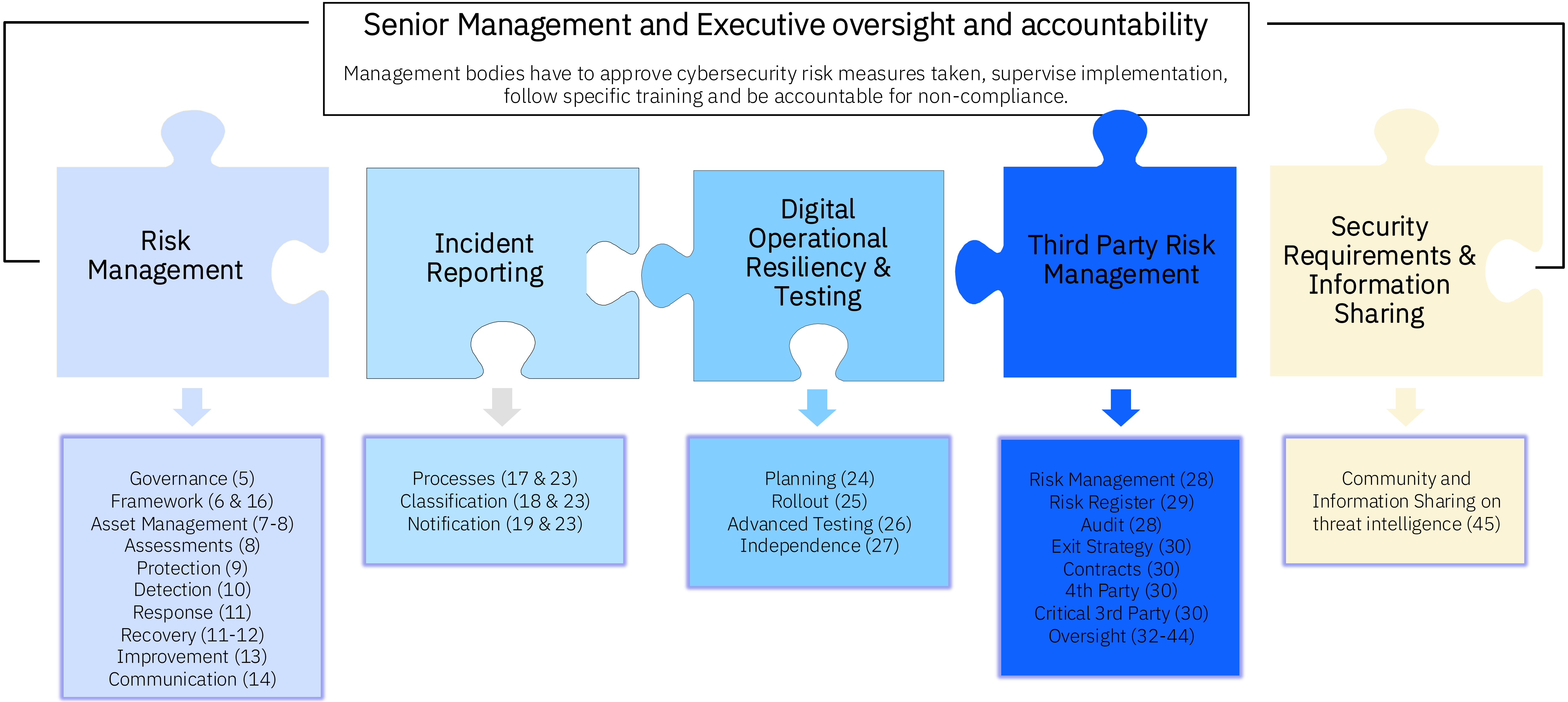
DORA – IBM’s Data Driven Approach for reducing risk, enhancing resilience and optimizing cost & Effort

Key areas that impact you



Senior Management and Executive oversight and accountability

Management bodies have to approve cybersecurity risk measures taken, supervise implementation, follow specific training and be accountable for non-compliance.

