ERM Lesson Learned

Lessons learned

1. *Broad involvement on the part of board members and employees is essential in determining the risk appetite of a company, and in identifying and prioritising risks.*
2. *Speed of onset and persistence of risks, in addition to impact and likelihood, are important considerations in the prioritization of risks.*
3. *Ongoing monitoring and concise reporting on key risk exposures are essential for effective risk management.*

Enterprise Risk Management (ERM) Strategy



ERM Strategy

A risk management strategy is a key part of the enterprise risk management (ERM) lifecycle.

After identifying risks and assessing the likelihood of them happening, as well as the impact they could have, you will need to decide how to treat them.

The approach to decide on the best way to respond is your ERM strategy often called risk treatment. There are four main risk management strategies, or risk treatment options:

- ❑Risk Acceptance
- ❑Risk Transference
- ❑Risk Avoidance
- ❑Risk Reduction

Risk Acceptance

A risk is accepted with no action taken to mitigate it.

This approach will not reduce the impact of a risk or even prevent it from happening, but that's not necessarily a bad thing.

Sometimes the cost of mitigating risks can exceed the cost of the risk itself, in which case it makes more sense to simply accept the risk

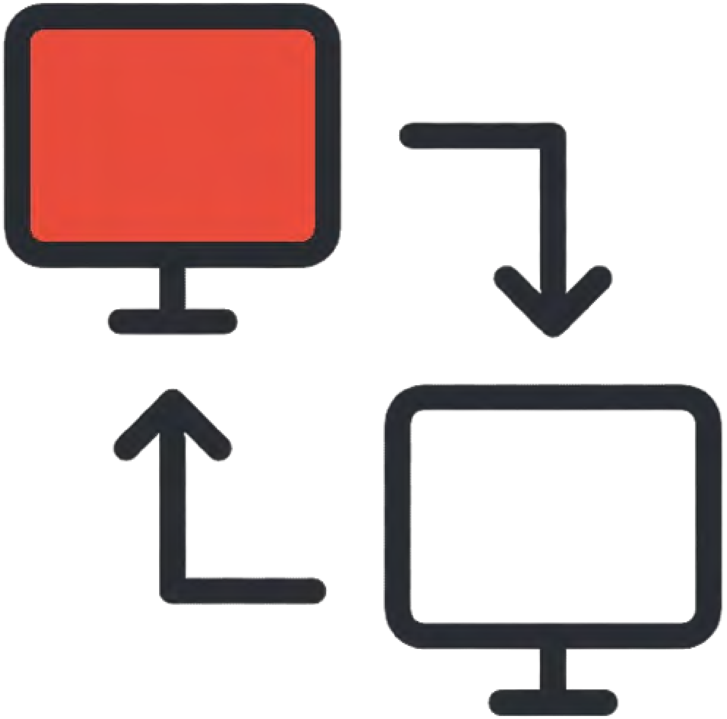
Risk Transference

A risk is transferred via a contract to an external party who will assume the risk on an organization's behalf.

Choosing to transfer a risk does not entirely eradicate it.

The risk still exists, only the responsibility for it shifts from your organization to another.

An example of this would be travel insurance where the risks of a lost suitcase or an accident abroad and the attendant costs is paid by a travel insurance company that bears the financial consequences.



Risk Avoidance

A risk is eliminated by not taking any action that would mean the risk could occur.

This aims to completely eliminate the possibility of the risk occurring. One example of risk avoidance would be with investment. If, after analyzing the risks associated with that investment, you deem it too risky, then you simply do not make the investment.

Risk Reduction

A risk becomes less severe through actions taken to prevent or minimize its impact.

Risk reduction is a common strategy when it comes to risk treatment and is sometimes known as lowering risk. One example of risk reduction would be within manufacturing and the risk of products being produced to incorrect specifications. Using a quality management system can lower the chance of this happening, so this would be a method of risk reduction.

ERM Appetite, Tolerance & Threshold

- ❑Risk appetite is the amount of risk which the company is willing to accept. It is a key enabling structure and active relation among risk management, strategy and target setting.

- ❑Risk tolerance is subject to the same wide variety of factors that determine risk appetite. But the amount of risk tolerance an organization accepts can vary on a case-by-case basis, depending on factors that include the nature of a project, a project's timeframe and the experience of the people involved. Risk tolerance can change over time as, for example, industry standards, regulations and accepted practices change.

- ❑Risk threshold is the maximum amount of risk that can be accommodated.

Risk Appetite

Risk Tolerance

Risk Threshold

Factors that influence ERM Appetite

Risk appetite, an integral component of ERM, can be influenced by a wide variety of factors, including the following:

- Organization culture
- Competitors
- Initiative types
- Current industry position
- Financial strength.

Developing Risk Appetite Framework

Risk appetite framework should be developed such that it aligned with organization mission towards achieving its strategic goals and objectives:

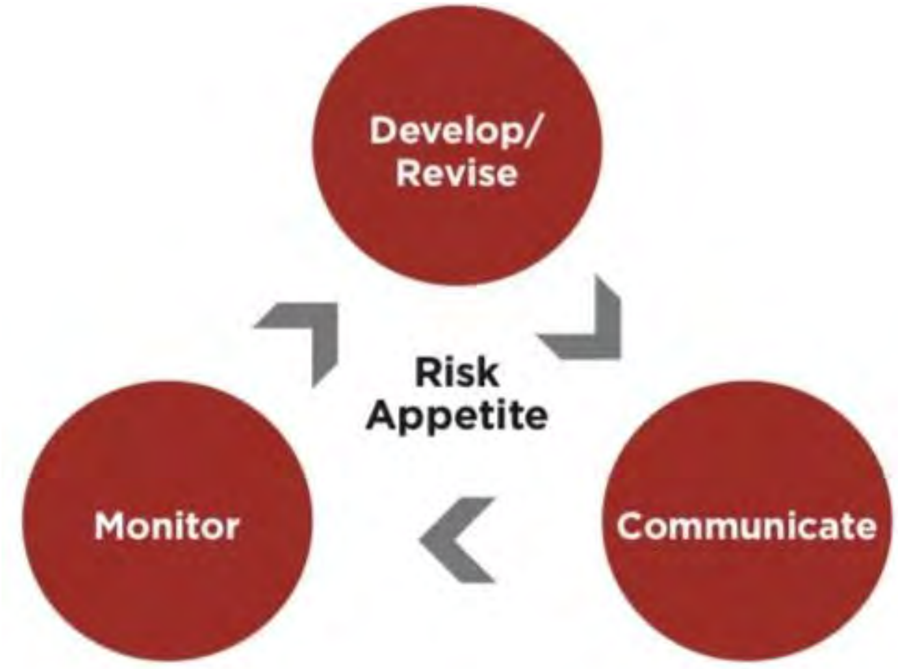
1. Understand the organization's strategic goals and objectives

2. Develop a risk appetite scale

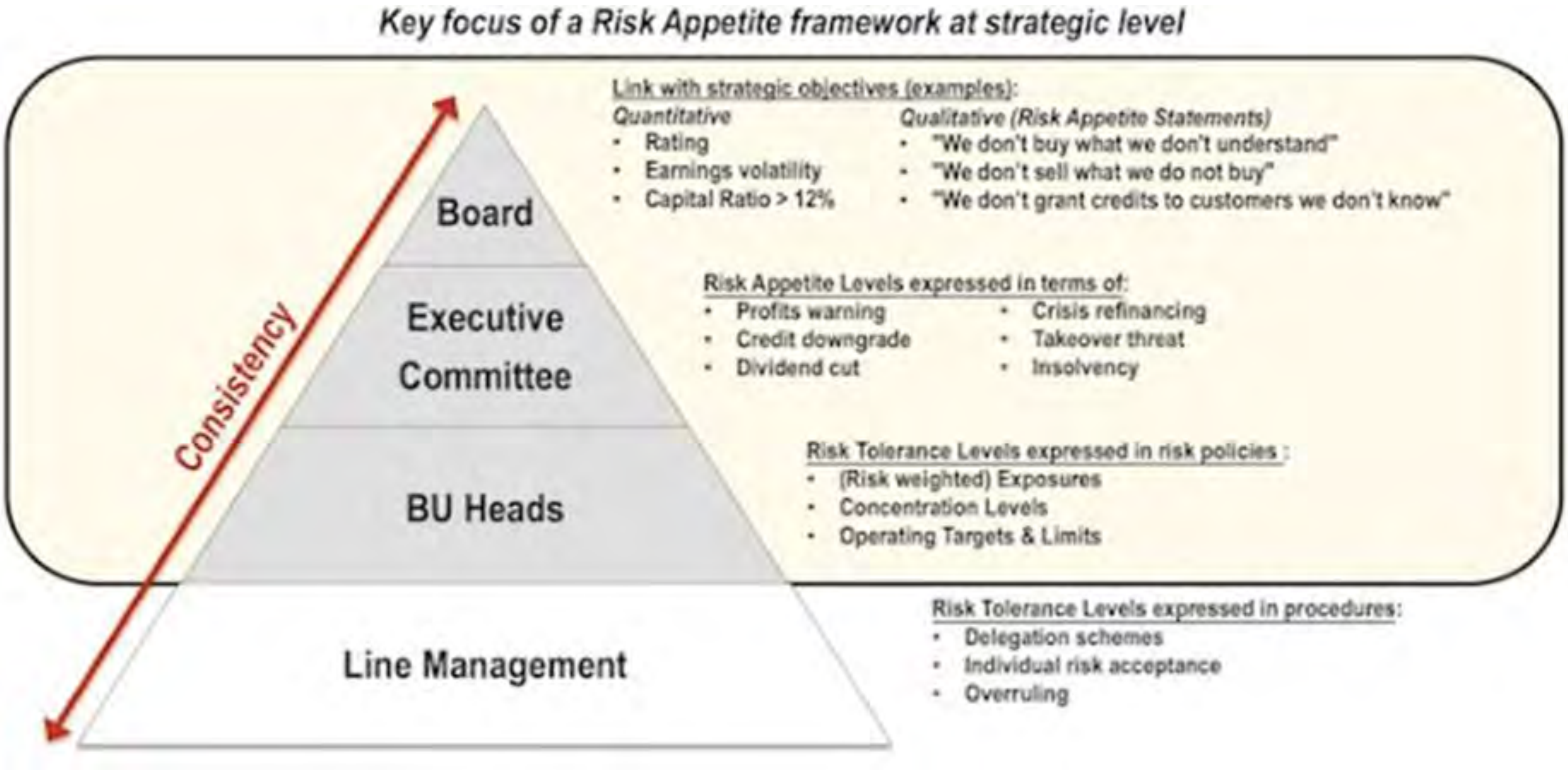
3. Connect with senior leadership

4. Utilize common language to develop a risk appetite statement

5. Develop prioritization tools



Risk Appetite Framework at Strategic Level



Key focus of a Risk Appetite framework at strategic level

Link with strategic objectives (examples):

Quantitative

- Rating
- Earnings volatility
- Capital Ratio > 12%

Qualitative (Risk Appetite Statements)

- "We don't buy what we don't understand"
- "We don't sell what we do not buy"
- "We don't grant credits to customers we don't know"

Risk Appetite Levels expressed in terms of:

- Profits warning
- Credit downgrade
- Dividend cut
- Crisis refinancing
- Takeover threat
- Insolvency

