Microsoft

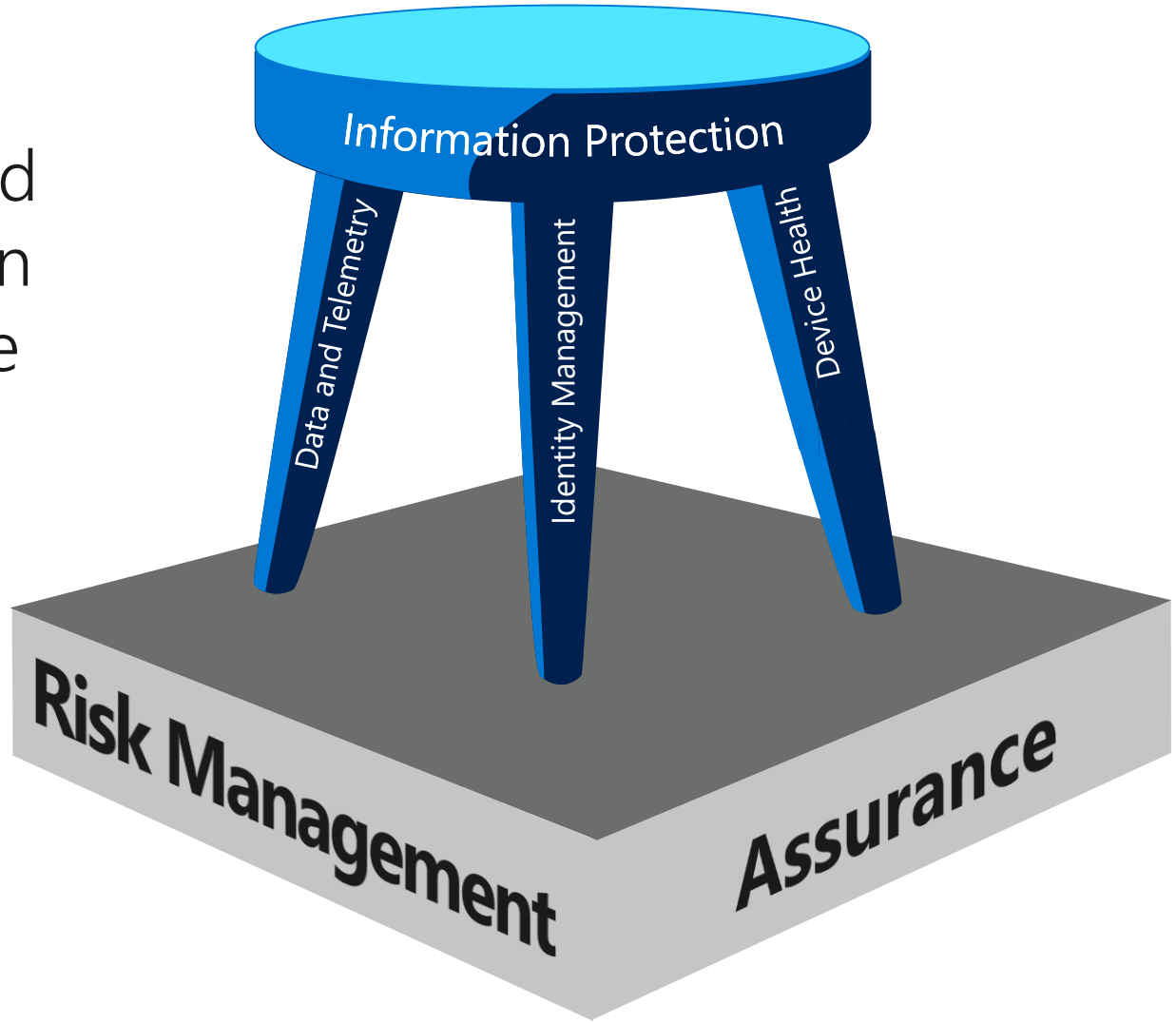
Speaking of security: Risk management

What we'll cover today

- Security focus
- Microsoft digital security strategy
- Risk management process
- Key actions
- Q&A