Risk Management

Governance (5)
Framework (6 & 16)
Asset Management (7-8)
Assessments (8)
Protection (9)
Detection (10)
Response (11)
Recovery (11-12)
Improvement (13)
Communication (14)

Incident Reporting

Processes (17 & 23)
Classification (18 & 23)
Notification (19 & 23)

Digital Operational Resiliency & Testing

Planning (24)
Rollout (25)
Advanced Testing (26)
Independence (27)

Third Party Risk Management

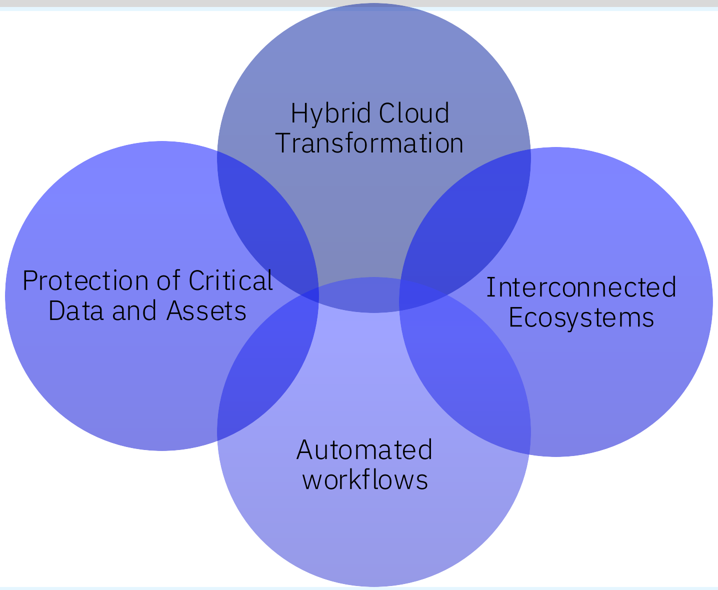
Risk Management (28)
Risk Register (29)
Audit (28)
Exit Strategy (30)
Contracts (30)
4th Party (30)
Critical 3rd Party (30)
Oversight (32-44)

Security Requirements & Information Sharing

Community and Information Sharing on threat intelligence (45)

External and internal factors are shaping the risk landscape

Business Transformation drives increased risk


Hybrid Cloud Transformation
Protection of Critical Data and Assets
Interconnected Ecosystems
Automated workflows

Security technologies are evolving exponentially

Threat landscape is rapidly evolving resulting in staggering data disruption costs → $82M Average annual impact of supply chain

Technology advancements for new and improved ways to adopt / manage AI and Gen AI.

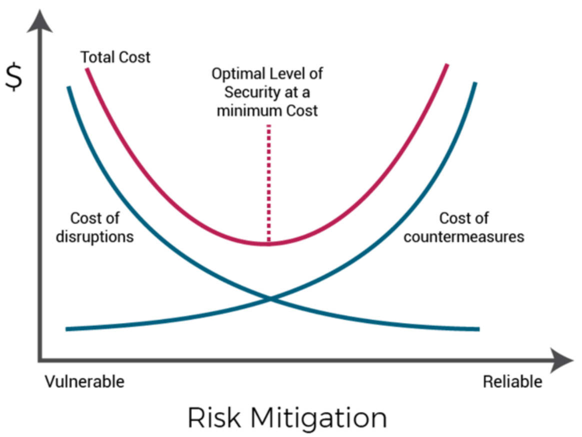
Complex and evolving regulatory risk mandates

The set of changing and emerging regulatory requirements make organizations lose an average of $5.87 Million in revenue due to a single non-compliance event.

