



Microsoft's Risk Management Approach

Abbas Kudrati

APAC Lead Chief Cybersecurity Advisor

Abbas.Kudrati@Microsoft.Com

@askudrati

<https://aka.ms/abbas>



About me

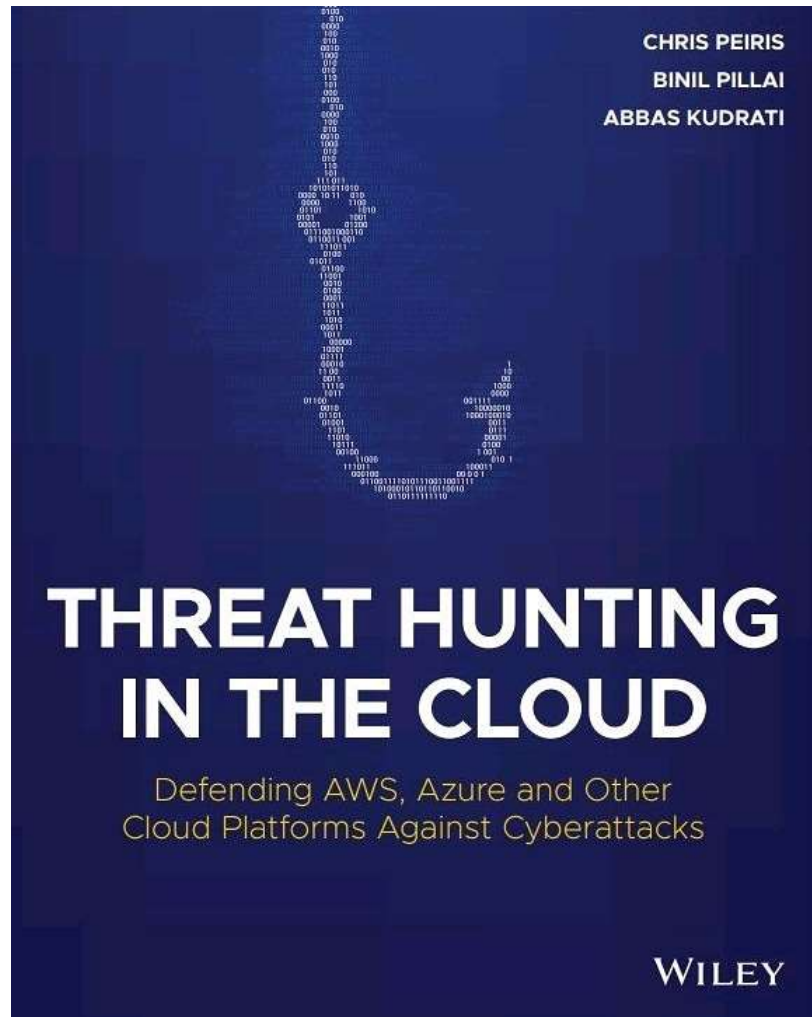
"You join Microsoft, not to be cool
but to make others cool"

Satya Nadella

- **Cybersecurity practitioner and CISO with 25 years of experience in Information / Cybersecurity.**
- **Part time Cybersecurity Professor with Deakin and LaTrobe University in Melbourne, Australia.**
- **Expertise in Zero Trust, Cybersecurity Strategy, Security Operations, Risk, Compliance, Cloud Security and Architecture.**



My books



**Releasing in Aug 2021,
Pre-order on Amazon.**



Target release by Dec 2021.

Today's risk management challenges



Cybersecurity



Data
privacy



Geopolitical
turmoil



Corruption



Financial reporting



Regulatory
reform



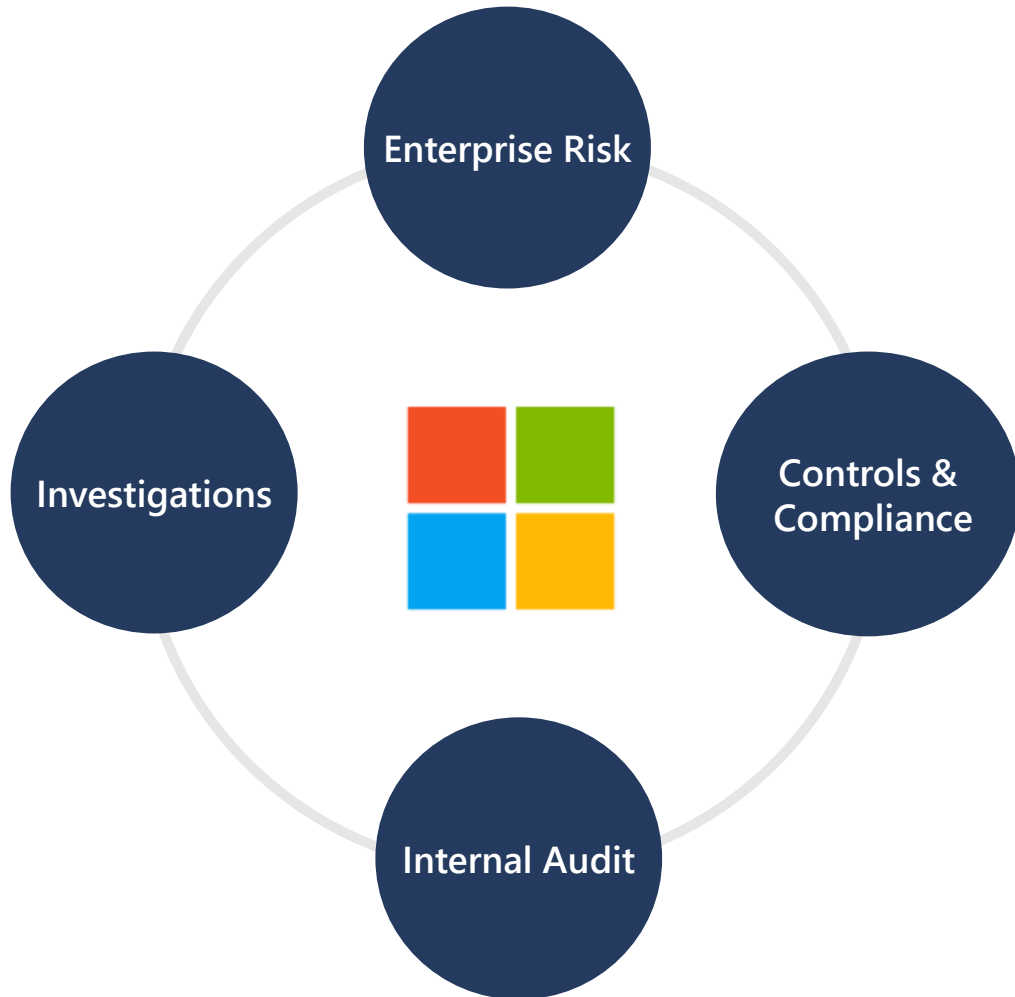
Market
instability



Software and
Service Quality
and Availability



Microsoft Audit, Risk & Compliance (ARC)