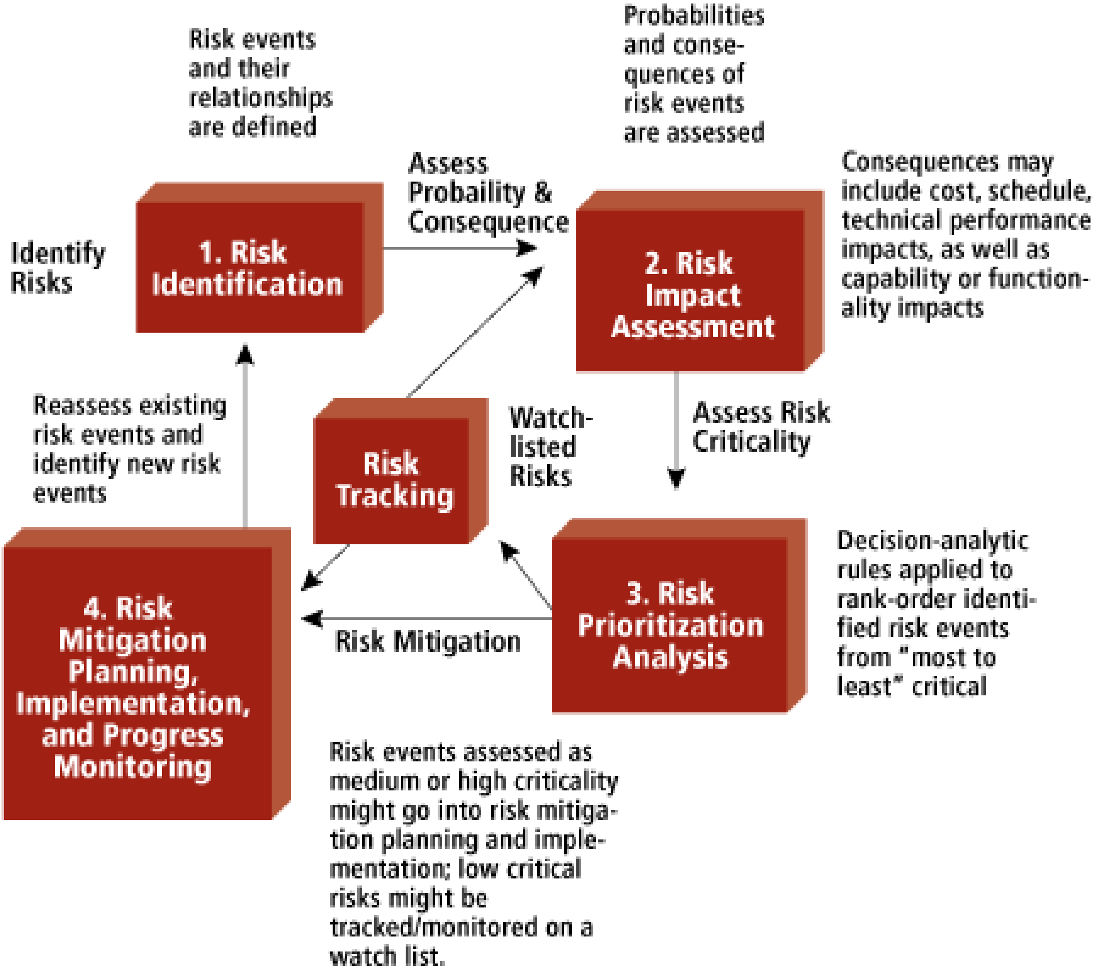
Risk Tolerance Levels expressed in risk policies :

- (Risk weighted) Exposures
- Concentration Levels
- Operating Targets & Limits

Risk Tolerance Levels expressed in procedures:

- Delegation schemes
- Individual risk acceptance
- Overruling

ERM Profile


Risk events and their relationships are defined
Identify Risks
1. Risk Identification
Assess Probaility & Consequence
Probabilities and consequences of risk events are assessed
2. Risk Impact Assessment
Consequences may include cost, schedule, technical performance impacts, as well as capability or functionality impacts
Assess Risk Criticality
Reassess existing risk events and identify new risk events
Risk Tracking
Watch-listed Risks
3. Risk Prioritization Analysis
Decision-analytic rules applied to rank-order identified risk events from "most to least" critical
4. Risk Mitigation Planning, Implementation, and Progress Monitoring
Risk Mitigation
Risk events assessed as medium or high criticality might go into risk mitigation planning and implementation; low critical risks might be tracked/monitored on a watch list.

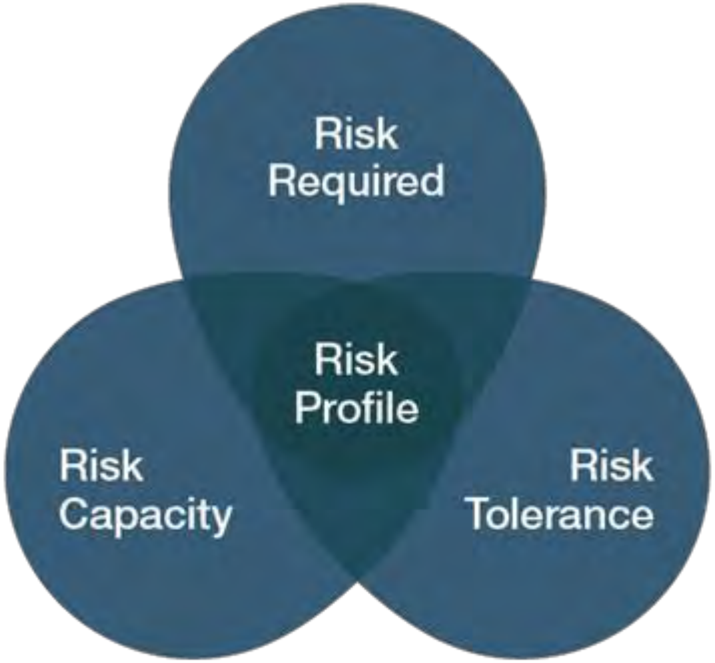
A risk profile examines threats, adverse effects, disruption and the associated costs with each type of risk

The outcome of risk profiling will be that the right risks have been identified and prioritized for action, and minor risks will not have been given too much priority. It also informs decisions about what risk controls measures are needed.

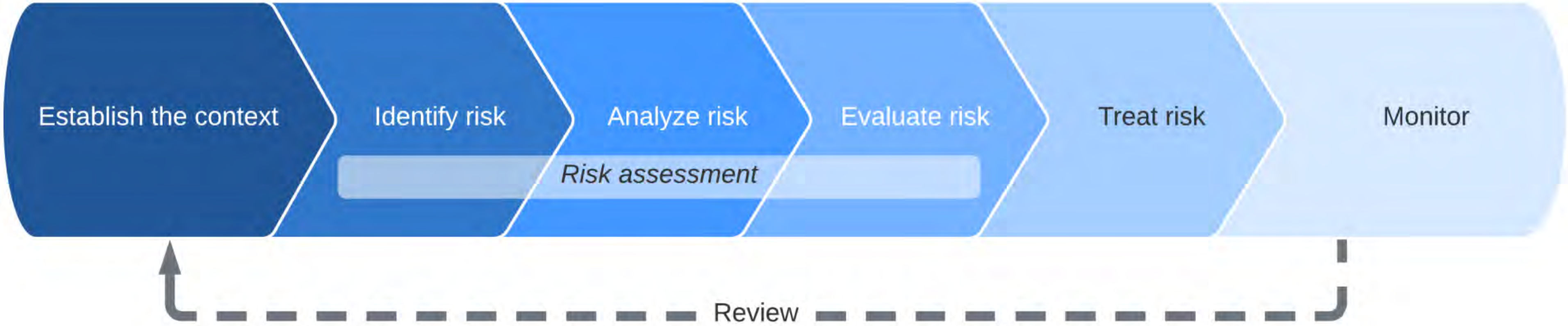
The ERM risk profile is ideally composed of three different components: risk required (tolerance), risk capacity and risk requirements.

When ERM profile is referred as aggressive or balance, it simply means risk tolerance or willingness to take risk.

Risk tolerance is a psychological factor, and deals with the comfort or volatility and the likelihood and size of negativity and the possible associated distress with the same.



Risk Management Process



1. Identify the risk
2. Analyze the risk
3. Prioritize the risk
4. Treat the risk
5. Monitor the risk

Step 1: Identify the Risk

The initial step in the risk management process is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks:

- Legal risks
- Environmental risks
- Market risks
- Regulatory risks etc.

Some techniques for identifying risk are:

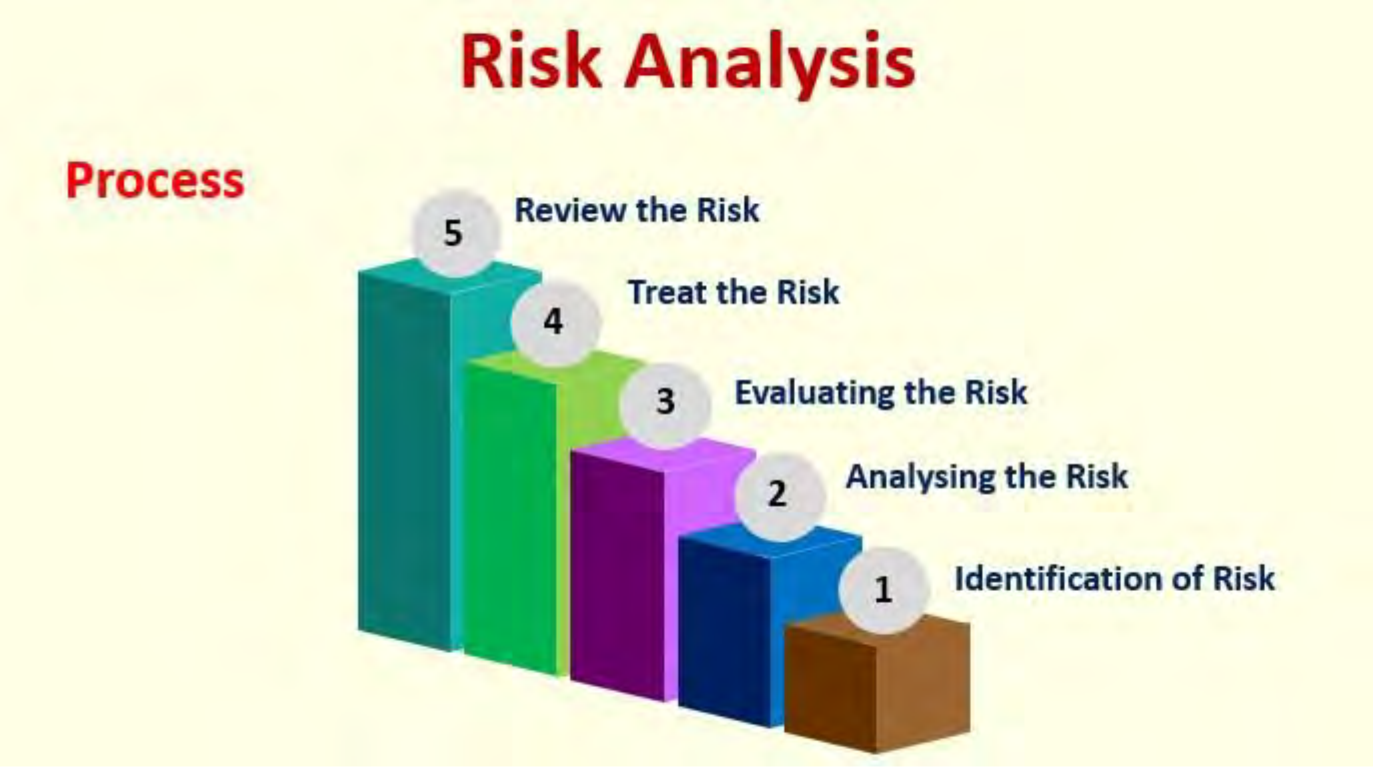
- Brainstorming.
- Event inventories and loss event data.
- Interviews and self-assessment.
- Facilitated workshops.
- SWOT analysis.
- Risk questionnaires and risk surveys.
- Scenario analysis.
- Using technology.

Step 2: Analyze the Risk

The scope of the risk must be determined.

Understanding the link between the risk and different factors within the organization.

Determine the severity and seriousness of the risk.



Step 3: Prioritize the Risk

Rank each risk by factoring in both its likelihood of happening and its potential effect on the project.

This step gives you a holistic view of the project at hand and pinpoints where the team's focus should lie. Most importantly, it’ll help you identify workable solutions for each risk. This way, the project itself is not interrupted or delayed in significant ways during the treatment stage.

Step 4: Treat the Risk

Every risk needs to be eliminated or contained as much as possible.

This is done by connecting with the experts of the field to which the risk belongs.

In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues.

The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls but in a risk management solution, all the relevant stakeholders can be sent notifications from within the system.

Step 5: Monitor and Review the Risk

Not all risks can be eliminated – some risks are always present.

Market risks and environmental risks are just two examples of risks that always need to be monitored.

Under manual systems monitoring happens through diligent employees.

These professionals must make sure that they keep a close watch on all risk factors.

Under a digital environment, the risk management system monitors the entire risk framework of the organization.

If any factor or risk changes, it is immediately visible to everyone. Computers are also much better at continuously monitoring risks than people.

Monitoring risks ensures the business continuity.

Autnhive

Automating Data Security & Privacy

Shockingly Simple, Fiercely Powerful

Enjoy military grade data protection without the complexities.

SCAN ME

KEYMATIX

DATAPLUS
GLOBAL SERVICES

nathansuyi@gmail.co

Automated Data Protection

****

Simplified Protect and Privatize Your Data Everywhere

…Work Securely Anywhere

.....your reliable partner

DATAPLUS
GLOBAL SERVICES

KEYMATIX

natansuyi@dataplusgs.com.ng

nathansuyi@gmail.com

+234 803 255 4123

https://nathanielatansuyi.com/

ncs
nigeria computer society

Workshop Activity 2:

Case of the Russian frozen chickens: A lesson in enterprise risk management

To supplement the understanding of enterprise risk management, I have adapted a case from **John J Hampton's *Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposure, and Seize Opportunity***.

The case examines four aspects of risk identified in pursuit of a risk opportunity associated with the export of a cargo of frozen chickens from Virginia and North Carolina to St. Petersburg, Russia. The company planned to load a number of 60-80 pound boxes on pallets for an ocean voyage. Except, the port of St. Petersburg had no shoreside refrigeration to allow quick unloading of an expensive reefer vessel.

Workshop Activity 2:
Scenario 1: Expropriation risk

If the ship wasted too long docked in St Petersburg waiting for containers to offload the shipment, it would incur significant fees for delayed operations. One solution would be to build a warehouse, but the risk manager identified an expropriation risk.

