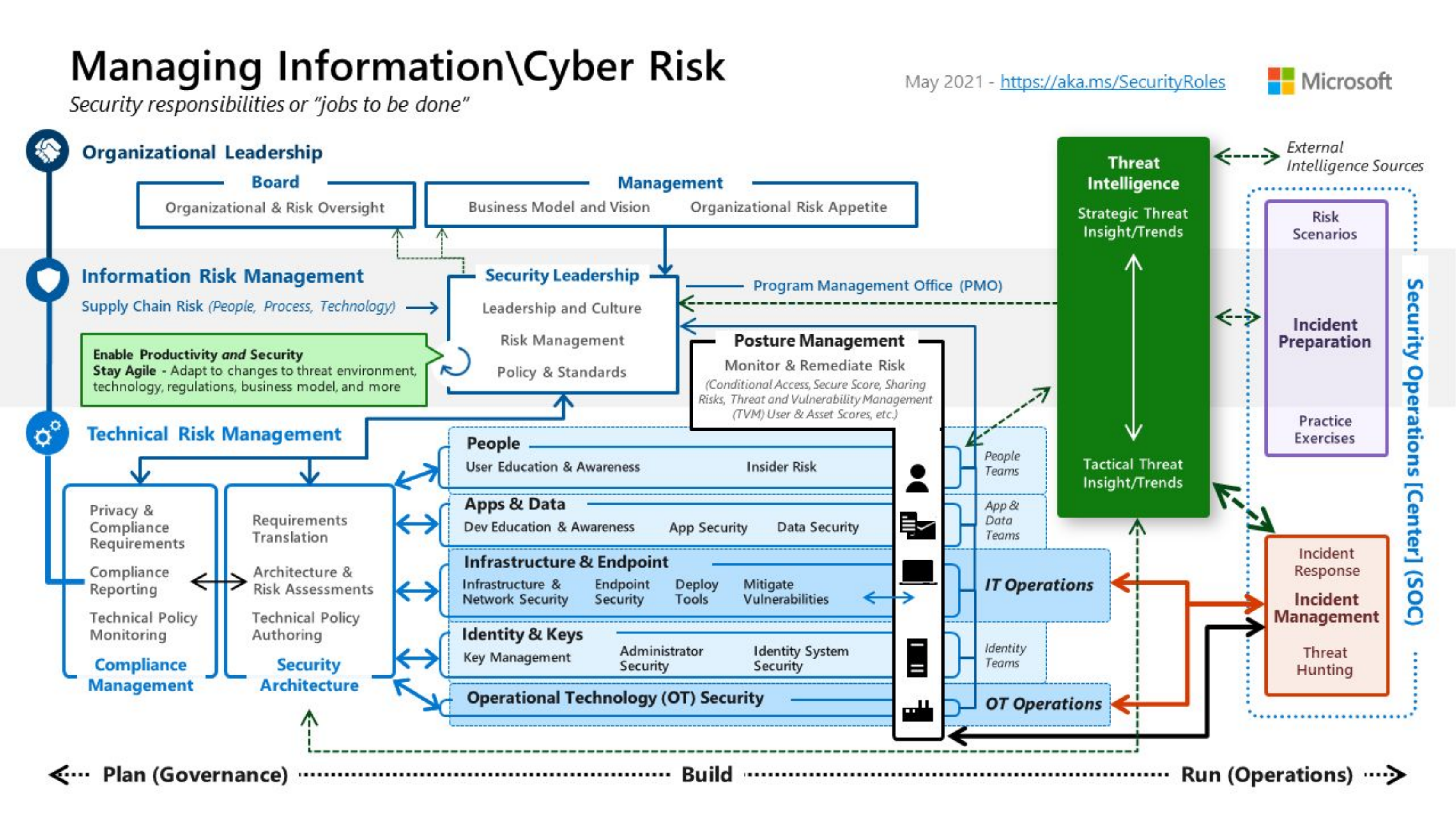

Managing Information\Cyber Risk
Security responsibilities or "jobs to be done"
May 2021 - https://aka.ms/SecurityRoles
Microsoft
Organizational Leadership
Board
Organizational & Risk Oversight
Management
Business Model and Vision
Organizational Risk Appetite
Information Risk Management
Supply Chain Risk (People, Process, Technology)
Enable Productivity and Security
Stay Agile - Adapt to changes to threat environment, technology, regulations, business model, and more
Security Leadership
Leadership and Culture
Risk Management
Policy & Standards
Program Management Office (PMO)
Posture Management
Monitor & Remediate Risk
(Conditional Access, Secure Score, Sharing Risks, Threat and Vulnerability Management (TVM) User & Asset Scores, etc.)
Technical Risk Management
Privacy & Compliance Requirements
Compliance Reporting
Technical Policy Monitoring
Compliance Management
Requirements Translation
Architecture & Risk Assessments
Technical Policy Authoring
Security Architecture
People
User Education & Awareness
Insider Risk
People Teams
Apps & Data
Dev Education & Awareness
App Security
Data Security
App & Data Teams
Infrastructure & Endpoint
Infrastructure & Network Security
Endpoint Security
Deploy Tools
Mitigate Vulnerabilities
IT Operations
Identity & Keys
Key Management
Administrator Security
Identity System Security
Identity Teams
Operational Technology (OT) Security
OT Operations
Threat Intelligence
Strategic Threat Insight/Trends
Tactical Threat Insight/Trends
External Intelligence Sources
Risk Scenarios
Incident Preparation
Practice Exercises
Incident Response
Incident Management
Threat Hunting
Security Operations [Center] (SOC)
Plan (Governance)
Build
Run (Operations)

Securing the Cloud: Frameworks for Proven Success

Introduction to Cloud Security Frameworks

Importance of Cloud Security Frameworks

Cloud Security Frameworks serve as comprehensive guides to secure cloud environments, ensuring organizations can systematically manage risks, enforce policies, and meet regulatory requirements.

The Cloud Controls Matrix (CCM)

The CCM is a cybersecurity control framework that provides a detailed understanding of security concepts and principles aligned with industry standards, best practices, and regulatory requirements.

The CSA STAR Registry

The CSA STAR Registry is a publicly accessible database that documents the security and compliance posture of cloud service providers, enhancing trust and assurance in cloud services.

Integrating Frameworks with Cloud Governance

Cloud Security Frameworks are critical components of an organization's overall cloud governance strategy, bridging the gap between strategic oversight and operational execution.

Cloud Security Frameworks, such as the CCM and CSA STAR Registry, provide the necessary tools and mechanisms to establish a secure, compliant, and transparent cloud environment, enabling organizations to effectively manage risks and ensure regulatory compliance.