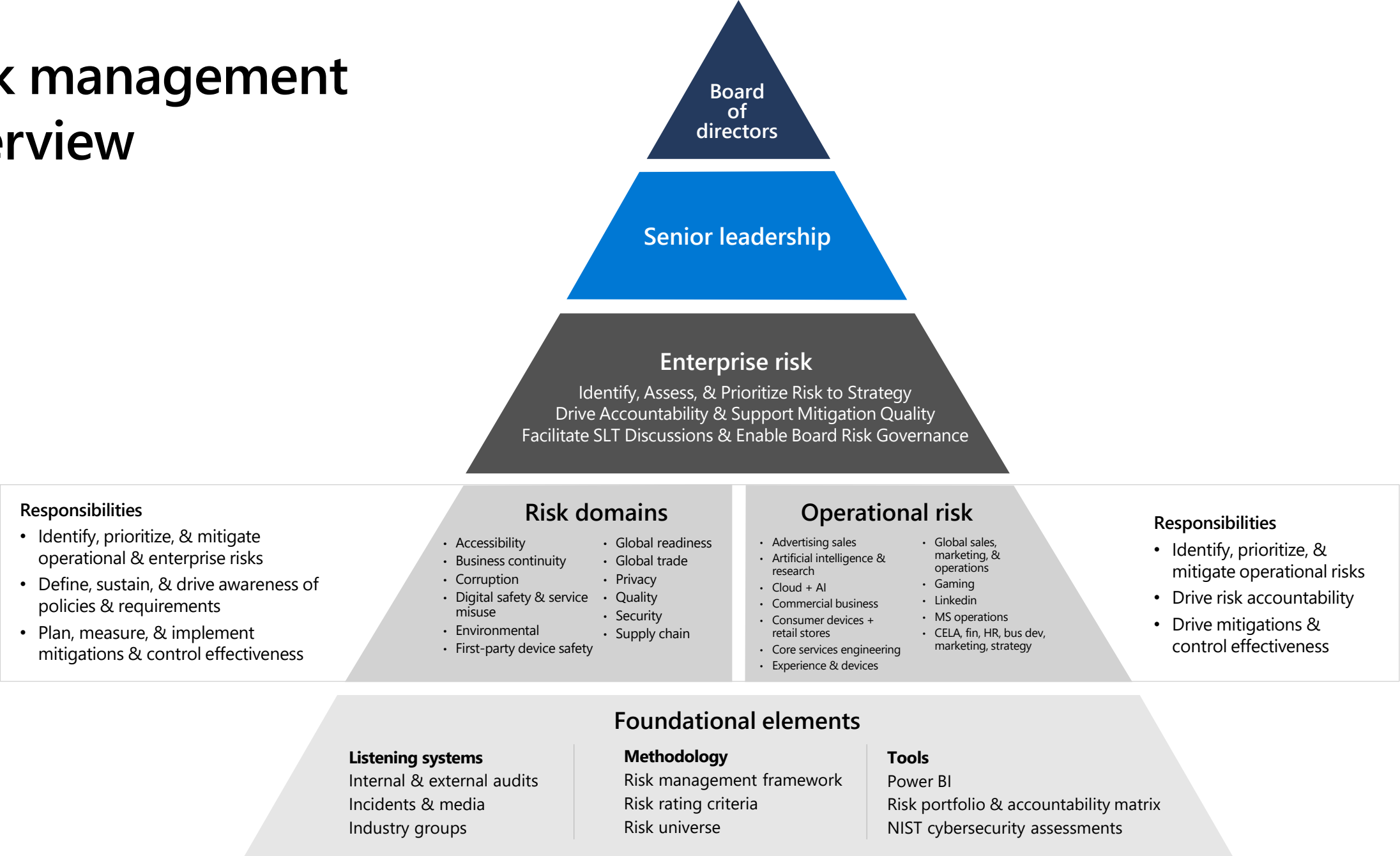


Providing advisory services and acting as the center of excellence for risk and compliance

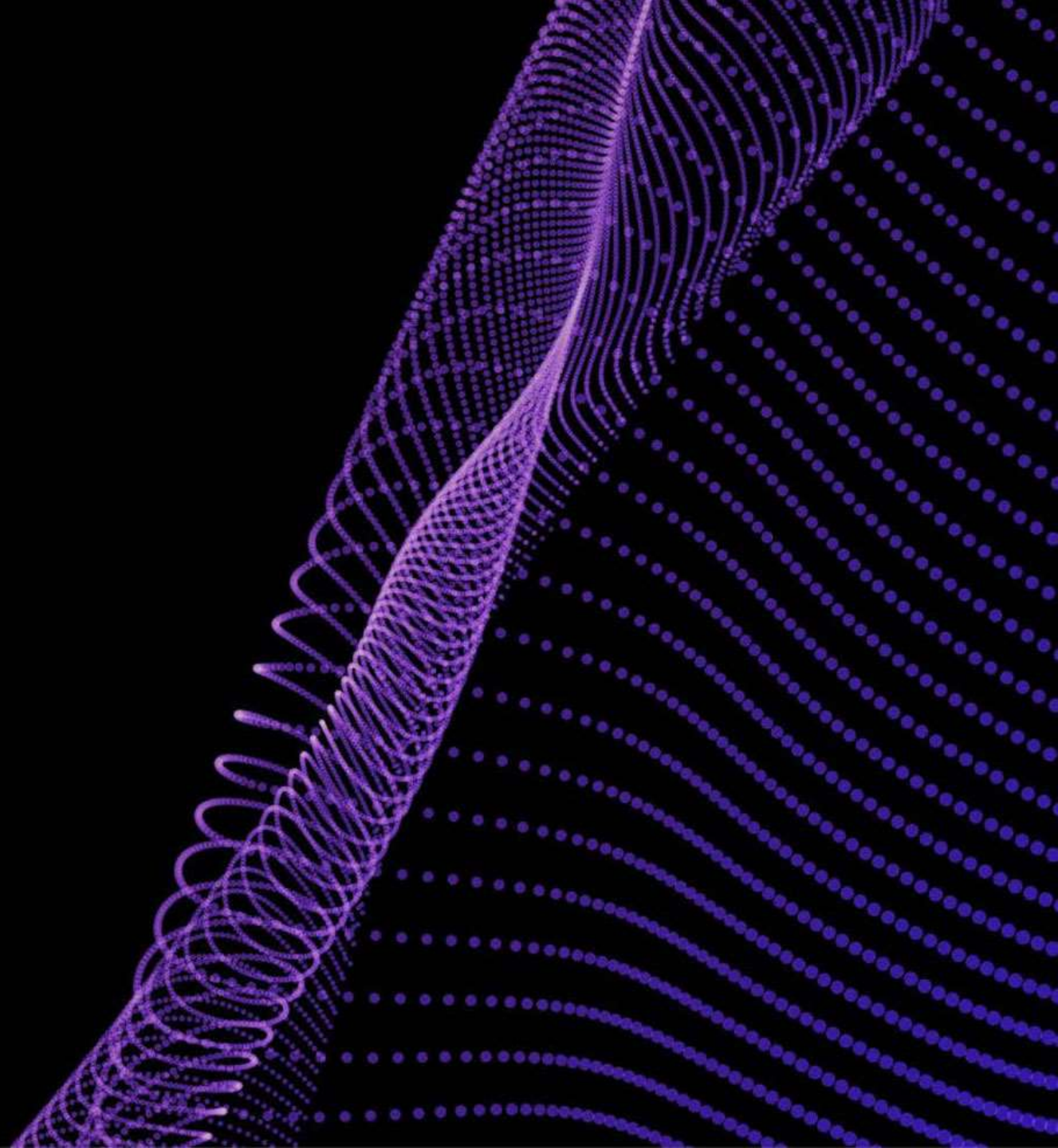
Supplying independent and objective audit and investigative services

Adopting new technologies and optimizing tools and processes to improve effectiveness and drive efficiencies