A case from the mid-1990s was cited: a European-invested Hotel in St. Petersburg incurred hefty fines after the Russian government learned it was using a foreign bank account to handle dollar transactions. The result was the expropriation of the hotel premises by the Russian government. While the risk manager knew she could obtain reimbursement insurance from a U.S. government agency, the identified expropriation risk didn’t seem to be the answer. Therefore, the company opted to seek a strong Russian partner with high-level government connections and allow the partner to accept the appropriation and storage exposure.

Practice

What is the Lesson Learned

Lessons learned

Investigate all options for risk reduction. Don’t assume that the obvious approach is the best answer!

Workshop Activity 2:
Scenario 2: Credit Risk

So far so good; the company had a strong Russian partner. This was also bad news, as it created a credit risk. How could the U.S. company make sure the Russian partner paid in a timely manner? It wasn't realistic to ask for an up-front payment, neither was it reasonable to obtain a letter of credit guaranteeing future payment. As it transpired, the Russian partner was not able to pay for the first cargo cargo until 30 days after receiving it. To deal with this problem of credit exposure, an agreement was made that the Russian partner would pay for one cargo before it received a subsequent. This mitigated exposure to credit risk because the stream of profits from a series of cargo shipments was significantly larger than a default payment on a single cargo.

If the Russian partner didn't pay by day 45 after receipt of a cargo, the ship carrying the next cargo would be diverted from Russia to a northern European port.

Practice

What is the Lesson Learned

Lessons learned

Give other parties incentives to help your organization mitigate risk.

Workshop Activity 2:
Scenario 3: Physical Security Risk

Once the Russian partner accepted the chicken in St. Petersburg, the shipment was transported by rail to Moscow, Yekaterinburg, and beyond via locked refrigeration containers loaded onto flat railcars. On the fifth journey, one of the containers was discovered to be empty when it arrived in Moscow after the three-day trip from St. Petersburg. The shipment had been stolen.

At this point, the partner was facing a physical security risk.

Two viable strategies were identified:

- Purchase insurance
- Door-to-door container placement so that the doors could not be opened if the locks were broken

The first strategy was dismissed quickly. Who would insure a cargo with an already-existing high chance of loss? Premiums would be prohibitively high.

The second strategy was chosen.

This proved effective for a time; however, the story was not over. Several journeys later, another container arrived empty.

Realizing that someone had a crane on a siding when the train stopped in the middle of the night, the Russian partner considered what else should be tried.

Finally, the problem was solved by placing a boxcar on the back of the train. The car had fitted heaters and cots, carrying guards armed with Kalashnikovs. Whenever the train stopped, the guards stepped out to protect the containers.

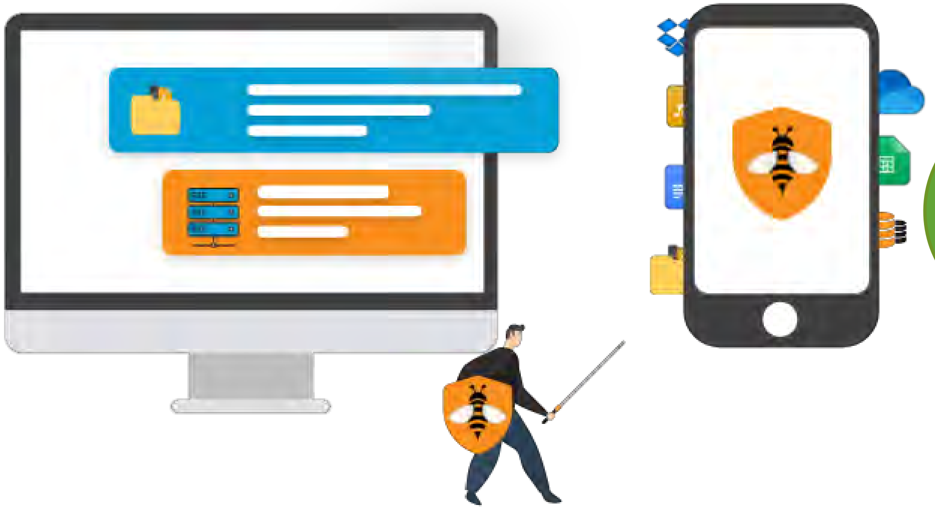
Practice

What is the Lesson Learned

Autnhive

Automating Data Security & Privacy

………. Protecting people – Making Digital Security a Reality for everyone and organisation



Smart Data Restoration

***

Effortless Data Tracking, Reporting and Compliance

***

Protect, Privatize and Consolidate your data

…Work Securely Anywhere

…..your reliable partner

DATAPLUS GLOBAL SERVICES

KEYMATIX

natansuyi@dataplusgs.com.ng

nathansuyi@gmail.com

+234 803 255 4123

https://nathanielatansuyi.com/

nigeria computer society

Lessons learned

Sometimes it's worth sticking with a risk management strategy, tweaking and fine-tuning the solution until the problem is solved. Not everything will work out-of-the-box.

Workshop Activity 2:
Scenario 4: Upside of Risk

While the security situation on Russian railroads has improved significantly since the 1990s, this story also identifies the upside of risk.

Once the cargo was being protected by armed guards, the Russian partner had the opportunity to offer insurance services to third parties to protect their cargoes as well as the frozen chickens.

The loss incurred from managing the risk with the paid armed guards and rear boxcar would, in that case, be offset by the confidence that the train would experience no losses, and the additional revenue from the insurance services offered.

Practice

What is the Lesson Learned

Lessons learned

Risk management does not end with the mitigation of risk – always look for an upside!

3

Cyber Security and Enterprise Risk Management (ERM) Integration

Why is Cybersecurity Important to ERM?

- Cybersecurity is a problem that will never be solved, but rather, a risk to be managed.
- Cyber risk has become an issue for the entire business, not just the tech or IT department.
- Risks from a business perspective, executives can make decisions with both protection and operational success in mind.
- Cyber risks evaluation in an organization, must understand the impact on each business aspect, in the context of cyber risk analysis.

As organizations increasingly rely on technology for their day-to-day operations, cybersecurity has become essential to comprehensive enterprise risk management.

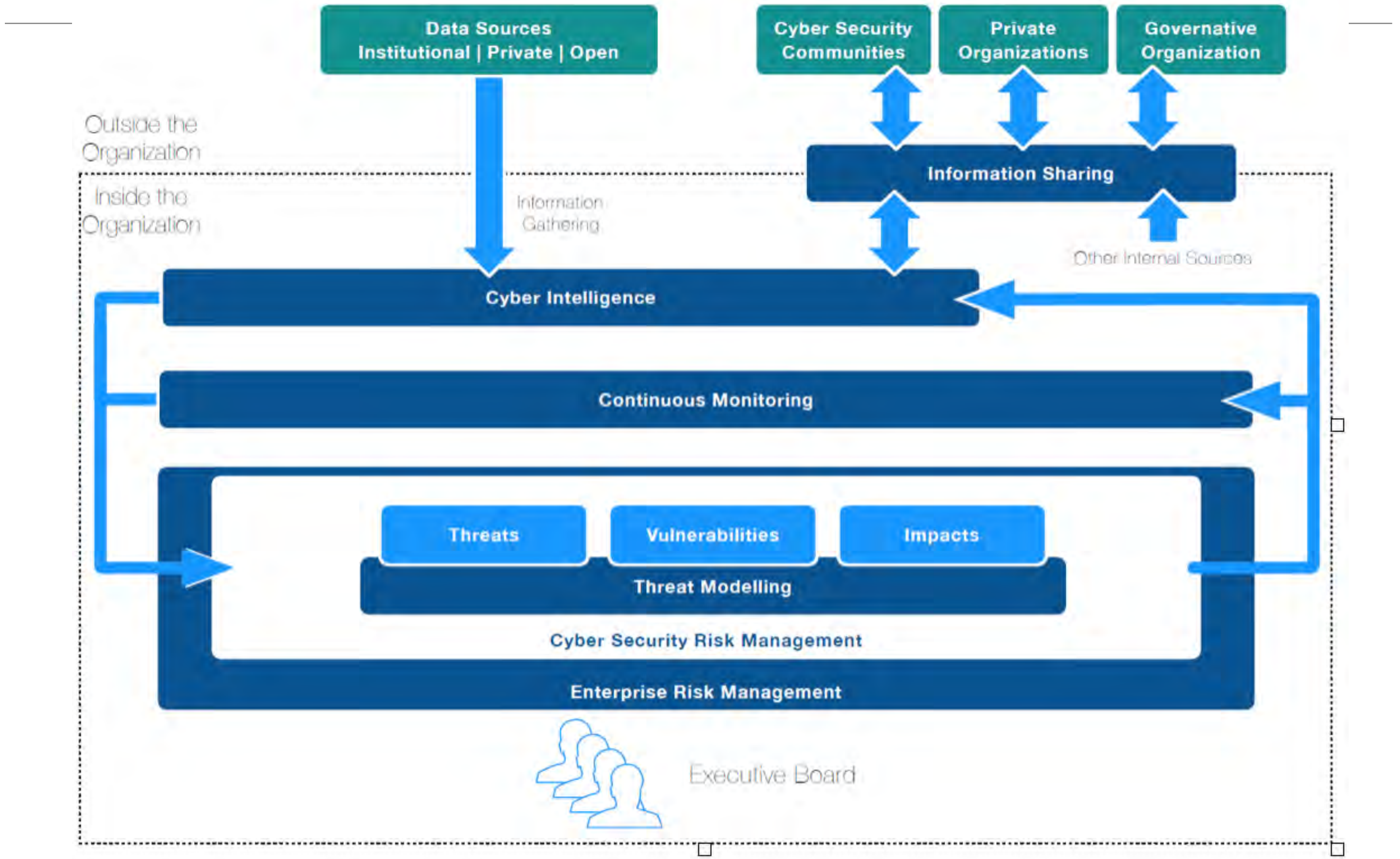
Cybersecurity Risk Management Framework (CRMF)

❑ A framework that brings a risk-based, full-lifecycle approach to the implementation of cybersecurity.

❑ CRMF supports integration of cybersecurity in the systems design process, resulting in a more trustworthy system that can dependably operate in the face of a capable cyber adversary.

❑ CRMF emphasizes integrating cybersecurity activities into existing processes including requirements
  ❑ Program protection planning
  ❑ Trusted systems and networks analysis
  ❑ Developmental and operational test and evaluation
  ❑ Financial management and cost estimating
  ❑ Sustainment and disposal

Cyber Security RMF process

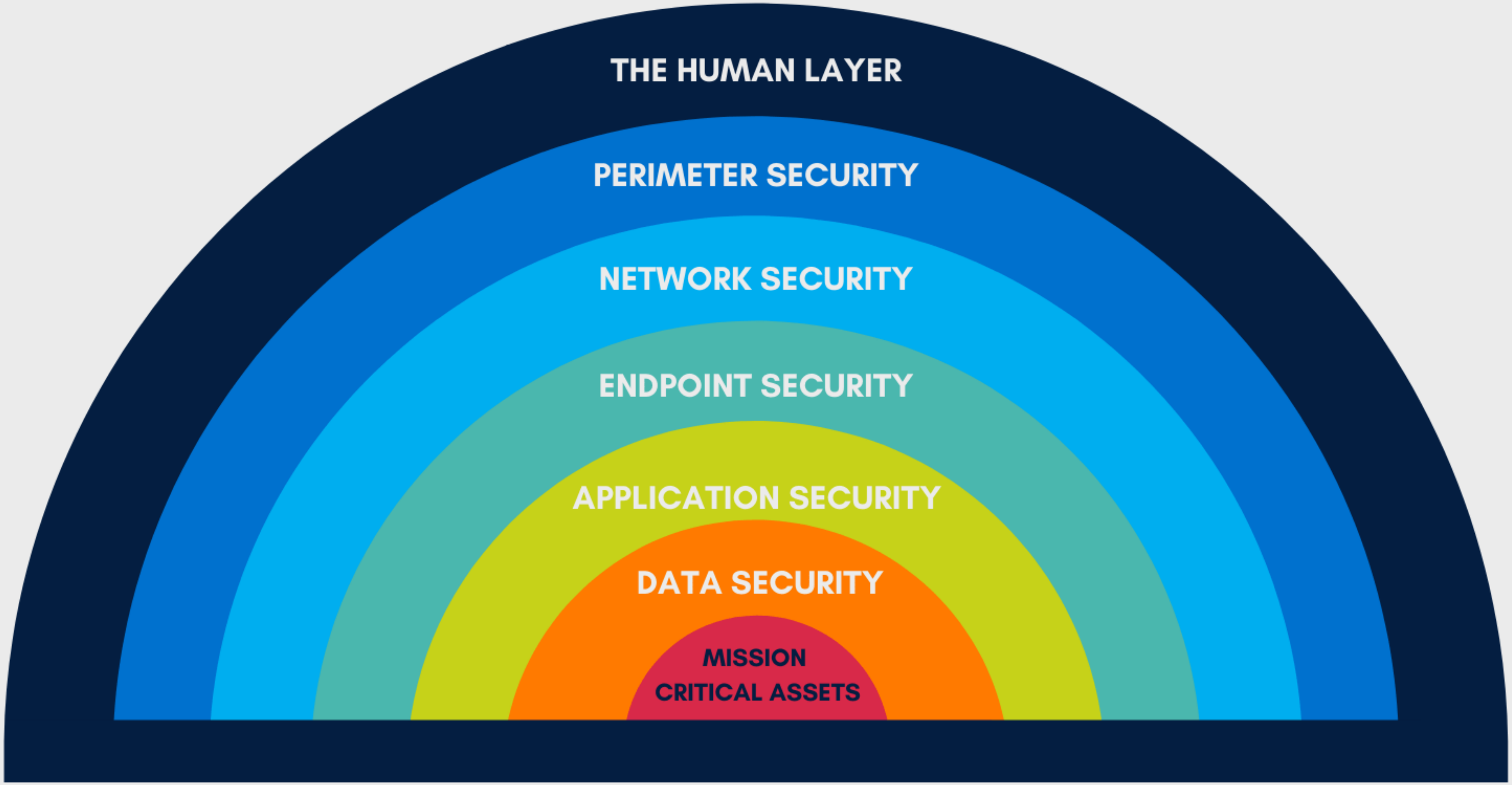


Cyber Threat

Cyber threat is any vector that can be exploited in order to breach security, cause damage to the organization, or exfiltrate data. Common threat categories facing modern organizations include:

- ❑ **Adversarial threats**—including third-party vendors, insider threats, trusted insiders, established hacker collectives, privileged insiders, ad hoc groups, suppliers, corporate espionage, and nation-states.
- ❑ **Natural disasters**—hurricanes, floods, earthquakes, fire, and lightning can cause as much damage as a malicious cyber attacker.
- ❑ **System failure**—when a system fails, it may cause data loss and also lead to a disruption in business continuity.
- ❑ **Human error**—any user may accidentally download malware or get tricked by social engineering schemes like phishing campaigns. A storage misconfiguration may expose sensitive data.

THE 7 LAYERS OF CYBERSECURITY



THE HUMAN LAYER

PERIMETER SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

APPLICATION SECURITY

DATA SECURITY

MISSION CRITICAL ASSETS

The 7 layers of cybersecurity should center on the mission critical assets you are seeking to protect>

1: Mission Critical Assets – This is the data you need to protect

2: Data Security – Data security controls protect the storage and transfer of data.

3: Application Security – Applications security controls protect access to an application, an application's access to your mission critical assets, and the internal security of the application.

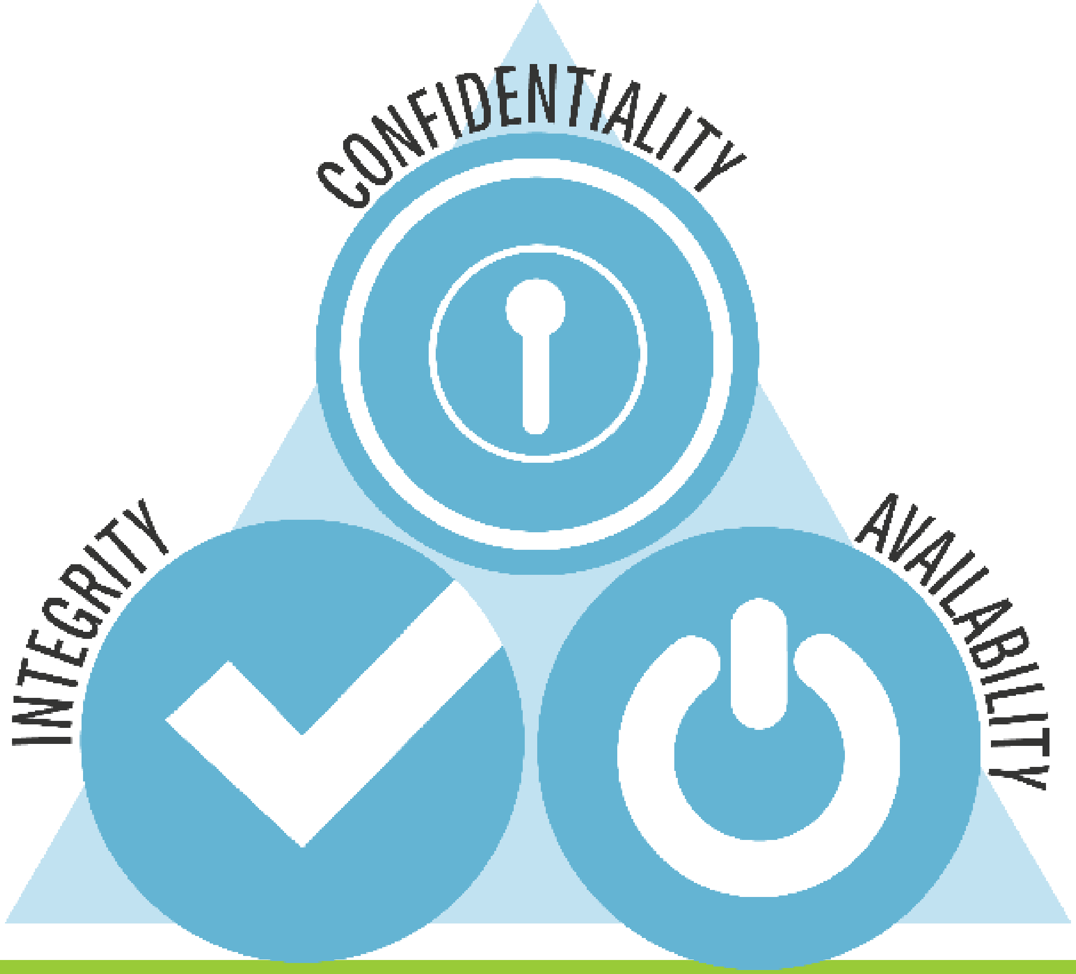
4: Endpoint Security – Endpoint security controls protect the connection between devices and the network.

5: Network Security – Network security controls protect an organization's network and prevent unauthorized access of the network.

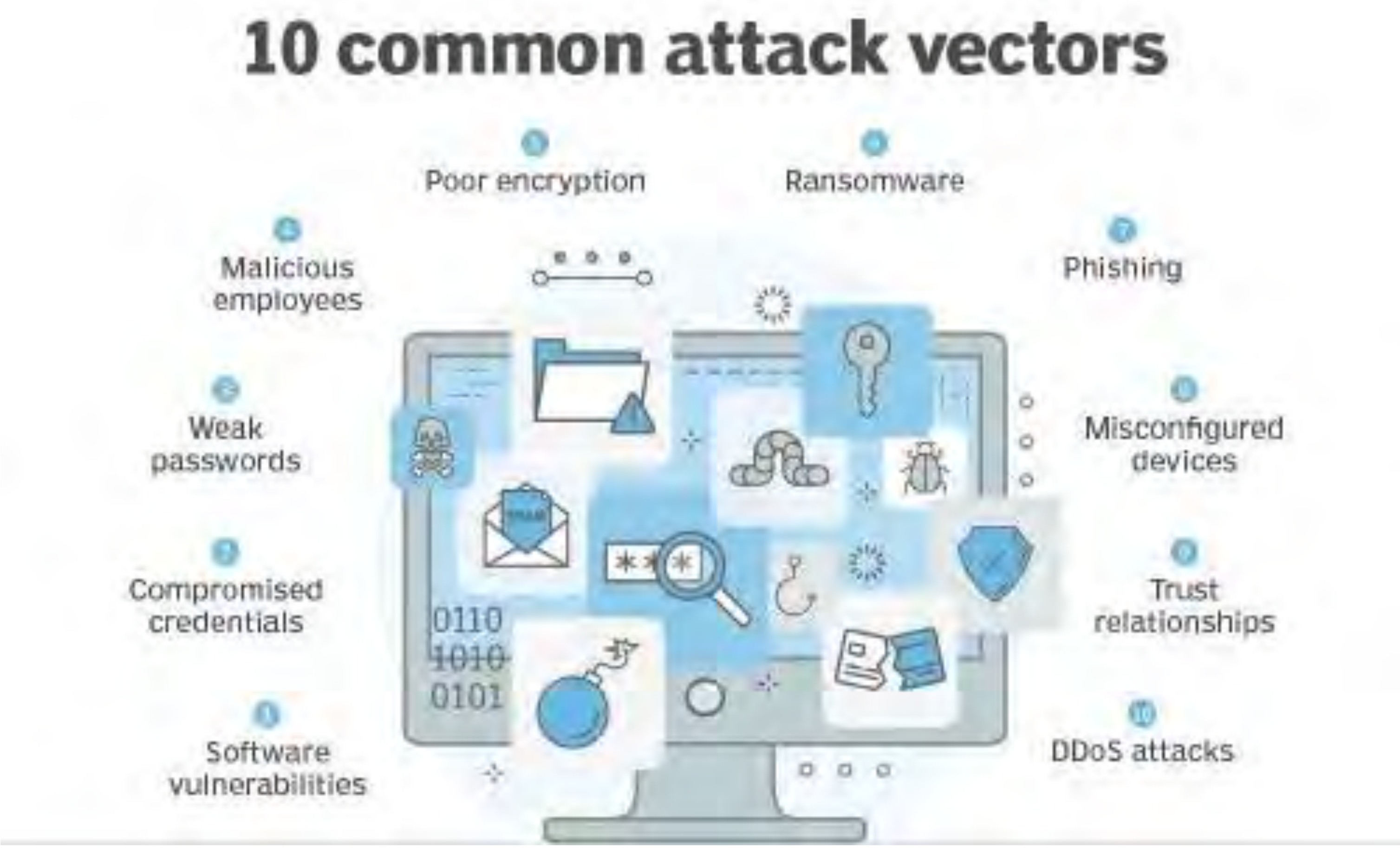
6: Perimeter Security – Perimeter security controls include both the physical and digital security methodologies that protect the business overall.

7: The Human Layer – Humans are the weakest link in any cybersecurity posture. Human security controls include phishing simulations and access management controls that protect mission critical assets from a wide variety of human threats, including cyber criminals, malicious insiders, and negligent users.

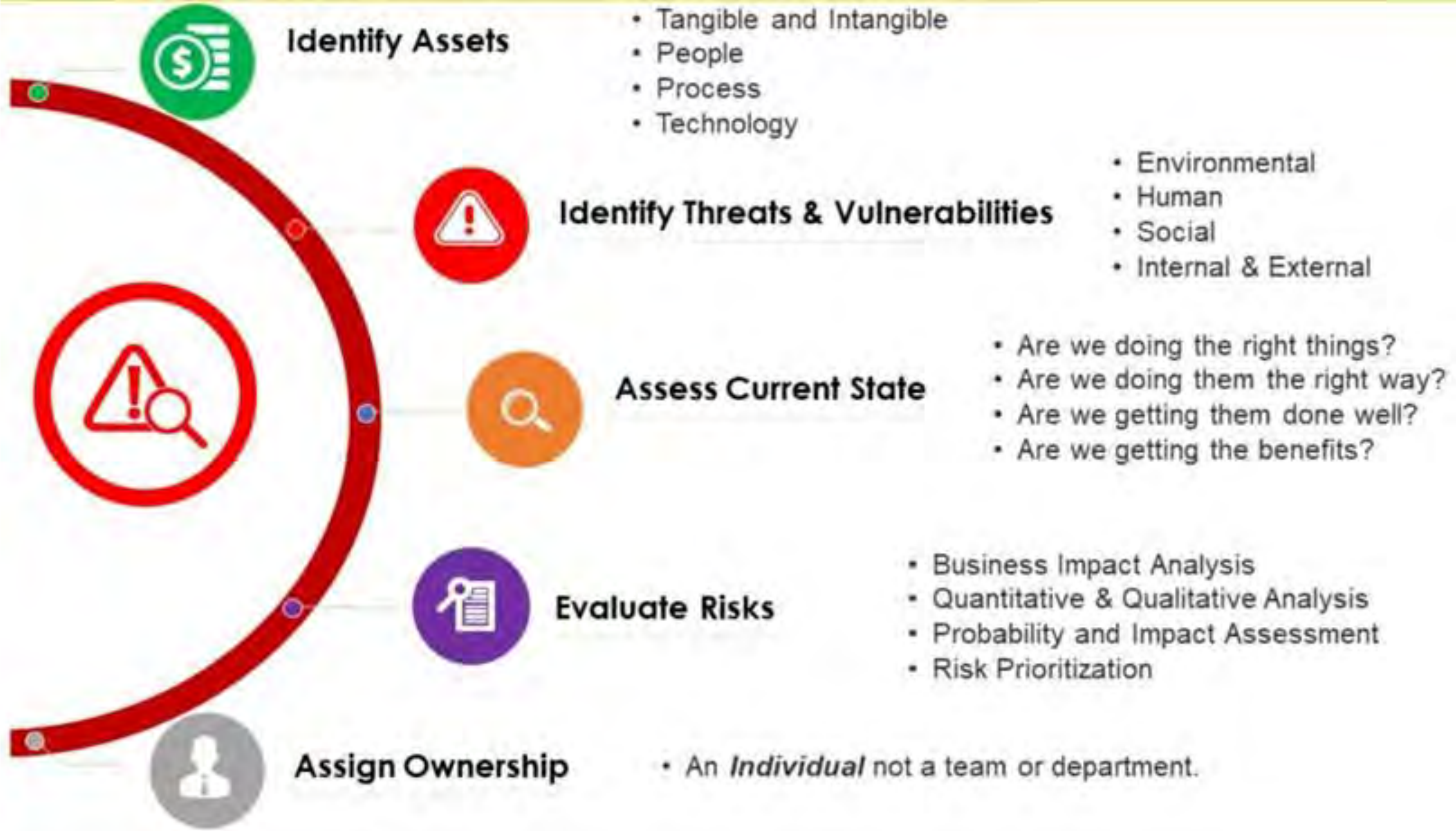
Cyber Security Goals



Key Threat Vectors



Cybersecurity Risk Assessment



Identify Assets

- Tangible and Intangible
- People
- Process
- Technology

Identify Threats & Vulnerabilities

- Environmental
- Human
- Social
- Internal & External

Assess Current State

- Are we doing the right things?
- Are we doing them the right way?
- Are we getting them done well?
- Are we getting the benefits?