Investments must keep pace with risks

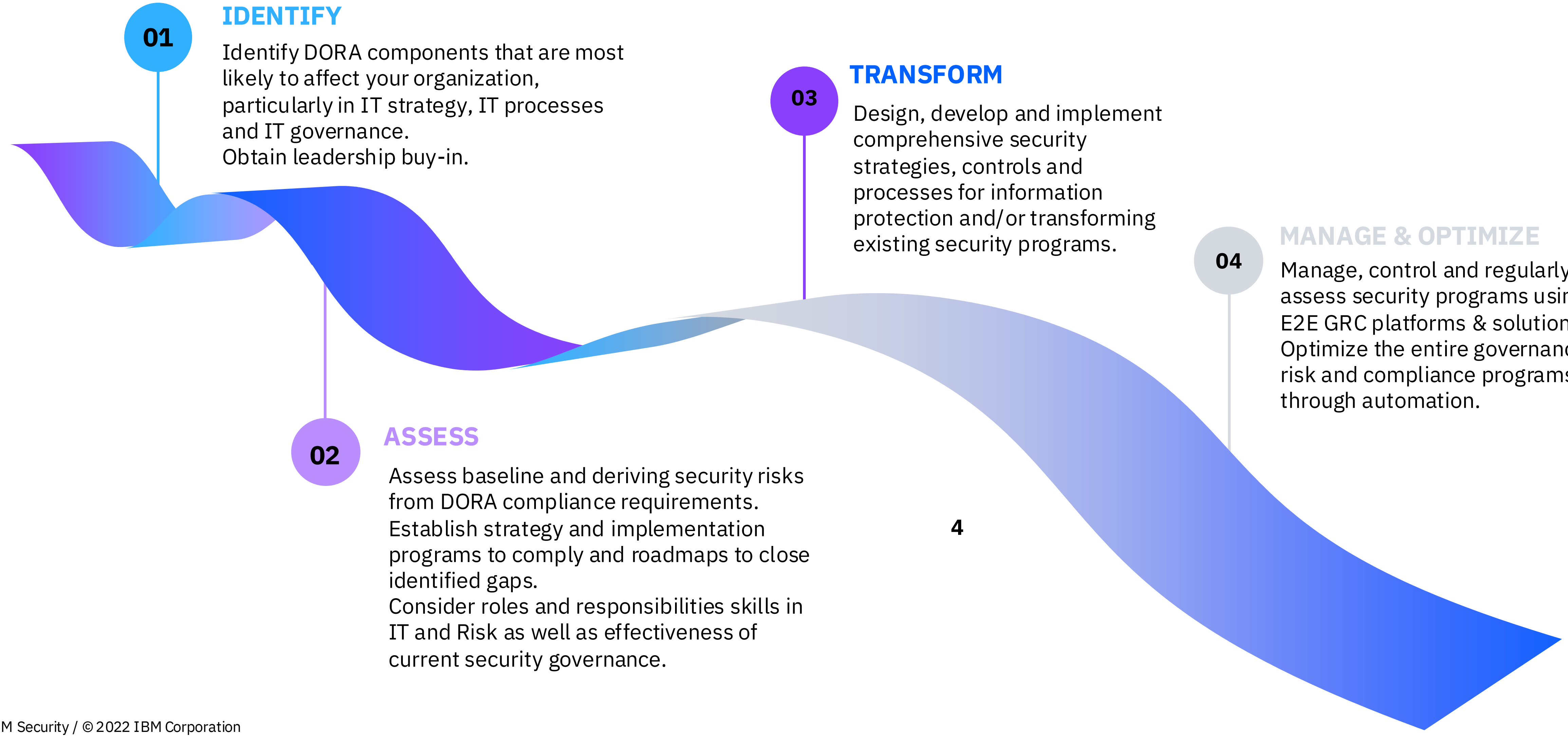
Organizations face Board level scrutiny and business pressures to demonstrate solid ROI for their cyber security practices across the Enterprise and Ecosystem.

Measuring Risk vs. Cost



IBM Security / © 2022 IBM Corporation

IBM approach addressing client needs



01 **IDENTIFY**

Identify DORA components that are most likely to affect your organization, particularly in IT strategy, IT processes and IT governance.
Obtain leadership buy-in.

02 **ASSESS**

Assess baseline and deriving security risks from DORA compliance requirements.
Establish strategy and implementation programs to comply and roadmaps to close identified gaps.
Consider roles and responsibilities skills in IT and Risk as well as effectiveness of current security governance.