Risk management overview

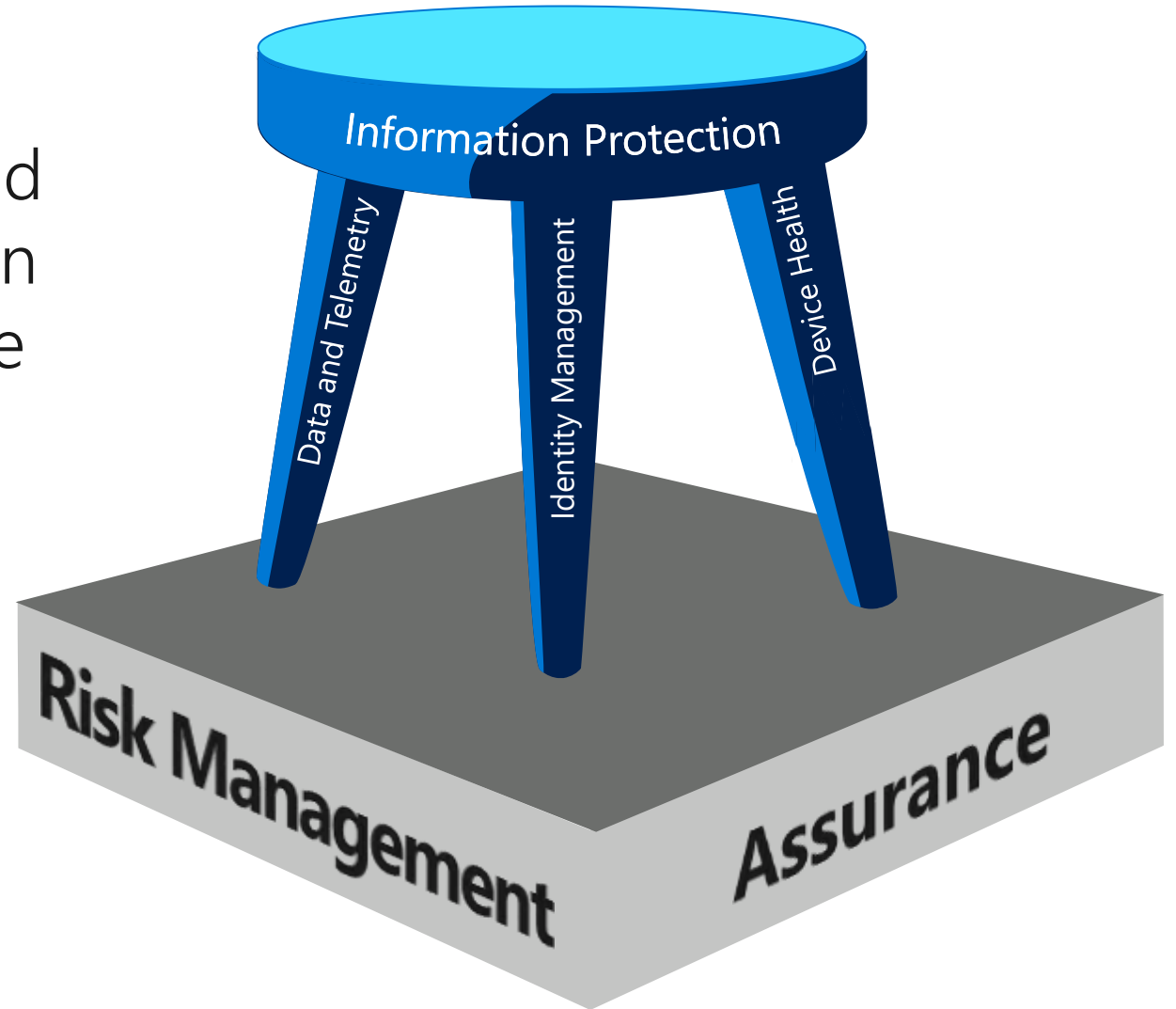


Enterprise Risk Management



Security focus

Balancing risk management, identity management, device health, data and telemetry, and information protection with risk management and assurance as the foundation.