The Cloud Controls Matrix (CCM)

Purpose

The CCM is a comprehensive framework that maps security controls to cloud computing environments. Its primary purpose is to help organizations assess the risk associated with cloud services and ensure they meet necessary security requirements before and during cloud technology adoption.

Control Domains

The CCM consists of control domains that encompass various security areas, such as Data Security and Information Lifecycle Management, Identity and Access Management, Infrastructure and Virtualization Security, and Risk Management and Governance.

Control Specifications

For each domain, the CCM provides specific control statements, detailed control objectives, and the rationale behind each control, serving as a checklist for organizations to evaluate the security posture of cloud service providers and internal cloud environments.

Mapping to Standards and Regulations

The CCM maps its controls to a range of industry standards and regulatory frameworks, such as ISO/IEC 27001, NIST SP 800-53, GDPR, HIPAA, and PCI-DSS, helping organizations achieve compliance in multiple areas simultaneously and providing a clear roadmap for audit readiness.

Implementing the CCM

Baseline Assessment

Perform an initial assessment of the current cloud security posture using the CCM as a benchmark. This involves reviewing existing policies, technical configurations, and operational practices against each control in the CCM framework.

Gap Analysis

Identify areas where the organization's cloud security measures fall short of the recommended CCM controls. Document these gaps and prioritize them based on risk severity and business impact.

Remediation Planning

Develop a detailed remediation plan to address the identified gaps. This may include deploying new security technologies, revising policies, or enhancing training programs for staff involved in cloud operations.

Continuous Monitoring and Auditing

Integrate the CCM into continuous monitoring processes. Automated tools and dashboards can help track compliance status and alert administrators when controls deviate from prescribed standards.

Vendor Evaluation

Utilize the CCM framework to evaluate cloud service providers. Assess provider documentation, third-party audit reports, and certifications to ensure that they adhere to the necessary CCM controls.

Case Study: Applying the CCM in a Financial Institution

A multinational bank sought to move critical financial applications to a cloud environment. Given the sensitivity of financial data and stringent regulatory requirements, the bank used the Cloud Controls Matrix (CCM) to evaluate potential cloud service providers (CSPs) and assess its internal security controls.