Evaluate Risks

- Business Impact Analysis
- Quantitative & Qualitative Analysis
- Probability and Impact Assessment
- Risk Prioritization

Assign Ownership

- An *Individual* not a team or department.

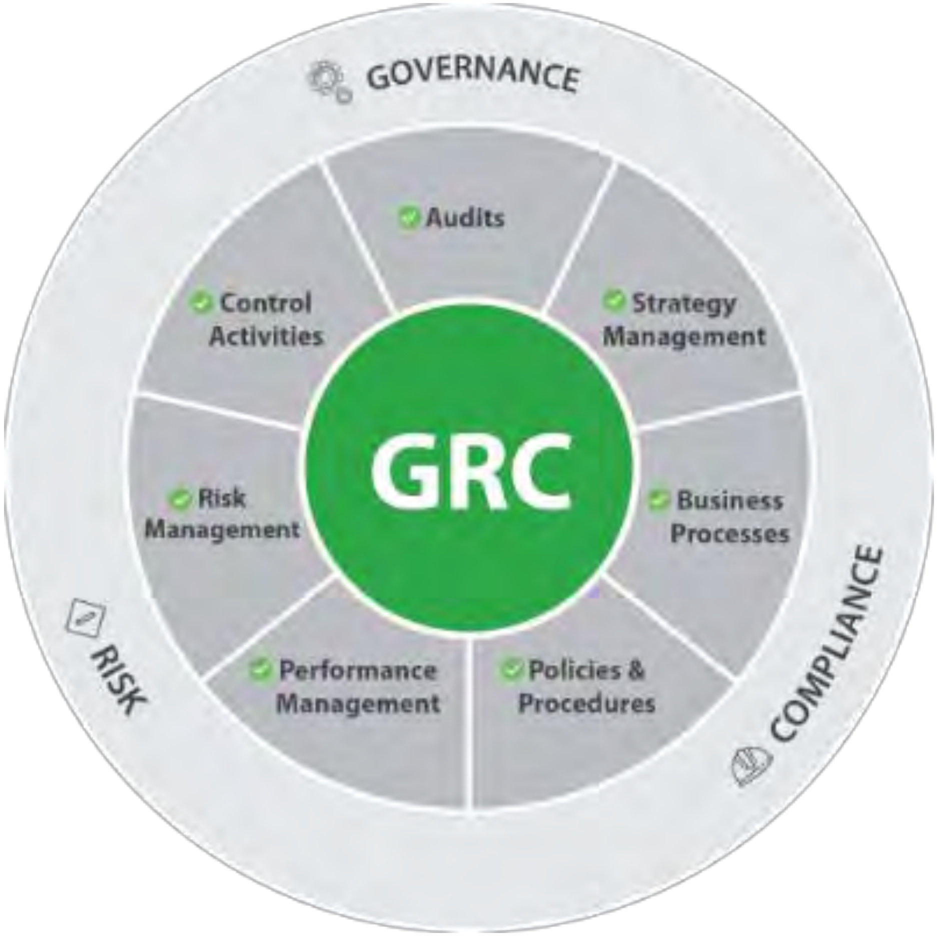
Cyber Security Risk Management (CSRM) as an Integrated Component of ERM

- ❑ Similarities and variances exist among approaches by public- and private-sector practices for ERM/CSRM coordination and interaction.
- ❑ Issues of confusing ERM and CSRM practices as separate stovepipes.
- ❑ The CSRM program is an integral part of the ERM portfolio, both taking its direction from ERM and informing it.
- ❑ ERM strategy and CSRM strategy are not divergent; CSRM strategy should be a subset of ERM strategy with particular objectives, processes, and reporting.

Governance, Risk Management and Compliance (GRC)

4

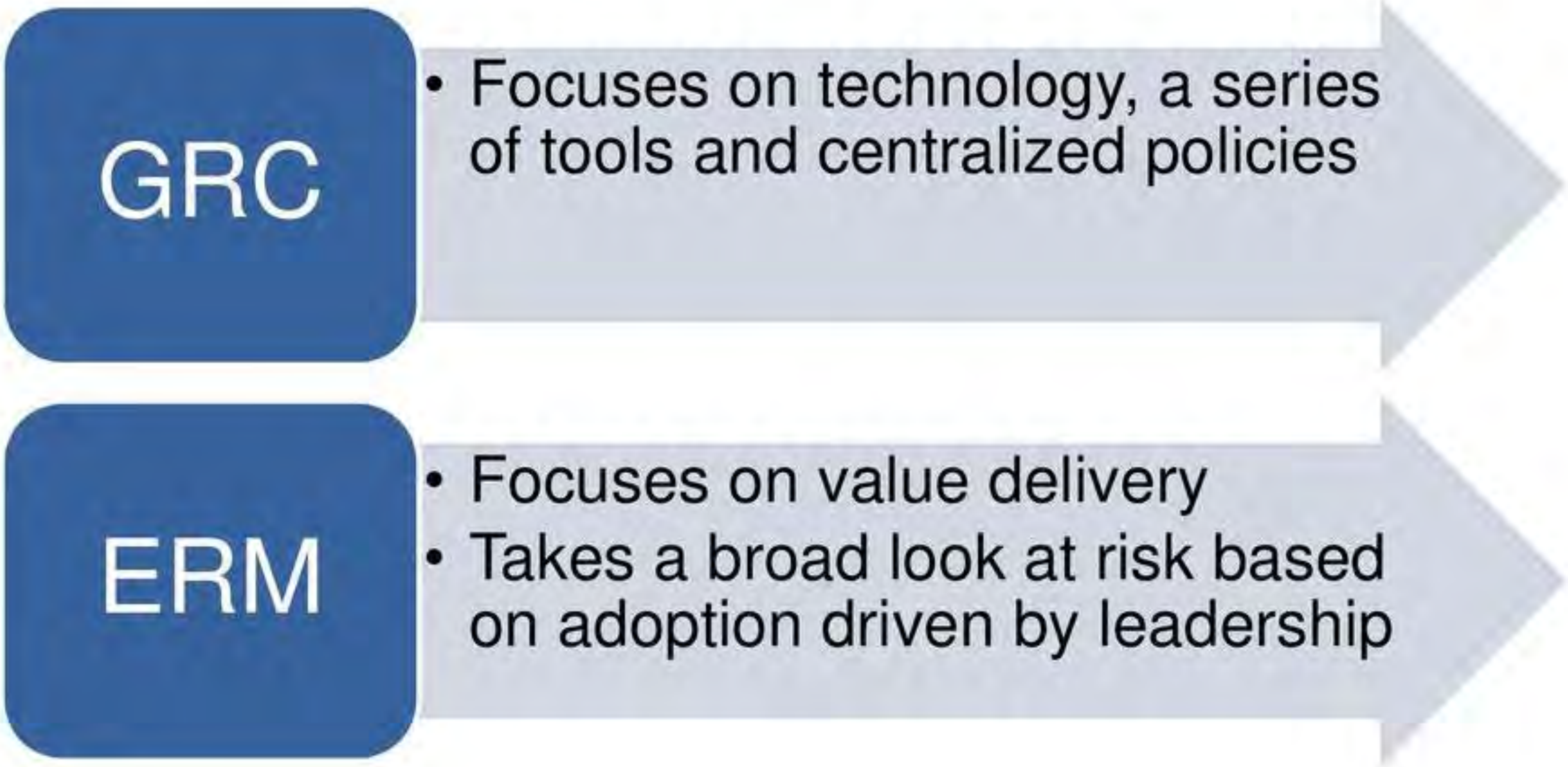
GRC



ERM can be thought of as a subset of GRC, focused on the 'risk management' component of GRC.

GRC can be thought of as a framework to help organizations create strategies to address enterprise risk management, governance, and compliance activities.

Differences Between GRC and ERM



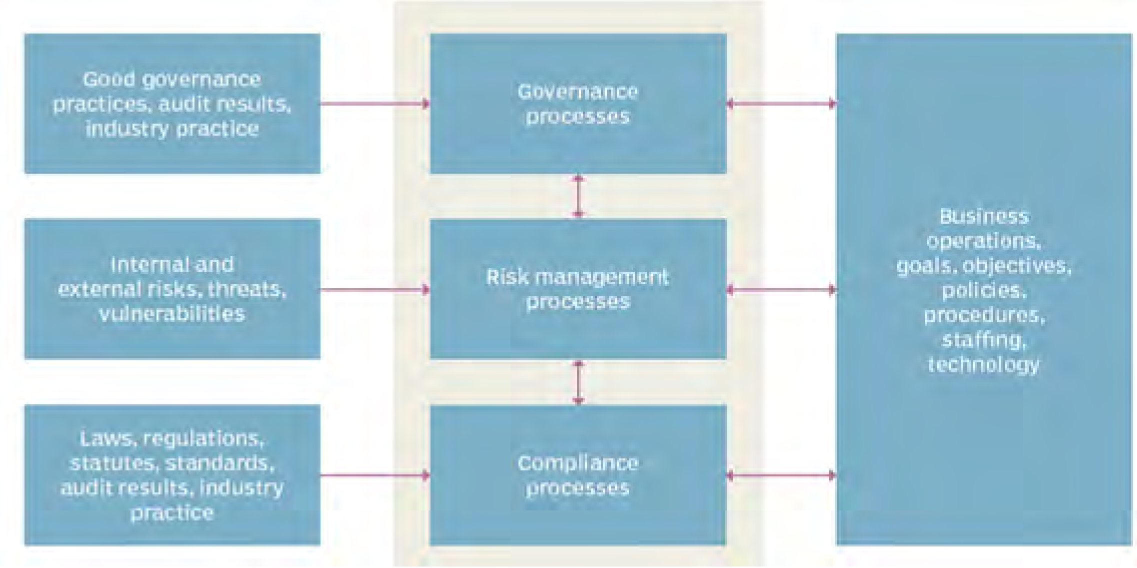
GRC

- Focuses on technology, a series of tools and centralized policies

ERM

- Focuses on value delivery
- Takes a broad look at risk based on adoption driven by leadership

Governance, Risk and Compliance (GRC) Frameworks


Good governance practices, audit results, industry practice
Internal and external risks, threats, vulnerabilities
Laws, regulations, statutes, standards, audit results, industry practice
Governance processes
Risk management processes
Compliance processes
Business operations, goals, objectives, policies, procedures, staffing, technology

GRC – is **a set of processes and procedures to help organizations achieve business objectives, address uncertainty, and act with integrity**.

The basic purpose of GRC is to instill good business practices into everyday life.

GRC is the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity.