Security focus

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



2019 Digital security strategy

	Risk Management	Assurance	Identity Management	Device Health	Data & Telemetry	Information Protection
EPICS	All internet facing interfaces are compliant Tier 1 critical services are resilient	Accelerate cloud security capabilities	Eliminate passwords Protect the administrators Simplify provisioning, entitlements, and access management	Evolve endpoint protection Only allow access from healthy devices Zero trust networks	Detect threats through user behavior anomalies	All Microsoft data is classified, labeled and protected
SERVICES	Business response and crisis management Compliance Enterprise business continuity management Enterprise security governance and risk Security education and awareness Security incident response Security standards and configuration	App & Infrastructure security Emerging security products External assessments Red team penetration testing Supply chain security	Administrator role services Authentication Certificate management Credential management Provisioning, entitlement management, and synchronization	Endpoint protection Phishing protection SAW HRE Vulnerability management Virtualization	Data intelligence Security intelligence platform Security monitoring Threat intelligence	Data loss prevention Insider threat

Security tools engineering

Security world view

Opportunities

Globalization means more markets, customers, and business potential

Always-on access provides **more productivity**

Ability to **analyze massive data** sets at scale and speed

Scalable, cloud-based storage is more efficient, cost effective, and secure

Modern engineering allows for more agility in building capabilities, features, and in responding to threats

Risks

Globalization can lead to **"digital xenophobia"**

More lucrative targets give rise to more **dangerous threat actors**

More surface area for attacks/exposure to harm, including **supply chain**

The client-to-cloud world requires a control shift
(Identity is the new perimeter)

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

How we think about risk

What is a risk?

The possibility that events will occur and affect the achievement of strategic, operational, financial, and legal/compliance objectives

- Strategic
- Operational
- Financial
- Legal/Compliance

Why we identify and track risks?

- Enable Board Governance
- Enable senior leaders to make risk informed decisions & remove remediation road-blocks in an effective, efficient, and consistent manner.
- Identify, prioritize, and report the most critical risks to key company strategies

Which risks are the right ones to mitigate?

The evolution of risk management

Pre-FY11

Coalition of the Willing
Pre FY11

- Siloed teams tackling security issues within their organization
- No centralized security governance organization

FY12

Coalition of the Willing
FY12

- **Information Risk Management Council** (IRMC) envisioned and core team launched: Global Security, Trustworthy Computing, Global Foundation Services, and Information Security and Risk Management (Microsoft IT)
- Focused on increasing awareness and ability to take action on some of the most critical cross-organizational risks
- Created one Microsoft Security Policy

FY13

Preliminary Expansion
FY13 – FY15

- Coalition had accomplished foundational goals and was ready to begin expansion across organization
- Engineering Groups originally brought in as extended team members, involved in risk assessments and Working Group planning
- Began formal governance of Working Groups with scorecards and status reporting

FY16

Full Cross-company Governance
FY15 – FY17

- Engineering Groups become Core Members of the Council
- Cyber attacks on the rise (e.g., Sony) result in need for more coordinated cross-company engagement
- Cyber Defense Preparedness Project jumpstarts coordination of the newly expanded Core team
- Data-driven risk analyses and assessments start enabling strategic action