Digital security strategy

Investment pillars



Risk Management



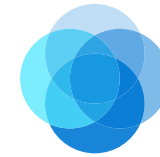
Assurance



Identity
Management



Device Health



Data & Telemetry









Information
Protection

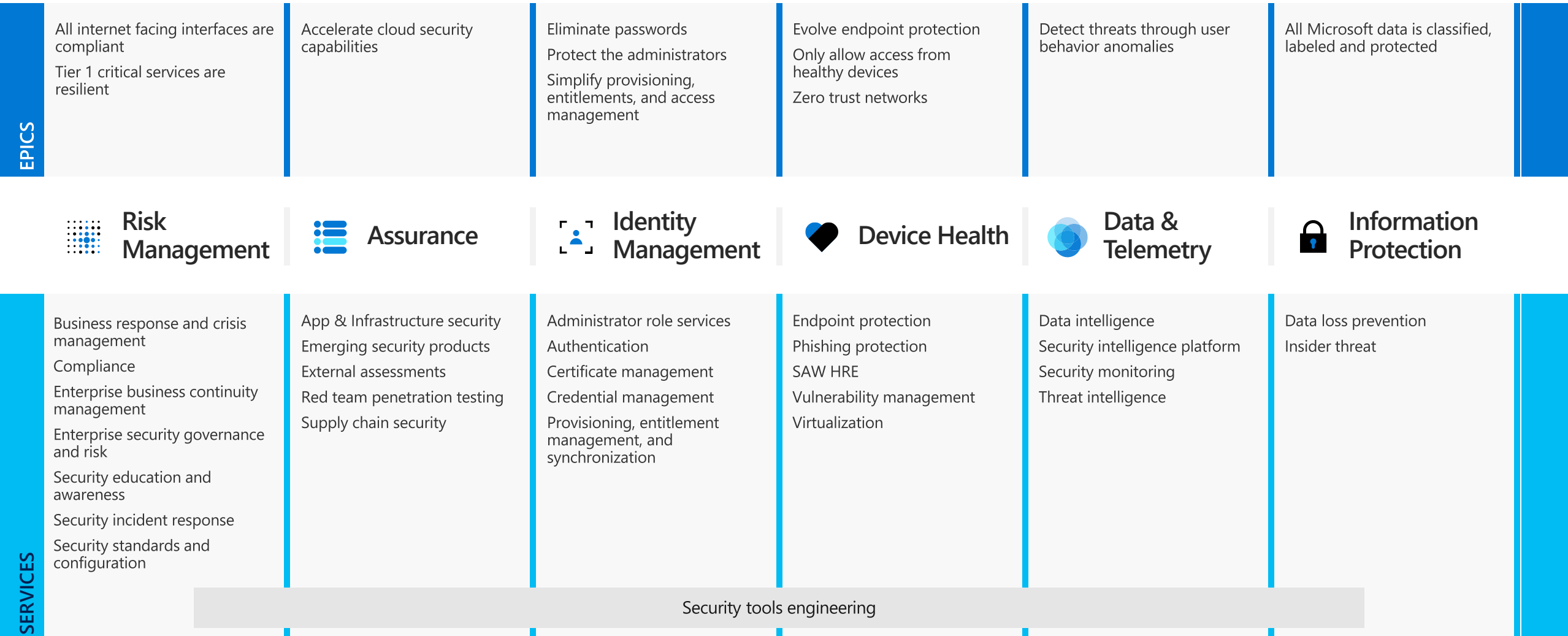
Digital security strategy



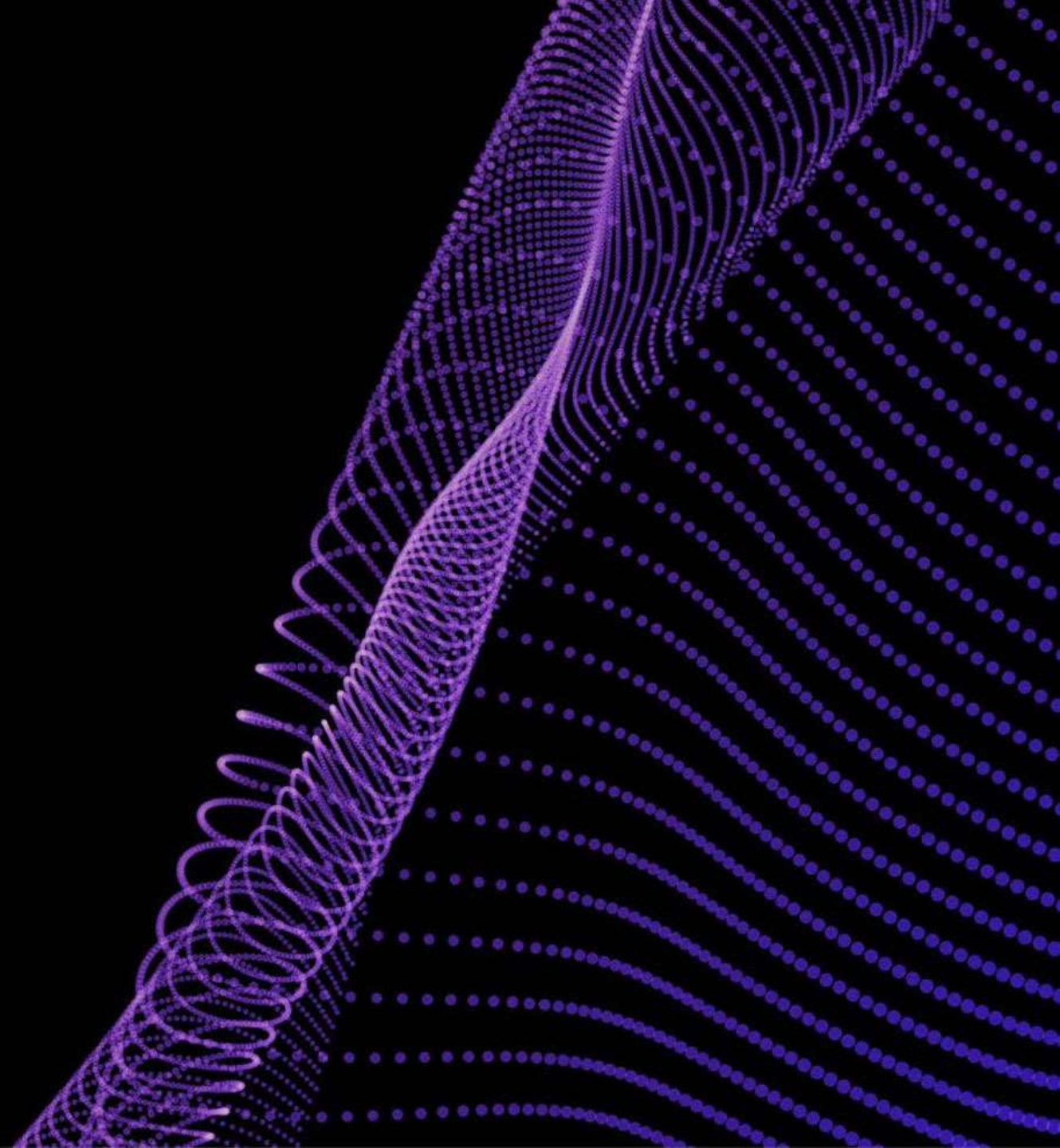
Digital security strategy

	 Risk Management	 Assurance	 Identity Management	 Device Health	 Data & Telemetry	 Information Protection
SERVICES	<div>Business response and crisis management</div> <div>Compliance</div> <div>Enterprise business continuity management</div> <div>Enterprise security governance and risk</div> <div>Security education and awareness</div> <div>Security incident response</div> <div>Security standards and configuration</div>	<div>App & Infrastructure security</div> <div>Emerging security products</div> <div>External assessments</div> <div>Red team penetration testing</div> <div>Supply chain security</div>	<div>Administrator role services</div> <div>Authentication</div> <div>Certificate management</div> <div>Credential management</div> <div>Provisioning, entitlement management, and synchronization</div>	<div>Endpoint protection</div> <div>Phishing protection</div> <div>SAW HRE</div> <div>Vulnerability management</div> <div>Virtualization</div>	<div>Data intelligence</div> <div>Security intelligence platform</div> <div>Security monitoring</div> <div>Threat intelligence</div>	<div>Data loss prevention</div> <div>Insider threat</div>
	Security tools engineering					

Digital security strategy



It starts with Risk
Management

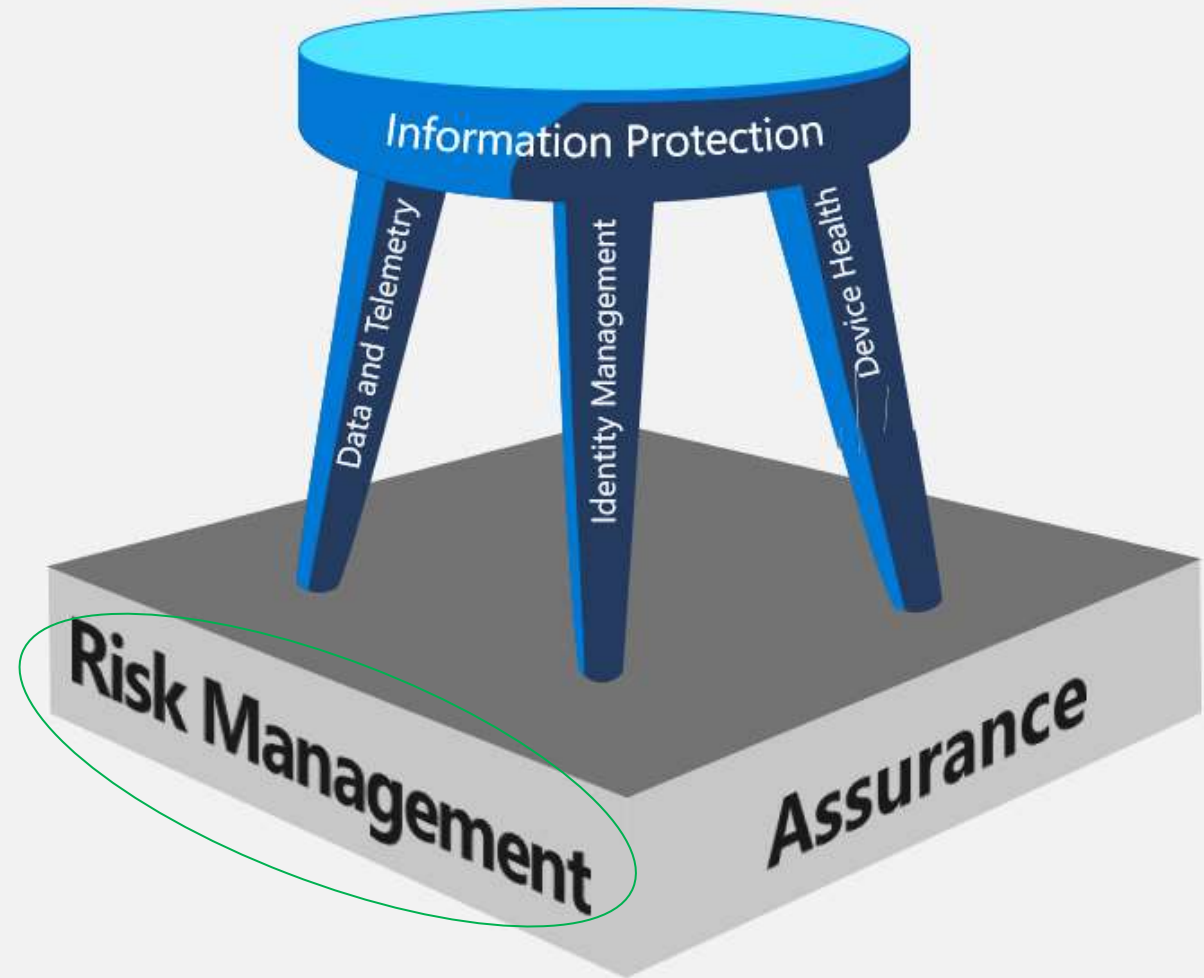


Our Risk Management focus

Risk Management forms **the foundation of our security efforts.**

We bring together security and business leadership from across Microsoft using an **established security governance model** to address Microsoft-wide **information security, general security, and privacy risks.**

This ensures a consistent approach to the **identification, mitigation, and response** for these top and emerging security risks impacting Microsoft.