GRC Drivers

Organizations must address today's challenging business climate. Even small businesses, nonprofits, and government agencies are facing issues that only large companies had to face in the past. Think of how many of these factors you have to deal with:

- ❑Stakeholders demand high performance along with high levels of transparency
- ❑Regulations and enforcement are ever-changing and unpredictable
- ❑Exponential growth of third-party relationships and risk is a management challenge
- ❑The costs of addressing risks and requirements are spinning out of control
- ❑The harsh (and scary) impact when threats and opportunities are not identified

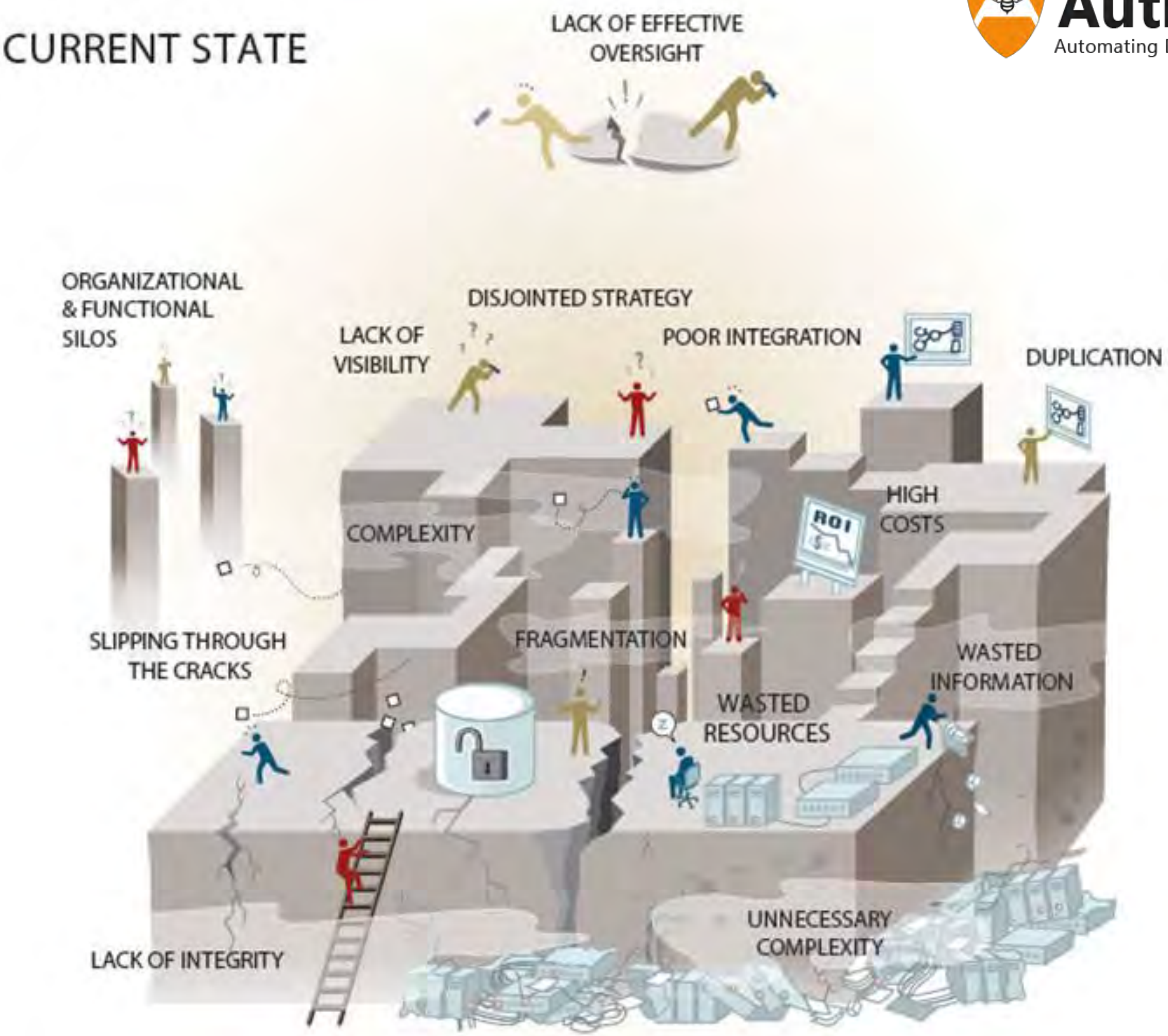
Effects of GRC Done Wrong

Studies have shown that disjointed GRC activities cause a number of problems. To address these drivers, organizations develop departments and programs such as: performance management; risk management; compliance; corporate social responsibility; and so on. Unfortunately, these departments and programs are often siloed, ineffective and yield troubling drawbacks:

- ❑ High costs
- ❑ Lack of visibility into risks
- ❑ Inability to address third party risks
- ❑ Difficulty measuring risk-adjusted performance
- ❑ Too many negative surprises

When these activities are siloed, it is highly likely that counter-productive objectives are established, sub-optimal strategies are selected, and performance isn't optimized.

CURRENT STATE



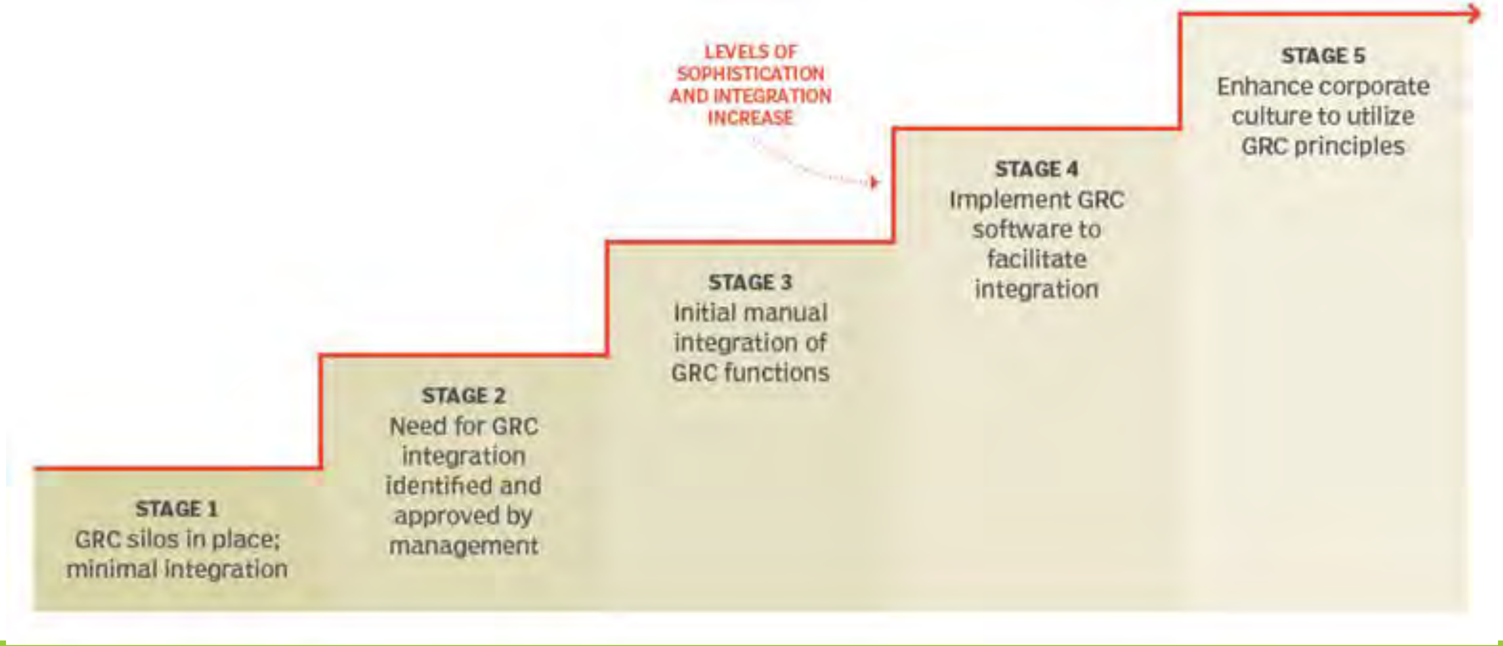
Effects of GRC Done Right

Integrating GRC capabilities does not mean creating a mega-department of GRC and doing away with decentralized management. Nor does it call for the use of only one GRC software system to manage it all. Rather, it is about establishing an approach that ensures the right people get the right information at the right times; that the right objectives are established; and that the right actions and controls are put in place to address uncertainty and act with integrity. When GRC is done right, the benefits accrue. Organizations that integrate GRC processes and technology across all or many silos have:

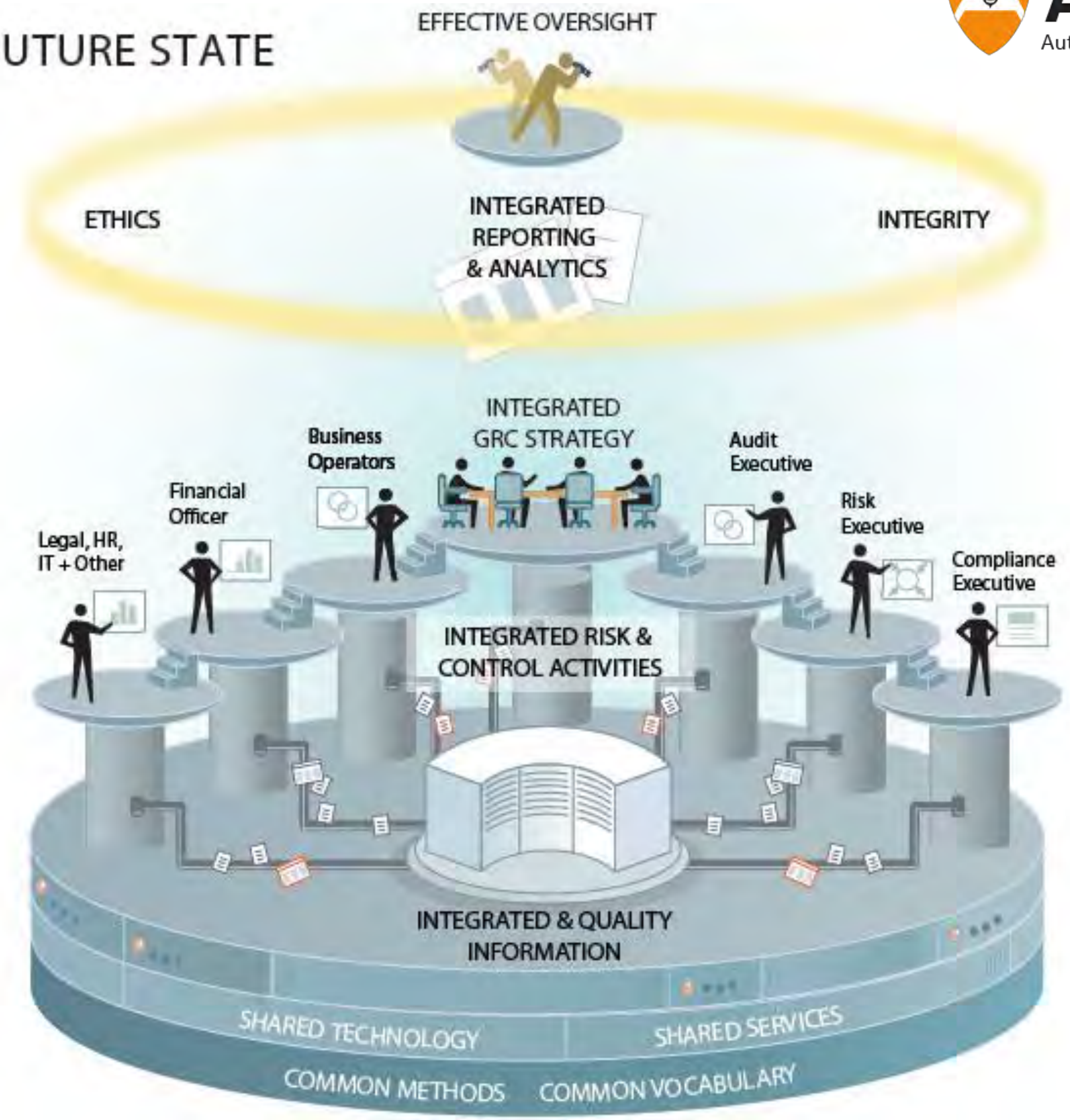
- ❑Reduced costs
- ❑Reduced duplication of activities
- ❑Reduced impact on operations
- ❑Achieved greater information quality
- ❑Achieved greater ability to gather information quickly and efficiently
- ❑Achieved greater ability to repeat processes in a consistent manner

GRC Maturity Model

A maturity model is one possible approach, as it defines the stages through which an organization can progress to achieve a suitable level of GRC excellence. The following figure presents a basic GRC maturity model. It can be expanded and modified into greater detail as needed and serve as part of the GRC program planning process.


LEVELS OF SOPHISTICATION AND INTEGRATION INCREASE
STAGE 1
GRC silos in place; minimal integration
STAGE 2
Need for GRC integration identified and approved by management
STAGE 3
Initial manual integration of GRC functions
STAGE 4
Implement GRC software to facilitate integration
STAGE 5
Enhance corporate culture to utilize GRC principles

FUTURE STATE



Outcomes of GRC Done right

1. **Achieve Business Objectives:** Ensure that all parts of the organization work together toward the achievement of enterprise objectives.
2. **Ensure Risk Aware Setting of Objectives and Strategic Planning:** Provide timely, reliable and useful information about risks, rewards, and responsibilities to the governing authorities, strategic planners, and business managers responsible for execution at all levels.
3. **Enhance Organizational Culture:** Inspire and promote a culture of performance, accountability, integrity, trust, and communication.
4. **Increase Stakeholder Confidence:** Grow stakeholder trust in the organization.
5. **Prepare and Protect the Organization:** Prepare the organization to address risks and requirements while protecting the organization from adversity and surprise and enabling it to grasp opportunities.

Outcomes of GRC Done right contd.