FY18

Improving Operational Effectiveness
FY18 and Beyond

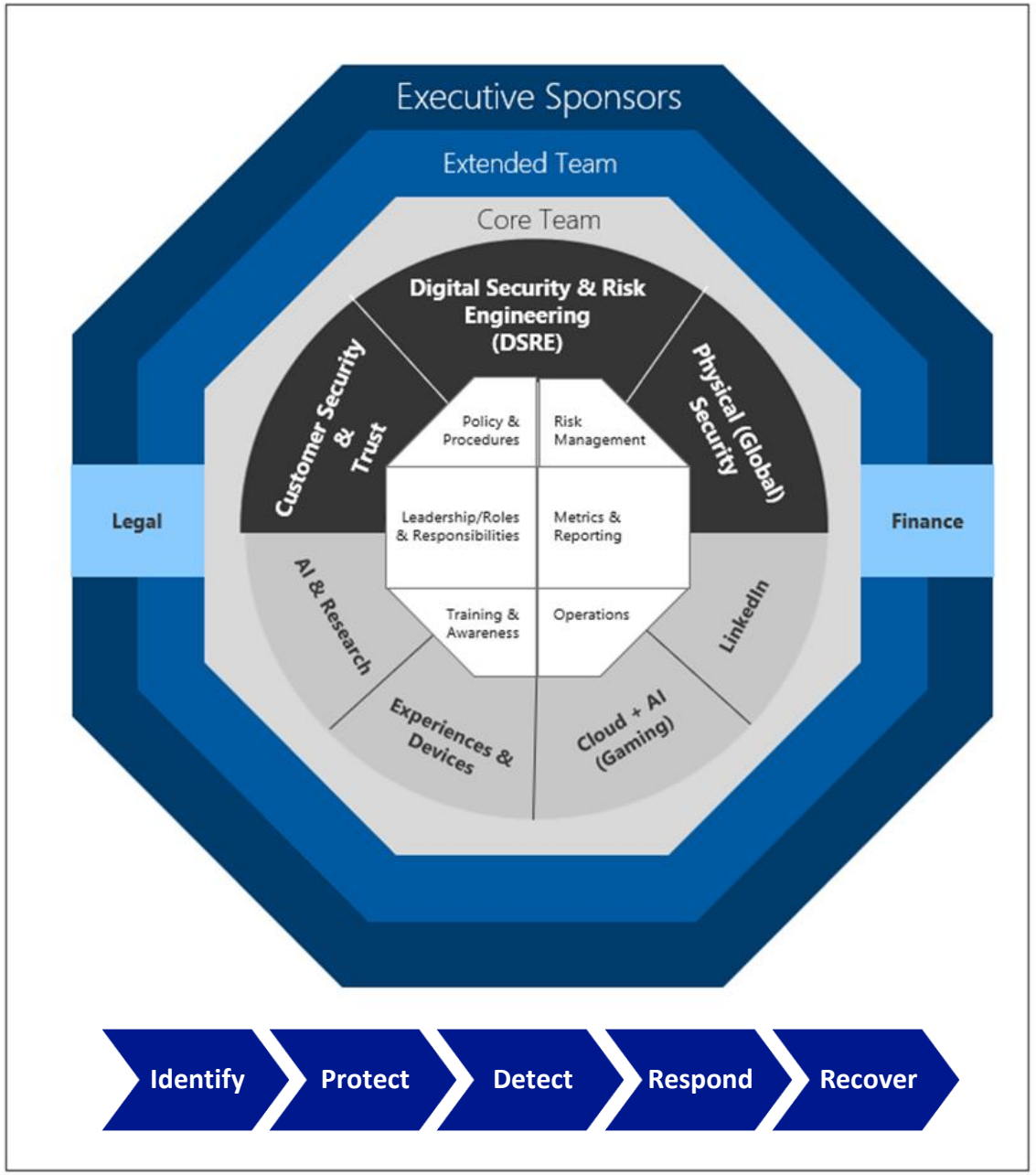
- IRMC continues to be the primary security governance body. However, a new level of standardization and enhanced governance is needed to address key challenges within the changing threat environment
- The Company revisits accountability and engagement across all groups to ensure consistent alignment, standards, and processes

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: 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)

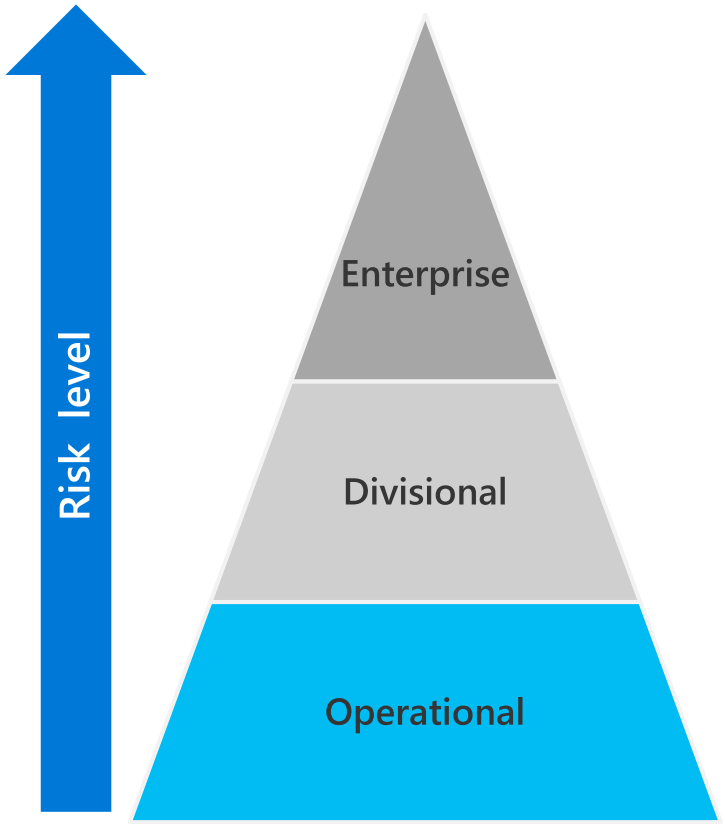
8. Mobilize and execute decision implementation
9. Track and report
10. Close/validate decision implementation