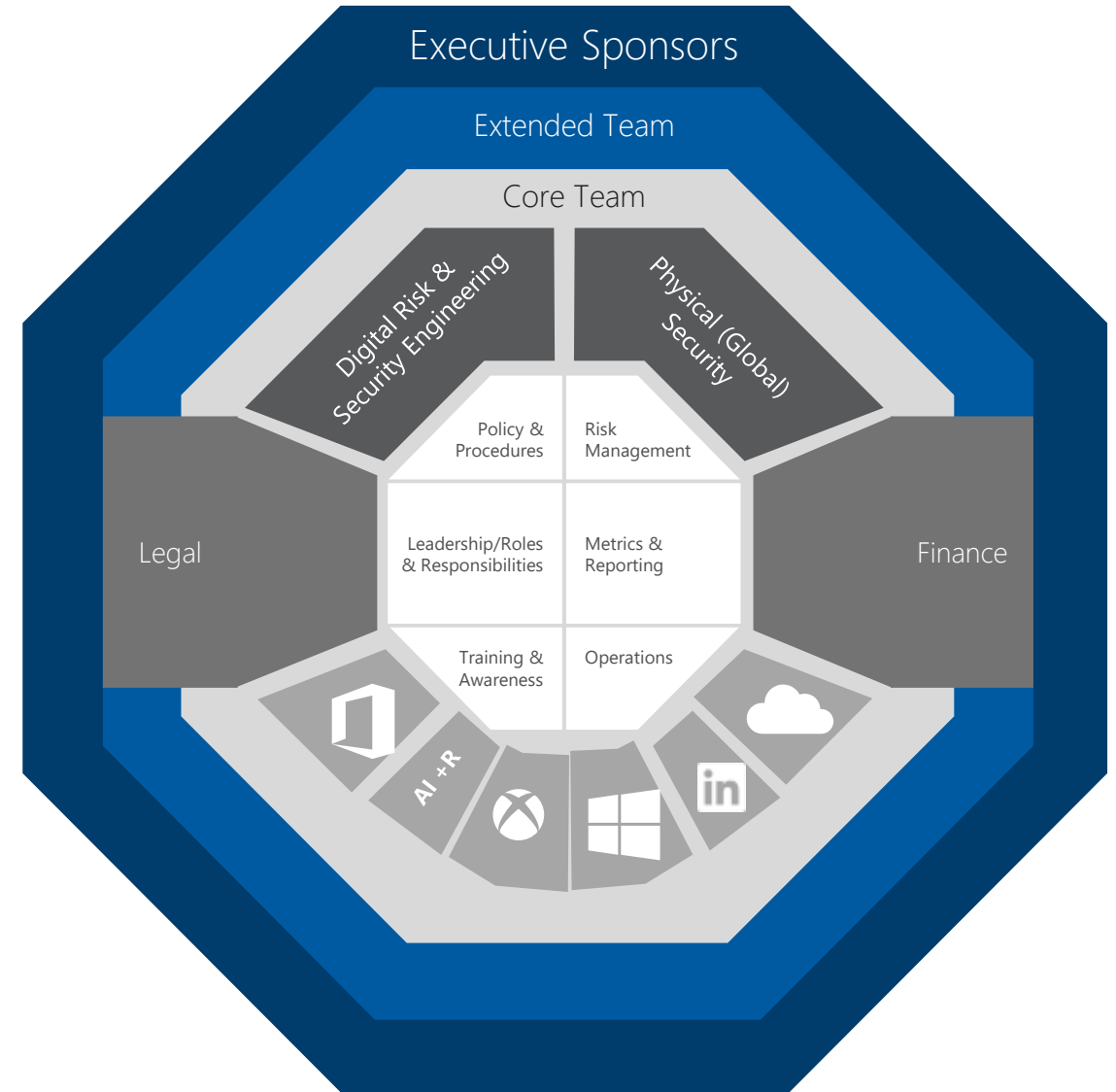


Security Governance

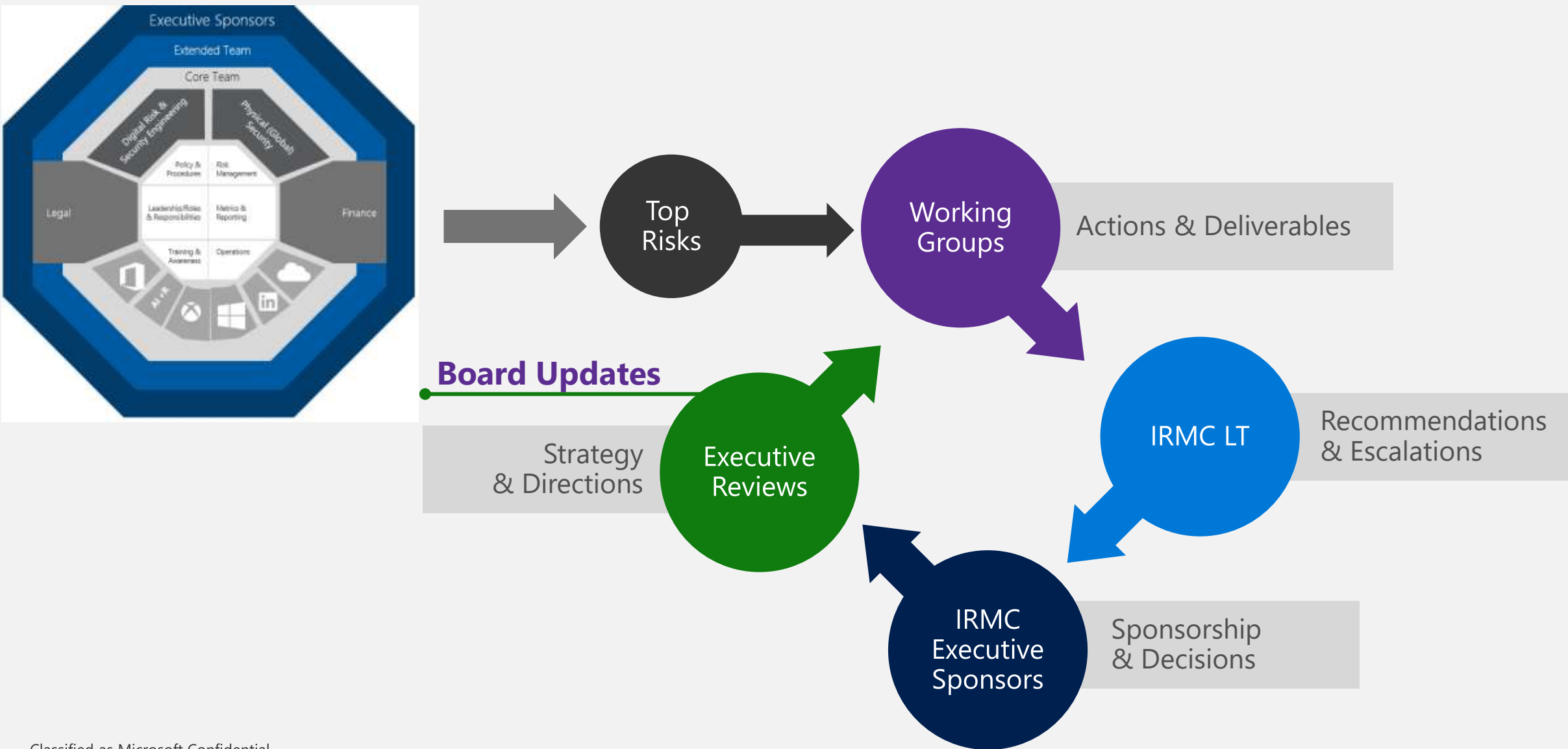
Information Risk Management Council

How do we manage enterprise risk?

The mission of the Information Risk Management Council (IRMC) program is to enable a risk-based approach for managing information security, physical security, and customer and employee privacy related matters.



IRMC Engagement



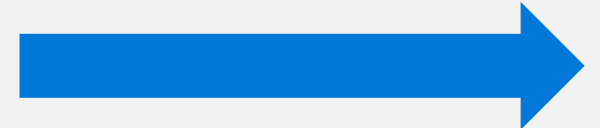
Risk Decisions – One input



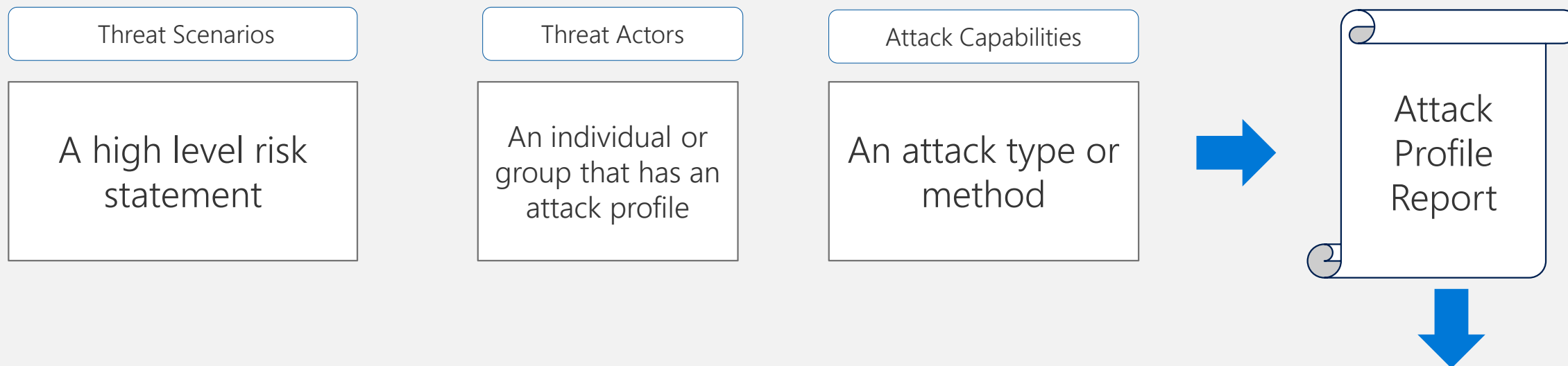
"Garbage in, Garbage out"(GIGO): in the field of [computer science](#) or [information and communications technology](#) refers to the fact that [computers](#) will unquestioningly process the most nonsensical of input data, "garbage in", and produce nonsensical output, "garbage out".

Too much data, is as big a problem as not enough.
Too much of the wrong data is worse...

We are going to use Threat Intel to help with this problem.