03 **TRANSFORM**

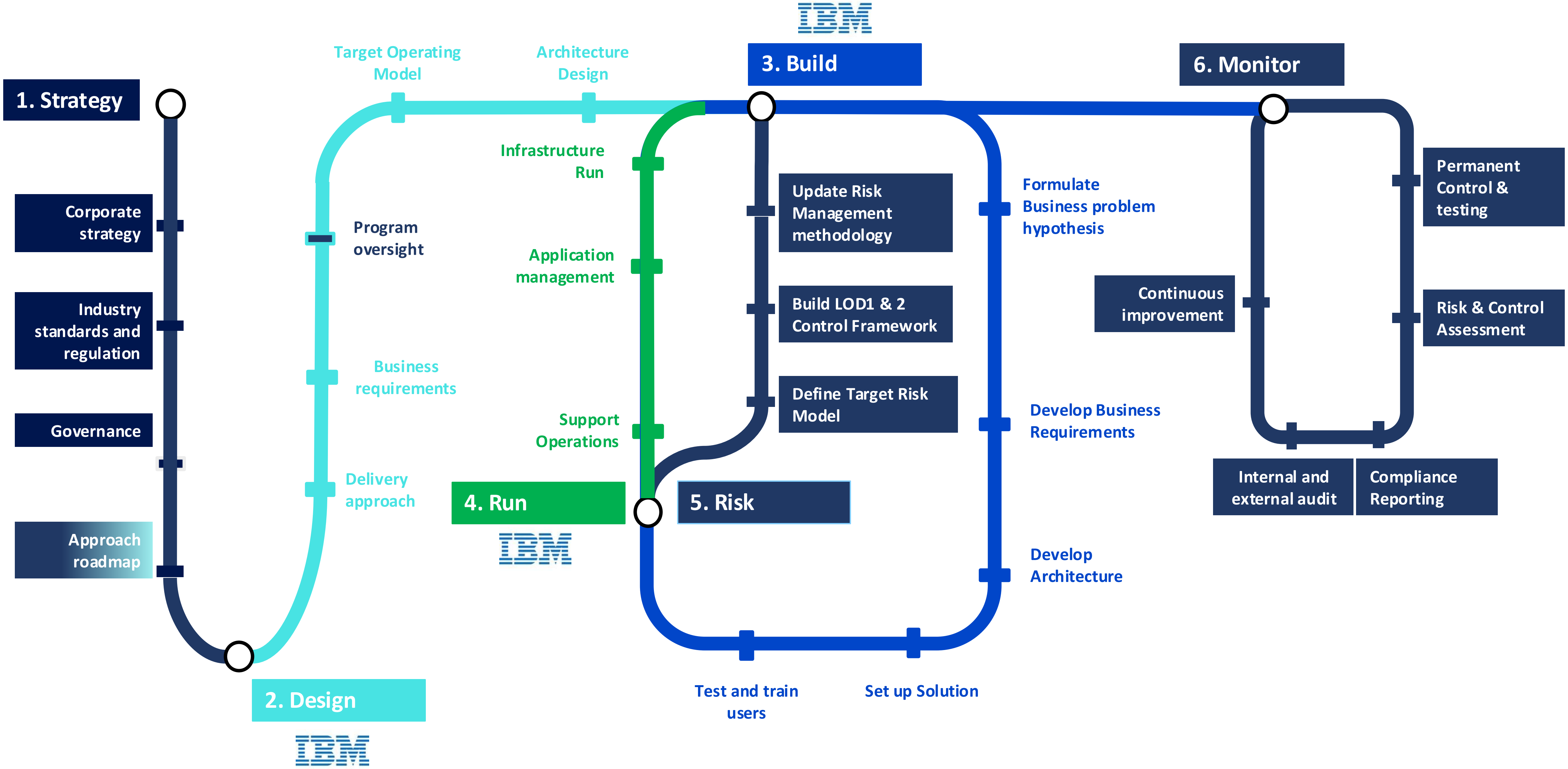
Design, develop and implement comprehensive security strategies, controls and processes for information protection and/or transforming existing security programs.

04 **MANAGE & OPTIMIZE**

Manage, control and regularly re-assess security programs using E2E GRC platforms & solutions.
Optimize the entire governance, risk and compliance programs through automation.