Emergency-type decisions should still follow the formal process but be initiated more quickly, 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 decision implementation



*Risk decision owner	Residual risk >10	Criteria Breadth of impact	**Business risk owner
IRMC	✓	Enterprise-wide	EVP/CVP
Sub-IRMC	✓	Two or more Business Groups (BG) (e.g., C+AI, E+D)	
Business Governance Meeting (e.g., CISO)	✓	One BG, or two or more sub-orgs (e.g., C+AI, Gaming, E+D)	CVP/VP
Group Leader/ Manager		One sub-org. (e.g., C+AI 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

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)	• 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	• How many service accounts that no longer interactive login rights
	Privileged User Accounts require Multi-factor Authorization (MFA), just-in-time (JIT), and full separation from info worker accounts	• Total population of persistent admins in your environment • How 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	• How many devices in your environment are fully patched within 30 days • How many corporate users are using approved and healthy devices to access company assets • What population of devices are enabled with Secure Boot or similar control
	All devices are up to date on patches, antivirus (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	• 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	• How many applications are delivering security–related telemetry
Network & Identity Isolation	Move corporate clients off the corporate network by default ("Internet First")	• How many corporate clients connect to the Internet by default
Incident Response	Track numbers of security and privacy incidents across the company	• How many critical security incidents are occurring monthly that require coordinated responses from security teams

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
- Ensure data is actionable

Resources

Access all IT Showcase resources at microsoft.com/ITShowcase

- Fostering a risk-based culture to secure the enterprise
- Speaking of security: A discussion with Bret Arsenault, CISO at Microsoft
- Integrating security into the mobile app development life cycle
- Building cloud apps using the Secure DevOps Kit for Azure
- Microsoft Security Intelligence Report

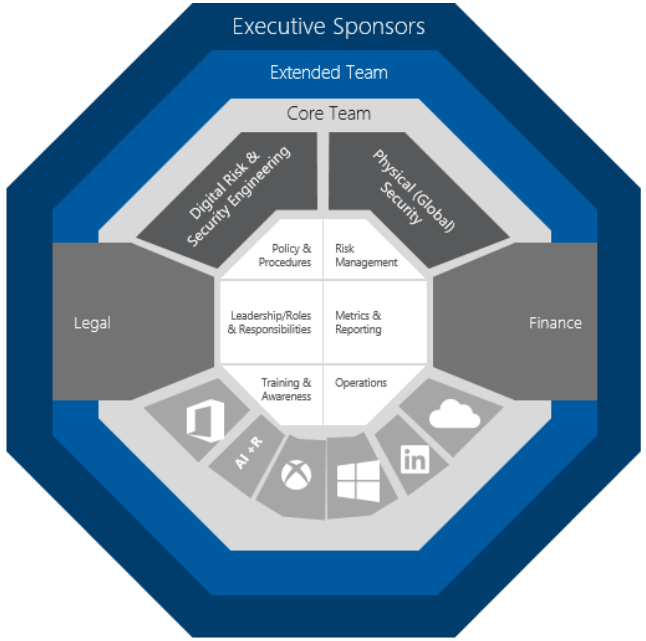
Microsoft

Microsoft IT Showcase

How Microsoft does IT

Visit the website
microsoft.com/itshowcase

IRMC Engagement



Top Risks

Working Groups

Actions & Deliverables

IRMC LT

Recommendations & Escalations

IRMC Executive Sponsors

Sponsorship & Decisions

Executive Reviews

Strategy & Directions

Board Updates