Threat Intel



Monitoring Program



Use Cases by Attack Stage: SAMPLE

Environment Coverage

Breadth of
detection
coverage



< 75% coverage



75% <= 50%



0% coverage

Depth of
detection
coverage

Attack Stage	Coverage										
	Windows Event Forwarding	FEP AV/AM	Fortinet	SourceFire IDS	Web Logs	Fidelis	Exchange Logs	DNS Logs	SCCM	Active Directory	Network Configuration
Reconnaissance	-	-	Y	Y	Y	-	-	-	-	-	-
Delivery	Y	Y	Y	Y	Y	Y	Y	-	-	Y	-
Exploitation	Y	Y	-	Y	Y	-	Y	-	-	-	Y
Command Control	Y	-	Y	Y	-	Y	-	Y	Y	-	-
Elevate Privileges	Y	Y	-	-	Y	-	-	-	-	Y	-
Move Laterally	Y	Y	-	-	Y	-	-	-	-	-	-
Modify or Exfiltrate Data	-	-	Y	Y	-	Y	-	-	-	-	-
Maintain Persistence	Y	Y	Y	Y	-	Y	-	-	Y	-	Y
Anti-Forensics	Y	-	-	-	-	-	-	-	-	-	-

Y = Use Case(s) Created

- = No Use Case(s) created / possible

IRMC: Risk decision making process

Pre-decision (Preparation)

1. Identify risks/exceptions
2. Classify risks/exceptions
3. Identify decision makers via a **Risk Decision Matrix**
4. Identify treatment options and recommendations

Decision making

5. Prepare for decision
6. Make decision on how we want to:
 - Improve policy/standards
 - Acknowledge
 - Mitigate
 - Monitor and measure
7. Document decision and implementation guidance

Post-decision (Implementation)

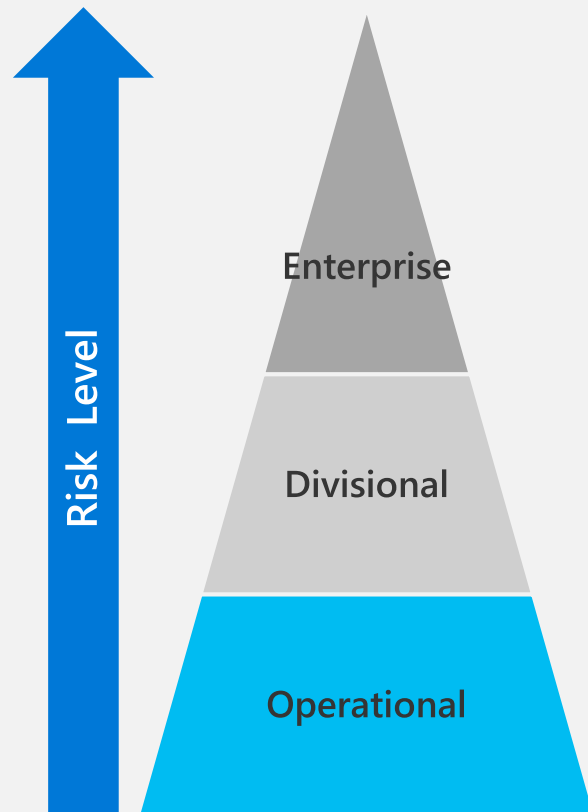
8. Mobilize and execute decision implementation
9. Track and report
10. Close/validate decision implementation











Emergency type decisions should still follow the formal process but be initiated quicker or in groups real-time via email or bridge call.

IRMC: Risk Decision Matrix

3. Identify decision makers via a Risk Decision Matrix

A Risk Decision Matrix helps identify specific stakeholders best suited to make a decision and execute on decision implementation

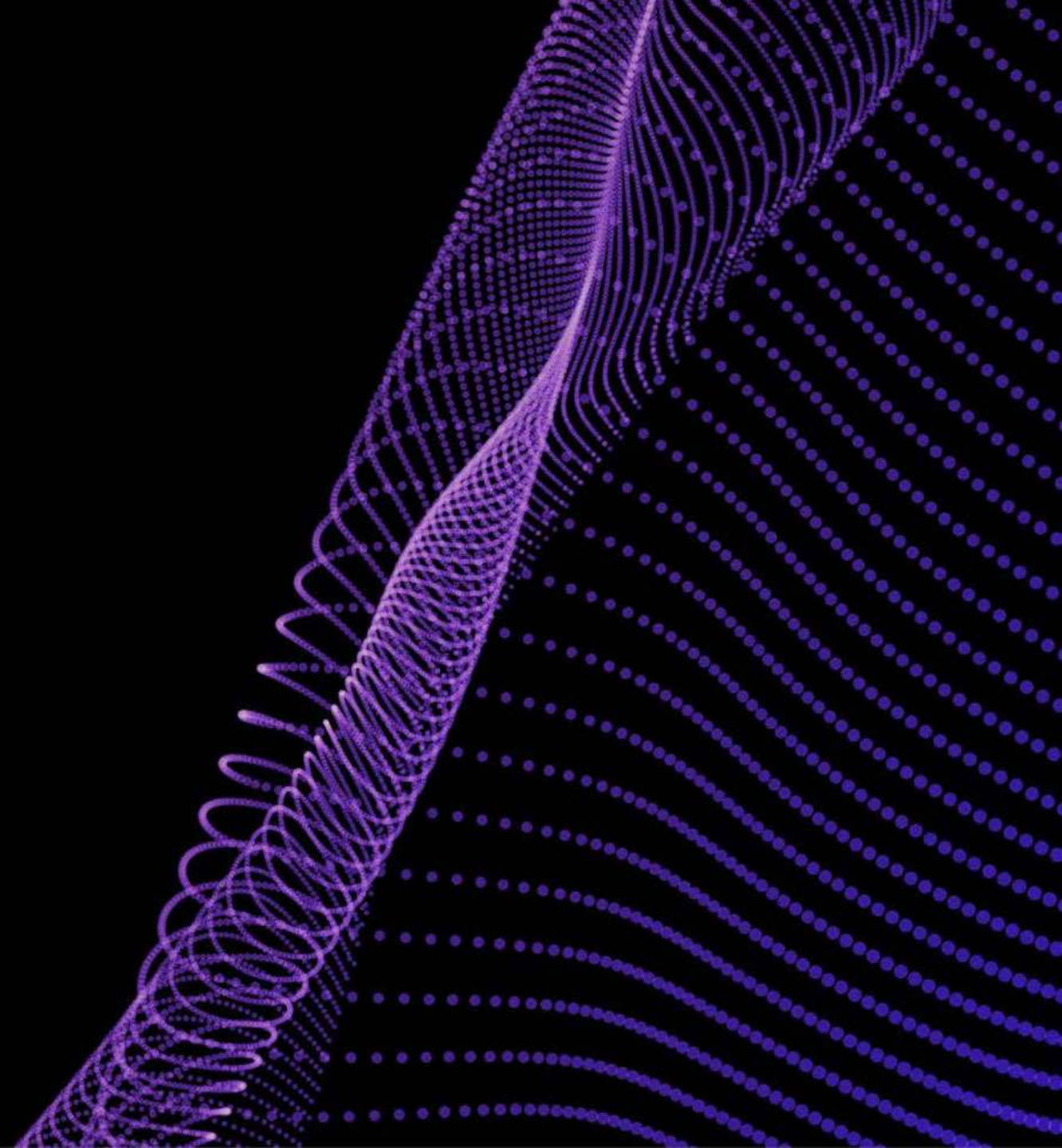


*Risk Decision Owner	Residual risk > 10	Criteria Breadth of Impact	**Business Risk Owner
 IRMC		Enterprise-wide	 EVP/CVP
 Sub-IRMC		2 or more Business Groups (BG) (e.g., WDG + OPG)	
 Business Governance Meeting (e.g. CISO)		1 BG or 2 or more sub-orgs (e.g., OPG Only, or O365 + Skype)	 CVP/VP
 Group Leader/ Manager		1 sub-org. (e.g., WDG only)	 GM/Partner

*Risk Decision Owner = Most appropriate stakeholder(s) responsible for understanding and making decisions on how to treat the risks.