4

IBM approach addressing client needs



1. Strategy

Corporate strategy

Industry standards and regulation

Governance

Approach roadmap

2. Design

Target Operating Model

Architecture Design

Program oversight

Business requirements

Delivery approach

3. Build

Formulate Business problem hypothesis

Develop Business Requirements

Develop Architecture

Set up Solution

Test and train users

4. Run

Infrastructure Run

Application management

Support Operations

5. Risk

Update Risk Management methodology

Build LOD1 & 2 Control Framework

Define Target Risk Model

6. Monitor

Permanent Control & testing

Risk & Control Assessment

Compliance Reporting

Internal and external audit

Continuous improvement

OUTCOME DRIVEN

Risk Management

Incident Reporting

- Processes (17 & 23)
- Classification (18 & 23)
- Notification (19 & 23)

Digital Operational Resiliency & Testing

Third Party Risk Management

Security Requirements & Information Sharing

Challenges & Trends

Return to Overview

86% believe SOC is vital to the overall cyber security strategy

49% are dissatisfied with SOC effectiveness & 44% say ROI is reducing

Alert fatigue, lack of skills, tool sprawl and attack sophistication are key challenges

How IBM helps customers

We help customers to transform to **Next Gen SOC** that enhance existing baseline through standardisation & optimisation to support next gen capabilities and provide world-class modern SOC service.

1 Transformation Services

Strategy & Design: Develop a robust strategy, modernise blueprint & develop outcome driven roadmap

Implement: A people, process & technology-based approach to implement the modern SOC and integrate across the enterprise landscape

Migration: In scenarios where customers need help to transform to a new detection platform, we can assist in developing the strategy and accelerating the migration.

2 Managed Security Services

IBM X-Force Threat Management: A programmatic & shared services model that delivers cutting edge Threat Management outcomes leveraging AI/ML and automation for IBM Cloud Pak for Security (CP4S), QRadar, Splunk & Azure Sentinel.

Bespoke Managed SOC Services: For customers that need a dedicated model due to business or regulatory concerns, we offer managed services that enhance customer’s existing platform & processes.

Cloud Native SOC Services: For customers that want to leverage existing investments and retain innovation, we offer managed services on QRadar-on-Cloud, Azure Sentinel, Google Chronicle

OUTCOME DRIVEN

Risk Management

Incident Reporting

Digital Operational Resiliency & Testing

- Planning (24)
- Rollout (25)
- Advanced Testing (26)
- Independence (27)

Third Party Risk Management

Security Requirements & Information Sharing

Challenges & Trends

Only 31% of enterprises have SLAs around vulnerability remediation

Over 50% of the vulnerabilities are not remediated due to lack of budget & resources

Only 26% of companies are conducting monthly security related exercises

How IBM helps customers

Risk-based vulnerability management and penetration testing reduces attack surface and minimises the number of entry points and indicators of exposure for an enterprise.

1 Risk-based Vulnerability Mgmt.

IBM helps prioritise remediation of the most relevant vulnerabilities that impact the business:

- Advisory Services – Maturity & gap assessment
- Risk-based VMS Program Rollout – Coverage across infrastructure, IoT/OT, Cloud, Applications
- Vulnerability & Remediation Managed Services – Prioritisation, Risk-based remediation with oversight and tracking of top ranked vulnerability remediation.

2 Pen Testing

IBM managed Penetration testing program covers applications, networks, hardware and personnel to uncover vulnerabilities exposing your most important assets to an attack.

In addition, IBM specialty penetration testing services cover:

- IoT device testing
- Hybrid Cloud testing
- ATM security testing
- Automotive testing
- Industrial Control Systems testing
- Blockchain testing

X-Force Red

3 Red Teaming

IBM uses advanced threat emulation, we evaluate your security operation (blue) team’s detection, response and defence capabilities.

IBM uses stealth and evasion techniques to steal or modify key information, build custom payloads and command and control (C2) frameworks to achieve the objective.

After the exercise, IBM X-Force Red hackers provide unbiased feedback and explanation of the processes used that helps customer Blue/Purple team.

X-Force Red

OUTCOME DRIVEN

Risk Management

Incident Reporting

Digital Operational Resiliency & Testing
- Planning (24)
- Rollout (25)
- Advanced Testing (26)
- Independence (27)