6. Prevent, Detect, and Reduce Adversity and Weaknesses: Establish actions and controls to prevent negative outcomes, reduce impact, detect potential problems, and address issues as they arise.

7. Motivate and Inspire Desired Conduct: Provide incentives and rewards for desirable conduct, especially in the face of challenging circumstances.

8. Stay Ahead of the Game: Learn information necessary to support quick changes in strategic and tactical direction while avoiding obstacles and pitfalls.

9. Improve Responsiveness and Efficiency: Establish capabilities that make the organization as a whole more responsive and efficient so that it has a competitive advantage.

10. Optimize Economic Return and Values: Allocate human and financial resources in a way that maximizes the economic return generated for the organization while maximizing its values.

Benefits of GRC Software and Tools

❑GRC software combines applications that manage the core functions of GRC into a single integrated package.

❑It enables an organization to pursue a systematic, organized approach to managing GRC-related strategy and implementation.

❑Instead of using siloed applications, administrators can use a single framework to monitor and enforce rules and procedures.

❑Successful installations enable organizations to manage risk, reduce costs incurred by multiple installations and minimize complexity for managers.

Effective GRC software includes risk examination and risk assessment tools that identify linkages to business processes, internal controls and operations. GRC software will identify the processes and tools that control those risks and integrate the single, multipoint and enterprise-wide software the business currently uses.

GRC Software Considerations

GRC software products are available from a number of vendors. Products accommodate virtually any type or size of organization, including organizations with many lines of business. GRC software can be confusing for businesses, however, because the market is replete with many types of products, including the following:

❑Integrated GRC products, which aim to provide an enterprise-wide approach to GRC, as noted above;

❑GRC products that target only certain areas, such as finance, IT or risk; and "point solution" products that may target one component of GRC but not all three.

GRC tools are increasingly cloud-based, but on-site systems are available, as are freeware options. Examples of GRC products includes:

IBM OpenPages with Watson; Galvanize's HighBond platform; ServiceNow Governance, Risk, and Compliance; Navex Global's Lockpath platform; and LogicManager.

Implementing GRC

GRC software implementation typically involves complex installations that include vendor negotiation and coordination of data between the vendor's technical team and multiple departments in the organization, including business, IT, security, compliance and auditing.

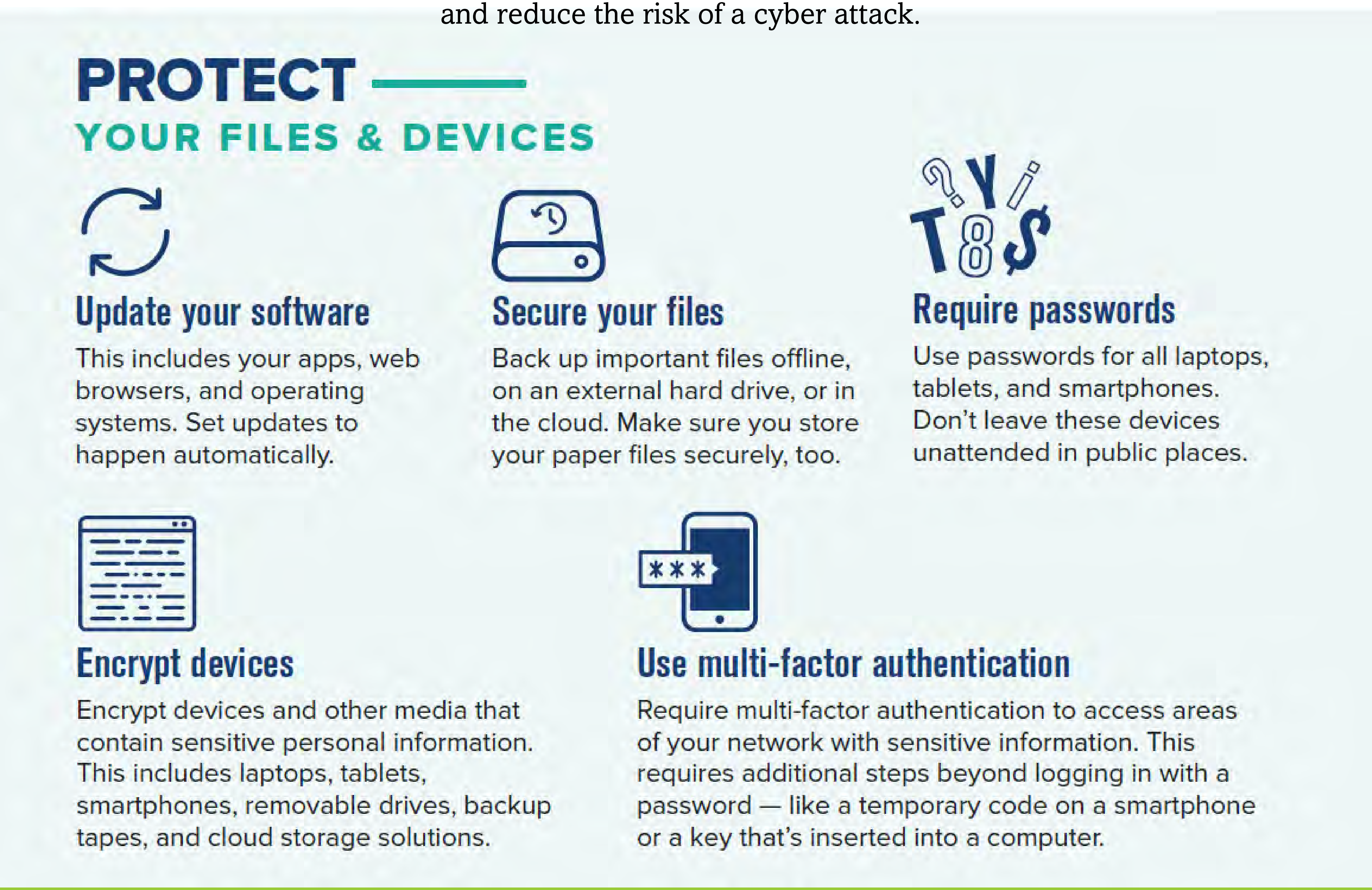
Major challenges include integrating data and other relevant information from internal departments and external organizations into useful GRC information and ensuring all GRC system users are properly trained to obtain maximum benefit from the software.

Changes in the corporate culture may be needed to accommodate the collaborative nature of the new GRC system. Periodic testing of GRC software is essential to ensure it is being properly used by internal departments. Like other critical systems, GRC software must be added to technology disaster recovery (DR) plans to ensure it remains operational in a disruptive event.

5

Cyber Security Tools

Knowing some cybersecurity basics and putting them in practice will help you protect your business and reduce the risk of a cyber attack.



PROTECT

YOUR FILES & DEVICES

Update your software

This includes your apps, web browsers, and operating systems. Set updates to happen automatically.

Secure your files

Back up important files offline, on an external hard drive, or in the cloud. Make sure you store your paper files securely, too.

Require passwords

Use passwords for all laptops, tablets, and smartphones. Don't leave these devices unattended in public places.

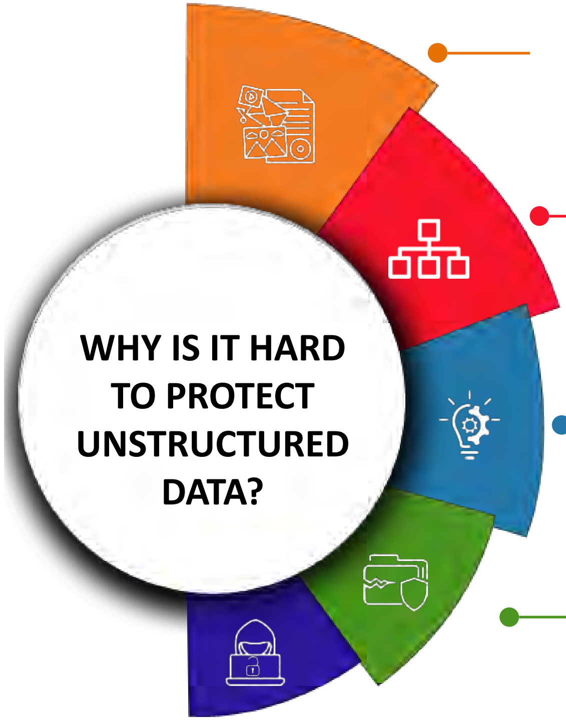
Encrypt devices

Encrypt devices and other media that contain sensitive personal information. This includes laptops, tablets, smartphones, removable drives, backup tapes, and cloud storage solutions.

Use multi-factor authentication

Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password — like a temporary code on a smartphone or a key that's inserted into a computer.

Current Status of Unstructured Data Protection



WHY IS IT HARD TO PROTECT UNSTRUCTURED DATA?

Unstructured data is **easy to create**, has **low visibility**, is **easily moved** around within and outside the organization and is therefore **hard to protect**

With today’s **connected enterprises**, endpoint devices (laptops, desktops, smartphones, etc.) have become gateways into an organization’s critical assets. Data protection has become more difficult in these widely distributed networks.

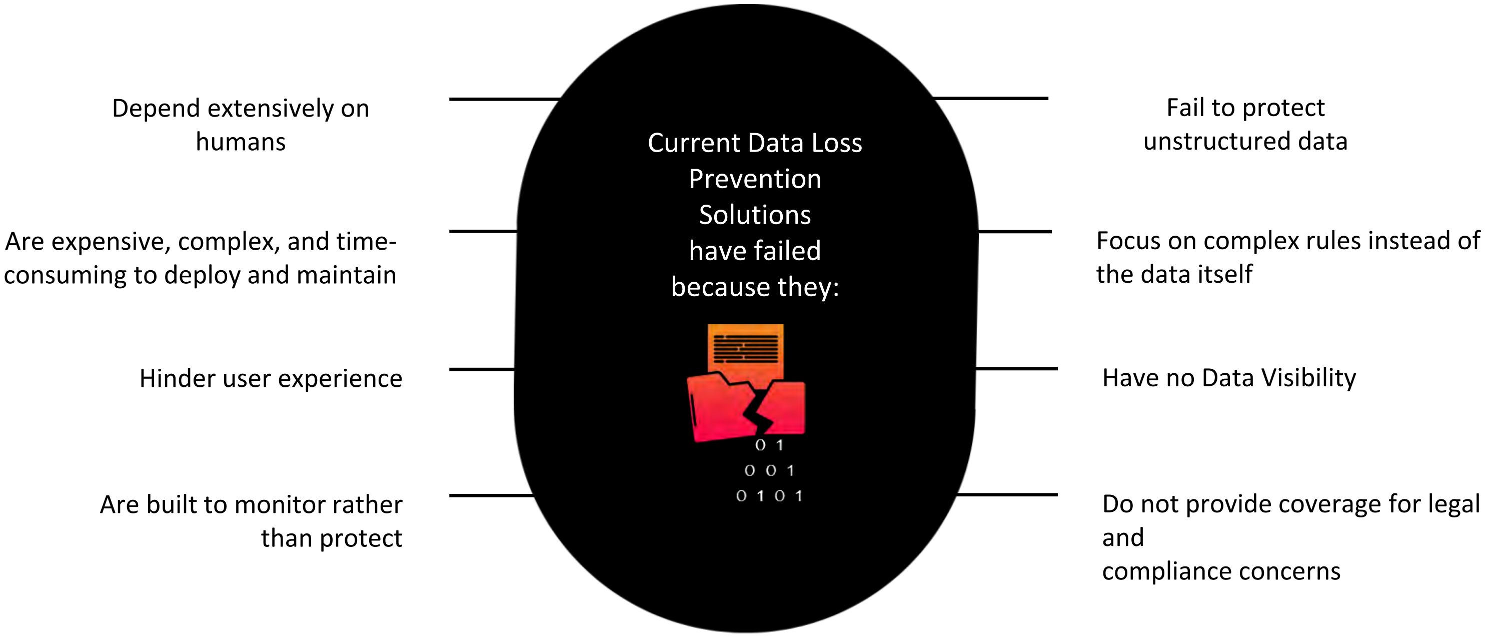
Lack of **technological innovation, human resources**, **knowledge, time, cost** and **quality user experience** make data security a nightmare

Implementing a well designed and constantly evolving “**Data Security by Design & Default” system is hard** for most organizations – It **takes focus away** from their primary business and **increases costs**

https://www.titanfile.com/blog/15-important-cybersecurity-statistics-in-2021/ - https://legaljobs.io/blog/privacy-statistics/ - -loss-statistics/ National Archives & Records Administration in Washington DC. -https://ontech.com/data-backup-sta

Current Data Security Failures

Hackers have developed malwares that exploit these weaknesses and get to your unstructured data.