**Business Risk Owner = Most appropriate stakeholder(s) accountable for understanding the risks and have the authority to acknowledge the risks

Key Metrics



Risk based audit approach

Drives our commitment to trust



Corruption



Financial Reporting



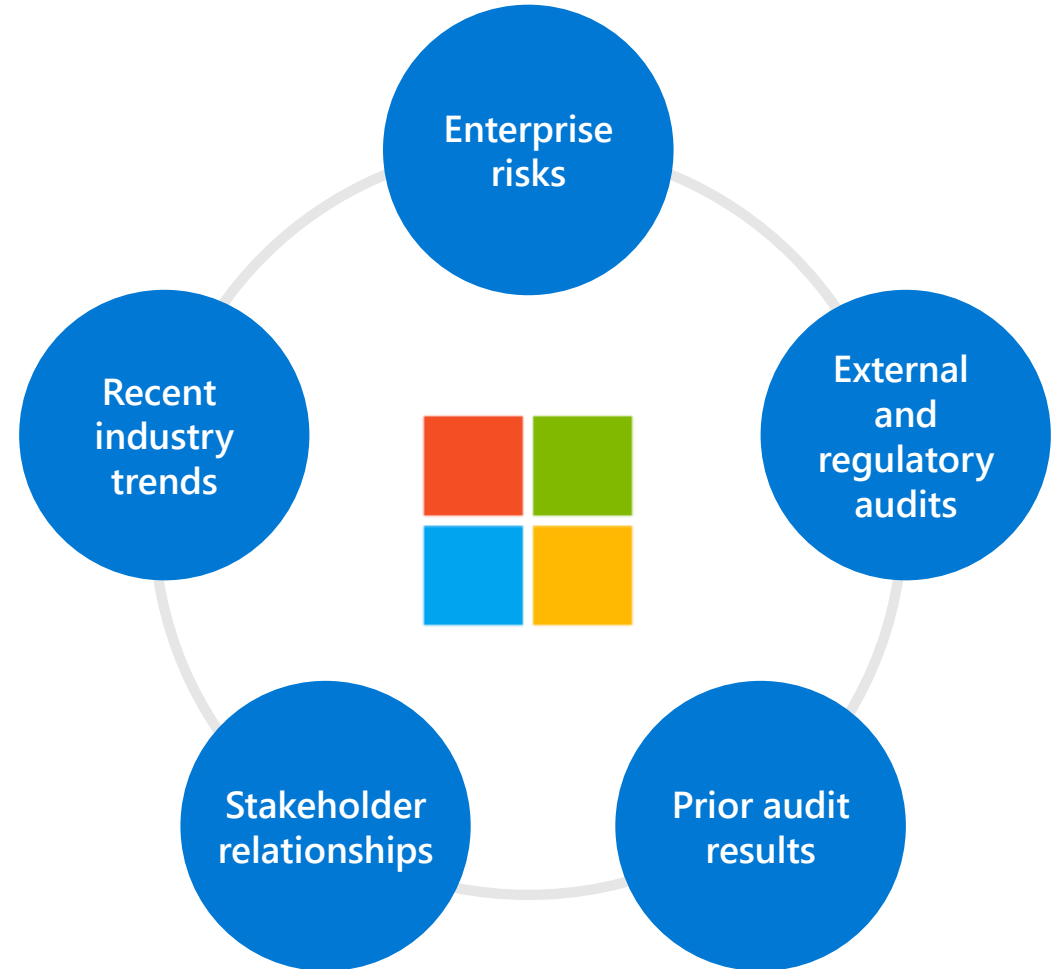
Cybersecurity



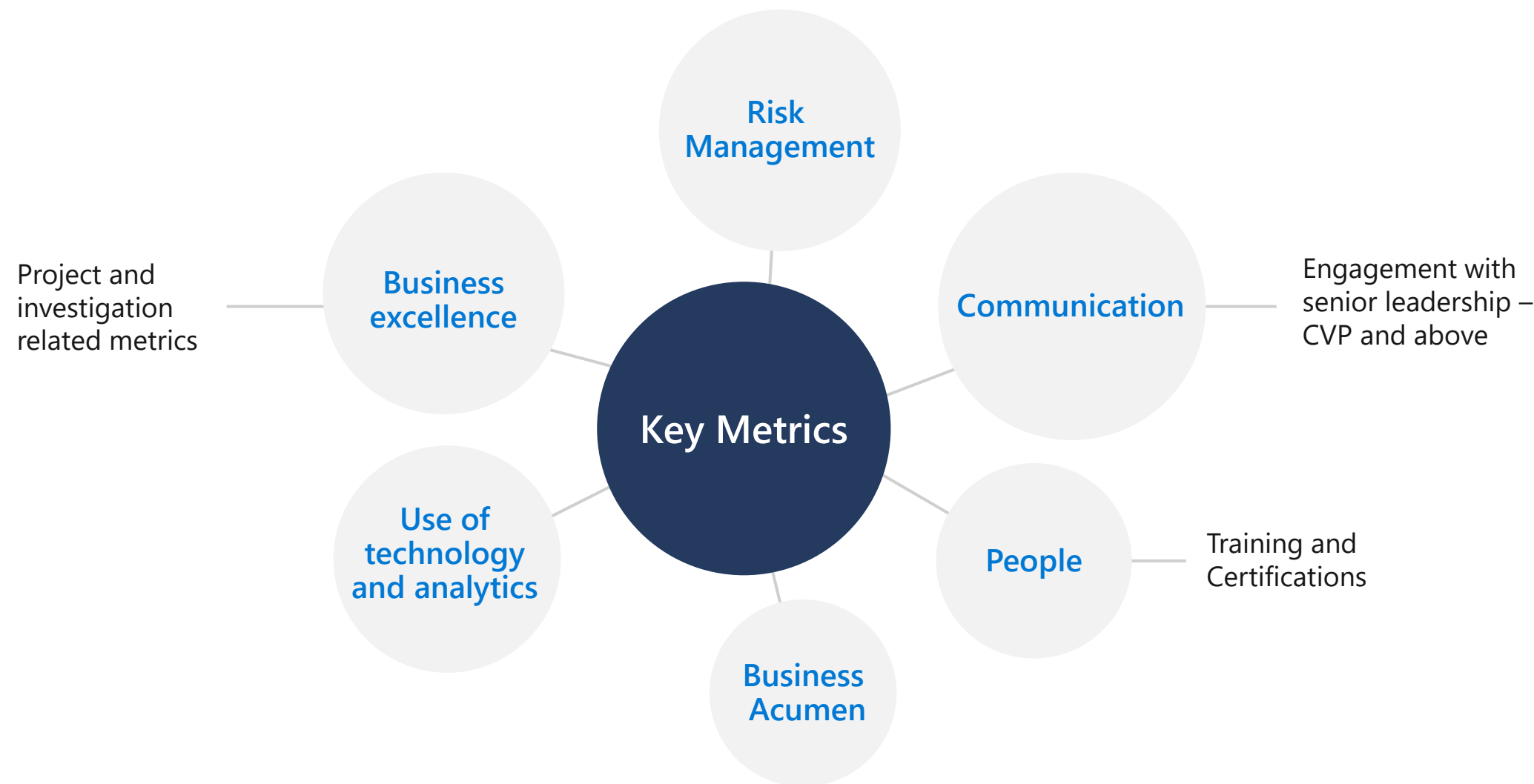
Data Protection & Privacy



Service Quality



Key metrics



ESS: The Enterprise Security Scorecard

Category	ESS Item	Example of Metric
Security Development Lifecycle	Security bugs should be triaged and fixed within Service Level Agreement (SLA)	<ul style="list-style-type: none">Measuring the number of high priority security bugs that are found during the development process and are resolved within an SLA
Identity Management	Create all service accounts with “zero trust”, no interactive logon rights, and require least privileged access	<ul style="list-style-type: none">How many service accounts that no longer interactive login rights
	Privileged User Accounts require Multi-factor Authorization, Just-in-Time (JIT), and full separation from info worker accounts	<ul style="list-style-type: none">Total population of persistent admins in your environmentHow many accounts need MFA versus how many actually have MFA enabled
Device Health	Deploy CredGuard (and Token Binding when available) to protect user and administrative credentials	<ul style="list-style-type: none">How many devices in your environment are fully patched within 30 daysHow many corporate users are using approved and healthy devices to access company assetsWhat population of devices are enabled with Secure Boot or similar control
	All devices are up to date on patches, anti-virus (AV), and security configurations	
	Accelerate Conditional Access (CA) deployment to allow access from only healthy devices	
	Require modern hardware and OS platform for critical assets (starting with secure boot + TPM 2.0)	
Security Monitoring	Require all hosts to be monitored for security events.	<ul style="list-style-type: none">How many devices in your environment are both monitored and providing telemetry on events
Logging/ Telemetry	Define and implement a standard security event framework for application and service telemetry	<ul style="list-style-type: none">How many applications are delivering security-related telemetry
Network & Identity Isolation	Move corporate clients off the corporate network by default (“Internet First”)	<ul style="list-style-type: none">How many corporate clients connect to the Internet by default
Incident Response	Track numbers of incidents across the company: Computer Security Incident Response Plans (CSIRPs) and Software and Services Incident Response Plans (SSIRPs)	<ul style="list-style-type: none">How many critical security incidents are occurring monthly that require coordinated responses from security teams