Third Party Risk Management

Security Requirements & Information Sharing

Challenges & Trends

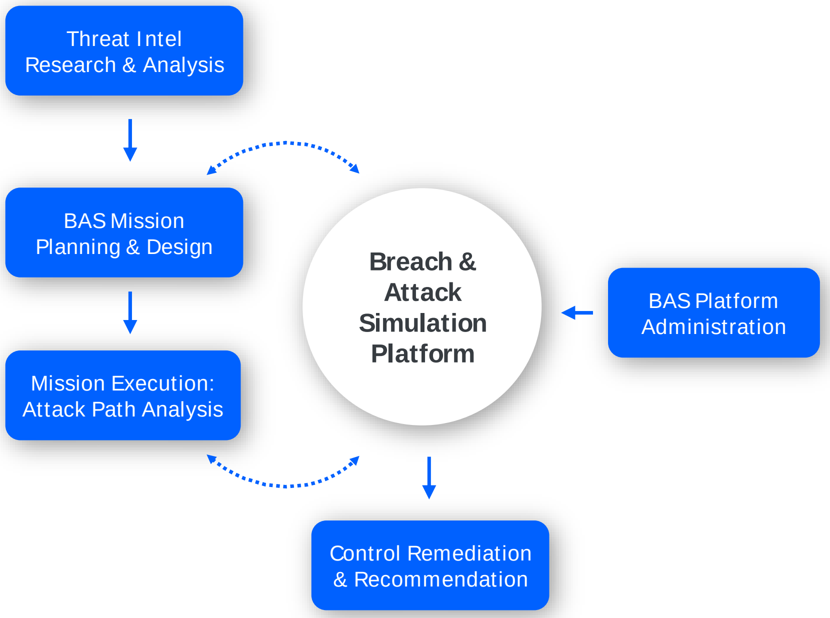
Insisting on more diligent audits won’t help understanding current security effectiveness

Penetration testing and red teaming are partial, infrequent, inconsistent and limited by creativity and available time

Frequent changes in an increasingly growing myriad of security solutions introduce error and deficiencies

How IBM helps customers

Continuous defence through **automated attack simulation.**


Threat Intel Research & Analysis
BAS Mission Planning & Design
Mission Execution: Attack Path Analysis
Breach & Attack Simulation Platform
BAS Platform Administration
Control Remediation & Recommendation

1 Mission Planning & Design

Design threat intel-based attack simulation scenarios

2 Mission Execution & Analysis

Configure technical attack scenarios & execute and analysis for blast radius and compromised assets

3 Control Recommendation & Remediation

Analysis based recommendation to deter specific techniques that are used by motivated APTs & remediation governance

4 BAS Platform Administration

Platform management, monitor agent health and upkeep of the environment

OUTCOME DRIVEN

Risk Management

Incident Reporting

Digital Operational Resiliency & Testing

- Planning (24)
- Rollout (25)
- Advanced Testing (26)
- Independence (27)

Third Party Risk Management

Security Requirements & Information Sharing

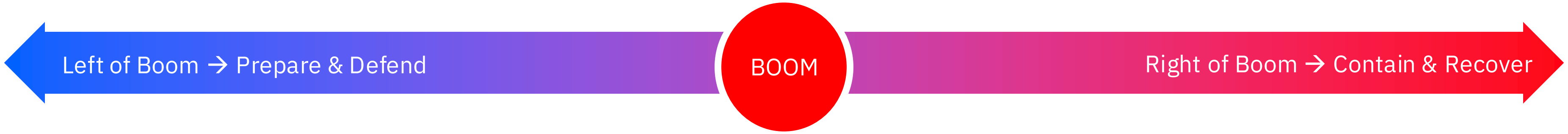
Challenges & Trends

54.8% cite shortage of staffing and skills as the biggest impediment to IR programs

50% lack the budgets for tools and technology needed to support enterprise IR programs

48.4% state that their IR programs have poorly defined processes and owners

How IBM helps customers


Left of Boom → Prepare & Defend
BOOM
Right of Boom → Contain & Recover

1 Proactive Preparation

IBM helps setup or strengthen an Incident Response capability, through the following services:

- IR program assessment
- Develop & enhance IR playbook
- IR tabletop exercise & training
- Cyber Range for Executives
- Cyber Range for IR teams

2 Rapid Response

IBM helps when you need it the most, enabling rapid 24/7 response and recovery from a cyber incident:

- Global 24/7 hotline
- IR retainer services
- Incident analysis
- Incident containment
- Incident eradication support
- Service restoration recommendations

3 Post Incident Support

IBM helps to identify the root cause of an incident and develop strategic recommendations to avoid future incidents:

- Forensics Analysis
- Support to engage with regulatory authorities & law enforcement
- Detailed incident analysis report

OUTCOME DRIVEN

Risk Management

Incident Reporting

Digital Operational Resiliency & Testing

Third Party Risk Management

- Risk Mgmt, Register & Audit (28)
- Exit Strategy & Contracts (30)
- 4th Party (30)
- Critical 3rd Party (30)
- Oversight (32-44)

Security Requirements & Information Sharing

Challenges & Trends

55% of security breaches are attributed to supply chain and third-party suppliers

62% of supply chain attacks sought to exploit the trust of customers

$4.46M is the average cost of a supply chain data breach

How IBM helps customers

IBM combines expert consultancy to design and build a comprehensive solution for a **centralized and integrated view of the supply chain ecosystem** to minimize compliance, real-time data and improved efficiencies.

IBM delivers

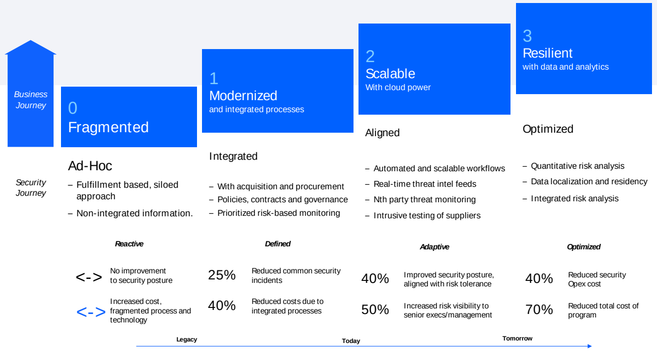
- Assess the current state of the TPRM program
- Design and improve the TPRM program
- Automate and monitor the program with a platform
- Manage and augment the program with automation and experts

Client impact

- Identify gaps and meet regulatory compliance
- Develop an effective TPRM program
- Automate processes and provide continuous vendor monitoring
- Co-source or fully outsourced program for a faster time-to-value of risk reduction initiatives

Outcomes

- Gap assessment and remediation recommendations
- Roadmap for implementation to close identified gaps
- Automated platform to provide more visibility and efficiency into the TPRM program
- Managed Security Services with TPRM experts


Business Journey
Security Journey
0 Fragmented
1 Modernized and integrated processes
2 Scalable With cloud power
3 Resilient with data and analytics
Legacy
Today
Tomorrow

Ad-Hoc
- Fulfillment based, siloed approach
- Non-integrated information.

Integrated
- With acquisition and procurement
- Policies, contracts and governance
- Prioritized risk-based monitoring

Aligned
- Automated and scalable workflows
- Real-time threat intel feeds
- Nth party threat monitoring
- Intrusive testing of suppliers

Optimized
- Quantitative risk analysis
- Data localization and residency
- Integrated risk analysis

Reactive		Defined		Adaptive		Optimized	
<->	No improvement to security posture	25%	Reduced common security incidents	40%	Improved security posture, aligned with risk tolerance	40%	Reduced security Opex cost
<->	Increased cost, fragmented process and technology	40%	Reduced costs due to integrated processes	50%	Increased risk visibility to senior execs/management	70%	Reduced total cost of program

IBM Consulting Security Services – A partner with leading advisory, systems integration and managed security services to collaborate on your strategy for success

Our expertise

- A global team of 5,500+ experts in 130 countries
- Deep industry and security domain expertise
- 1,200+ certifications in security and cloud solutions and platforms

Our practices

- Industry best practices and standard frameworks
- Design Thinking approach to bring business and security leaders together
- Solutions tailored to your specific business needs now and as your challenges evolve

Our operations

- 8 global security operations centers, 5 regional SOC locations, and local delivery capability
- 4.7T+ security events from thousands of clients analyzed per month

Our impact

Hundreds of advisory engagements delivered each year

Thousands of managed service clients protected

Market leadership in the Global + EU Forrester Wave, IDC MarketScape and Omdia reports

To find out more – some useful links

Cybersecurity Thought Leadership from IBM

“Prosper in the Cyber Economy”

“Generative AI – Cybersecurity”

“Cost of Data Breach Report”

Thank you