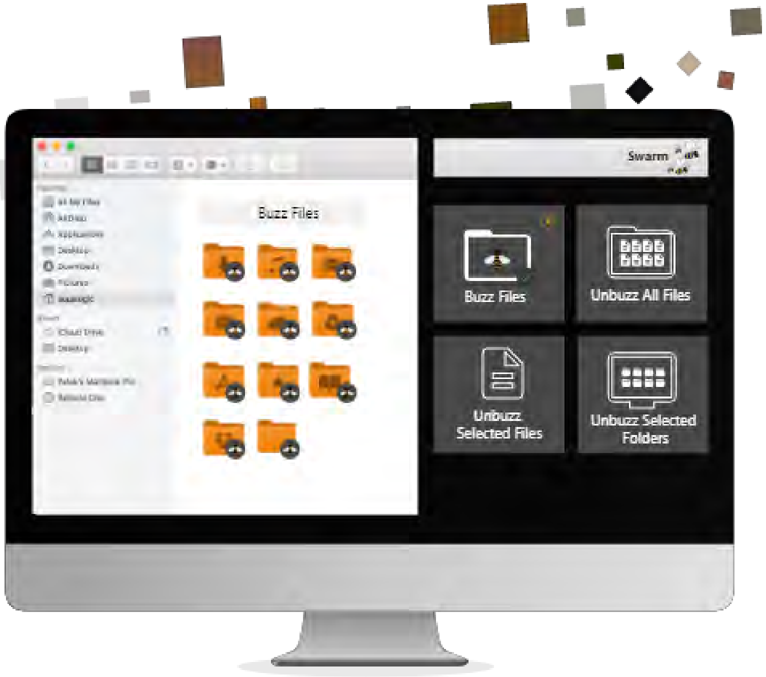


Current Data Loss Prevention Solutions have failed because they:

- Depend extensively on humans
- Are expensive, complex, and time-consuming to deploy and maintain
- Hinder user experience
- Are built to monitor rather than protect
- Fail to protect unstructured data
- Focus on complex rules instead of the data itself
- Have no Data Visibility
- Do not provide coverage for legal and compliance concerns

Introducing Autnhive

Autnhive
Automating Data Security & Privacy



Protect Your Data and Privacy,
Before it’s Lost.
Swarm simplifies data protection and privacy, to avoid costly data loss/leak and corporate espionage.

Shockingly Simple, Fiercely Powerful.

Enjoy military grade data protection without the complexities.

Automated Data Protection Simplified

- ❑ Automatically locate, protect and backup your sensitive data so you do not loose it.

Discover The Ultimate Smart Data Protection

- ❑ Protect and Privatize Your Data Everywhere.

Easy to Use, Continual Data Protection & Privacy

- ❑ With 600% increase in hacking, who has time and resources to constantly track if your files are protected and privatized?

Protect, Privatize and Consolidate your data

- ❑ Swarm centralizes this level of data control for you, so you don't have to worry.

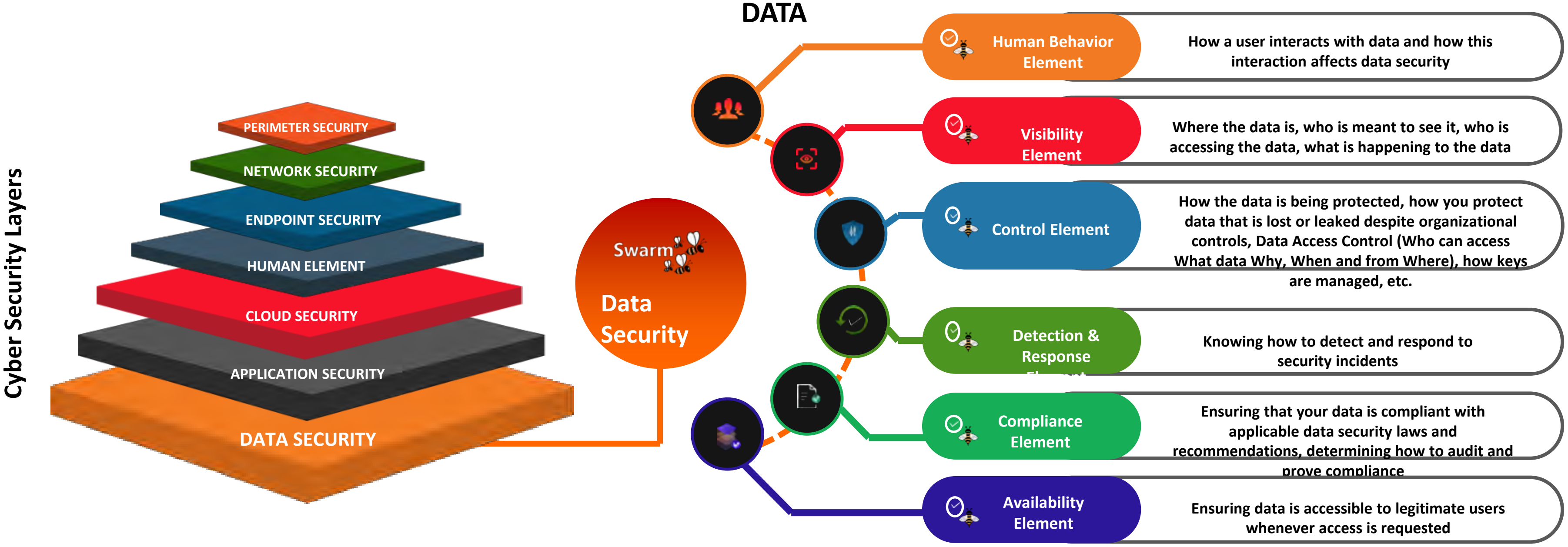
Smart Data Restoration

Effortless Data Tracking, Reporting and Compliance.

Decisive Data Security

SWARM

DECISIVE SECURITY FOR YOUR UNSTRUCTURED DATA



Cyber Security Layers

PERIMETER SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

HUMAN ELEMENT

CLOUD SECURITY

APPLICATION SECURITY

DATA SECURITY

Swarm Data Security

Human Behavior Element — How a user interacts with data and how this interaction affects data security

Visibility Element — Where the data is, who is meant to see it, who is accessing the data, what is happening to the data

Control Element — How the data is being protected, how you protect data that is lost or leaked despite organizational controls, Data Access Control (Who can access What data Why, When and from Where), how keys are managed, etc.

Detection & Response Element — Knowing how to detect and respond to security incidents

Compliance Element — Ensuring that your data is compliant with applicable data security laws and recommendations, determining how to audit and prove compliance

Availability Element — Ensuring data is accessible to legitimate users whenever access is requested

To implement these elements of data security, companies face challenges with technology, Human Resources, knowledge, time, cost and user experience.

PROTECTING PEOPLE – MAKING ELECTRONIC SECURITY A REALITY FOR EVERYONE

Swarm – **Decisive** Data Security

DATA PROTECTION BY "DESIGN & DEFAULT"
Integrate or 'bake in' proactive data protection throughout your everyday business activities rather than having data protection as an afterthought.

ENSURE PRIVACY & CIA
Ensure the Privacy, Confidentiality, and Integrity of your data by automatically implementing CISA and FBI recommendations for ransomware protection.

ACCESS CONTROL
Manage data on a granular file level.

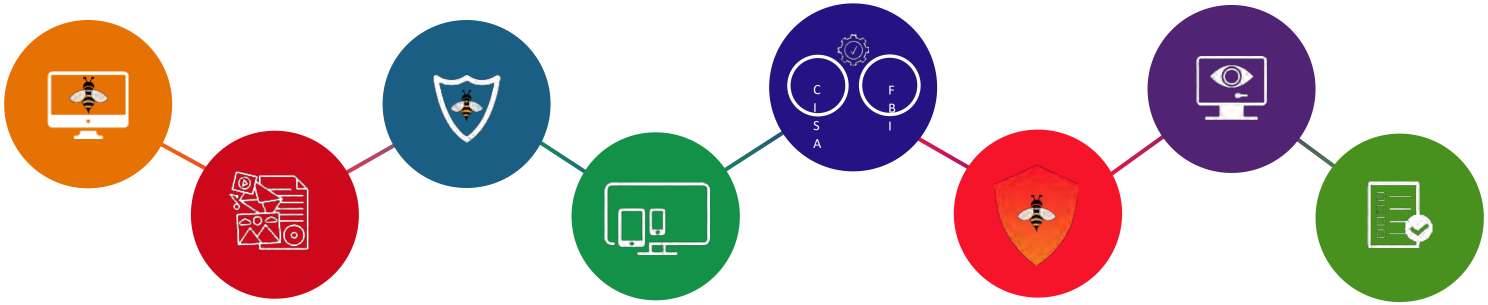
DECREASE DATA SECURITY COST
Automate data level security. Reduce the cost of data security and the cost of breaches.

INCREASE DATA VISIBILITY & CONTROL
Ensure the stakeholders of your data (owner & custodians) have full visibility and control over your data, enabling good Data Access Governance.

AUDITABLE COMPLIANCE
Rapidly become compliant with laws and recommendations such as HIPPA, GDPR, CPRA, NIST 800-207 (Zero Trust). Provide auditable reports for your unstructured data.

DETECT & RESPOND TO DATA THREATS
Know how and when your data is being attacked and respond decisively.

How It Works



Automatically Crawl your systems and mounted drives

Automatically Discovers and Indexes your unstructured data

Enables Granular Data Level Security Controls, as recommended by the law.

Delink Data & Device for further protection

Automatically deploys CISA & FBI recommendations for ransomware protection

Automatically detect & respond to unstructured data threats

User gains full protection, control and visibility of their unstructured data at a granular file level

User gets auditable compliance (HIPPA, GDPR, CPRA, NIST Zero Trust, State and Federal Encryption laws etc.)

PROTECTING PEOPLE – MAKING ELECTRONIC SECURITY A REALITY FOR EVERYONE

nathansuyi@gmail.com

Dr. Nathaniel **ATANSUYI**, FIIM, MNCS, MCPN (C.itp)

IT Advisory & Consulting | Analytics & Insights | Automation & AI | IOT, Cloud & Digital Technology | Cyber Security | Coach | Author

IT Advisory & Consulting | Analytics & Insights | Automation & AI | IOT, Cloud & Digital Technology | Cyber Security | Coach |Author

Autnhive
Automating Data Security & Privacy

DATAPLUS
GLOBAL SERVICES

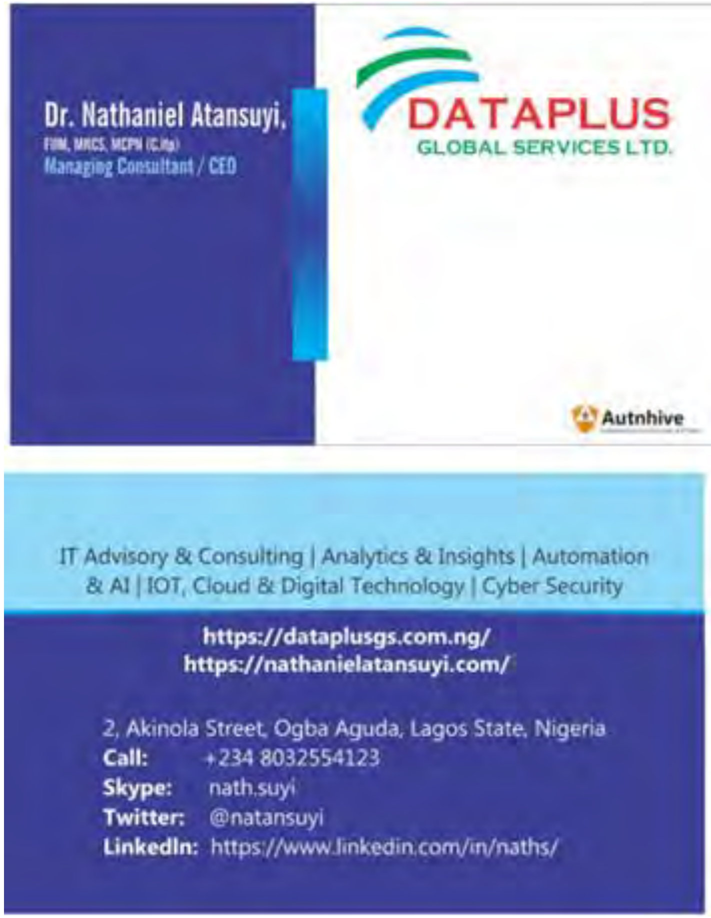
…for data access prevention

CISCO | DUO

…for data protection

Autnhive
Automating Data Security & Privacy

Contact:



Dr. Nathaniel Atansuyi,
FIIM, MNCS, MCPN (C.Ng)
Managing Consultant / CEO

DATAPLUS
GLOBAL SERVICES LTD.

Autnhive

IT Advisory & Consulting | Analytics & Insights | Automation & AI | IOT, Cloud & Digital Technology | Cyber Security

https://dataplusgs.com.ng/
https://nathanielatansuyi.com/

2, Akinola Street, Ogba Aguda, Lagos State, Nigeria
Call: +234 8032554123
Skype: nath.suyi
Twitter: @natansuyi
LinkedIn: https://www.linkedin.com/in/naths/

natansuyi@dataplusgs.com.ng

nathansuyi@gmail.com

+234 803 255 4123

…Work Securely Anywhere