Risk portfolio access model



General site access to:

Risk Titles & Risk Descriptions

Supplemental information

Role Type	Permission Level
Senior Management	View Only
Risk Owners & Focal	View Only
Enterprise Risk Organization	View Only
Other Risk Community Stakeholders	View Only



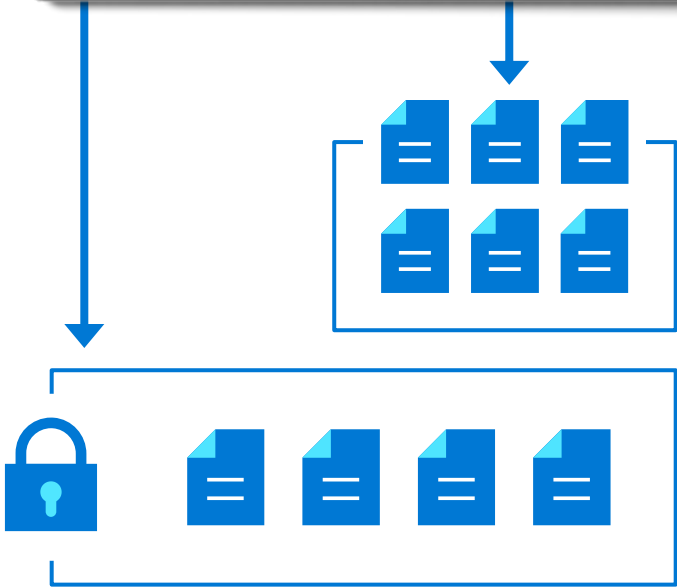
Individual Risk Reports

Role Type	Permission Level	ERM Pillar
Senior Management	Read Only	All
Risk Owners & Focal	Read Only	Varies by role type
Enterprise Risk Organization	View Only	Varies by role type



Management's ERM Report

Role Type	Permission Level
Senior Management	Read Only



Business risk engagement

[illegible]

Risk accountability

It starts with ownership at the top

Enterprise Risk Accountability				
Risk Category	Risk Title	Board	SLT Owner	Risk Owner(s)
Improve	Competition	Full	CEO	Chief Marketing Officer
	Corruption	AC	General Counsel	Deputy General Counsel
	Cyber Security	AC/RPP	Online Platforms President	Chief Information Security Officer
	Recruitment & Retention	Comp	Chief People Officer	Human Resources
	Business Continuity	AC/RPP	COO	Chief Information Officer
	Data Privacy	RPP	COO	Chief Privacy Officer
	Strategic Investments	Full	CFO	Business Development
	Data Sovereignty	RPP	General Counsel	Deputy General Counsel
	Regulatory Complexity & Uncertainty	RPP	General Counsel	Deputy General Counsel
	International Operations	AC	COO	International Sales & Marketing
	Supply Chain	RPP	COO	Supply Chain
Monitor	Data Management	AC	COO	Chief Information Officer
	Customer Relationships	AC	COO	Customer Service & Support
	Acquisitions & Divestitures	AC	CFO	Venture Integration
	Facility Access and Security	AC	CFO	Security
	Operational Infrastructure	Full	CEO	Chief Information Officer
	Interest Rate Changes	AC	CFO	Treasurer
	Tax Strategy & Optimization	AC	CFO	Tax
	Currency Fluctuations	AC	CFO	Treasurer
	Credit & Collections	AC	CFO	Treasurer

Board Acronyms:

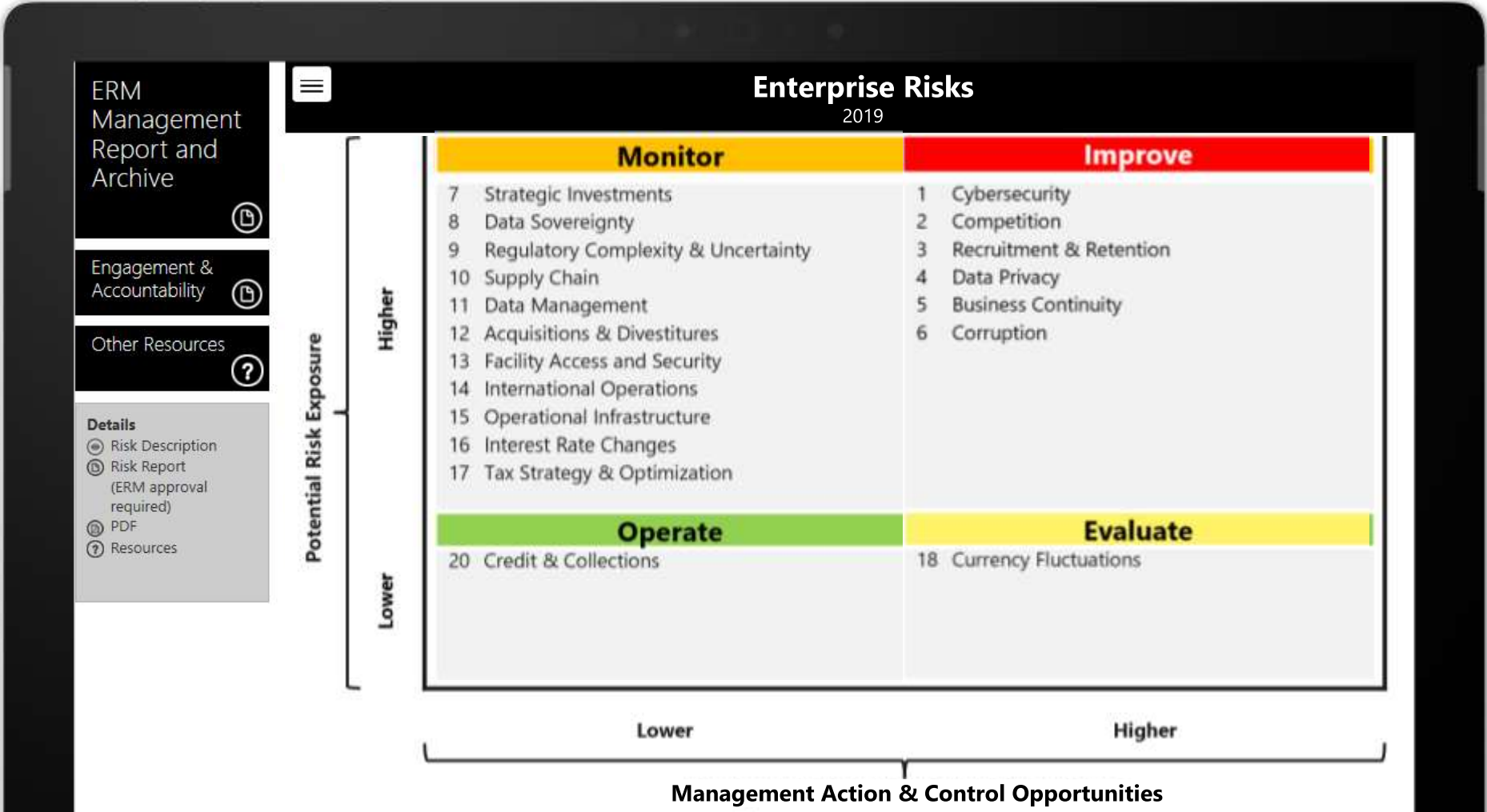
Full	Full Board
AC	Audit Committee
RPP	Regulatory & Public Policy Committee
Comp	Compensation Committee

Risk management methodology



Risk Matrix

Example



*The content displayed on this example is for demonstration purposes only and does not represent Microsoft's real Enterprise Risk Matrix

Key action items (Go Do)

Start with a coalition of the willing

Ensure the group is willing to make the hard calls

Know your threat landscape

Educate and leverage senior business leadership

Your data should be actionable



Thank You

@askudrati

<https://aka.ms/abbas>

An abstract graphic on the right side of the slide, composed of numerous small purple dots arranged in a series of concentric, wavy lines that create a sense of depth and movement, resembling a stylized wave or a digital signal.