The CSA STAR Registry

Purpose

To enhance trust and assurance in cloud services by enabling organizations to review security assessments and certifications of cloud service providers (CSPs)

Self-Assessment (Level 1)

CSPs can submit a self-assessment based on the Cloud Controls Matrix (CCM) to provide initial insight into their security controls and practices

Third-Party Assessments (Level 2)

CSPs can undergo independent, third-party audits to verify their adherence to the CCM and other relevant standards, providing a higher level of assurance

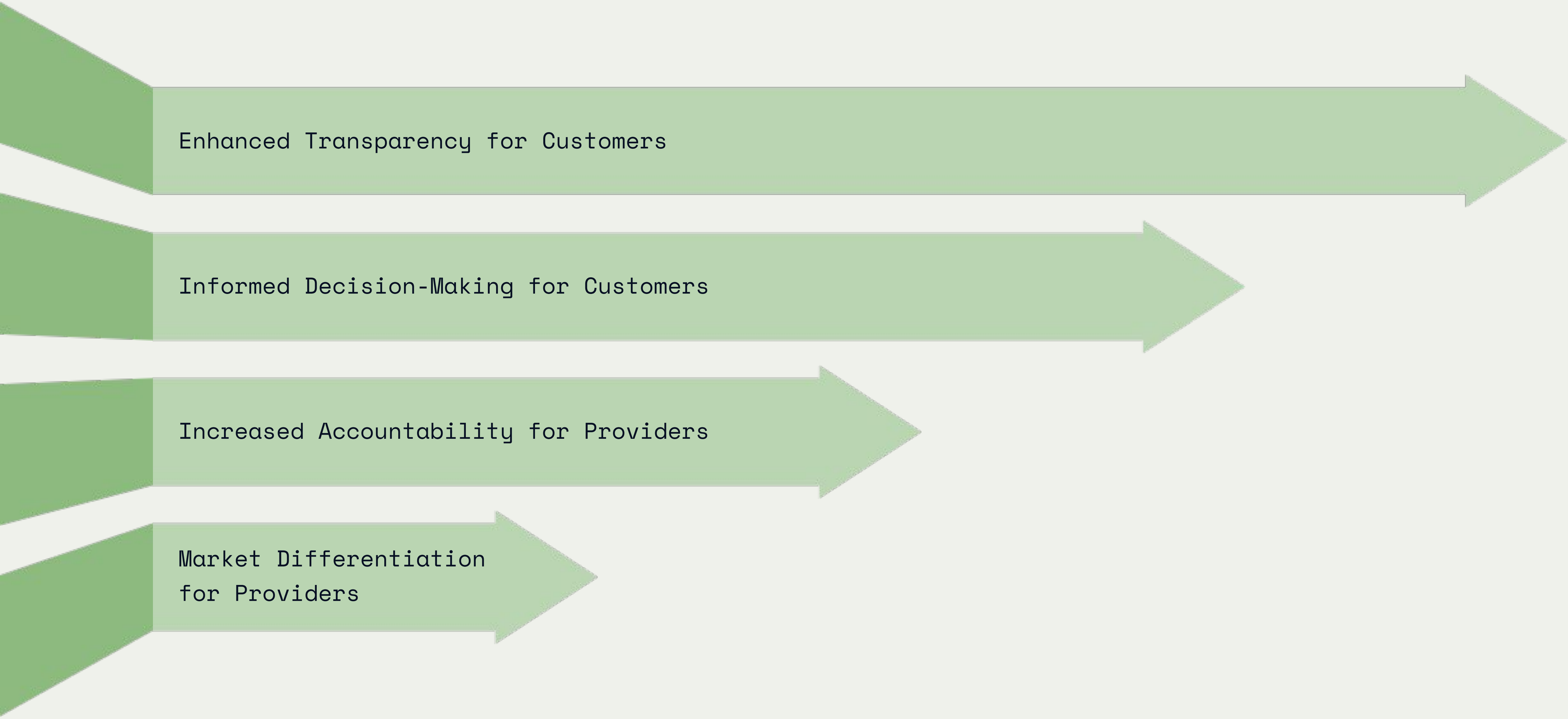
Continuous Monitoring and Certification (Level 3)

The highest level of assurance is achieved through continuous monitoring and certification processes, ensuring that CSPs' security practices remain robust and up-to-date

Benefits

Enhanced transparency, informed decision-making, increased accountability, and market differentiation for CSPs

Benefits of the STAR Registry



Enhanced Transparency for Customers

Informed Decision-Making for Customers

Increased Accountability for Providers

Market Differentiation for Providers

Best Practices for Cloud Providers

- Adopt a Comprehensive Assessment Approach

  Providers should conduct thorough internal assessments against the Cloud Controls Matrix (CCM) before submitting to the STAR Registry. This ensures that all security controls are in place and operating effectively.

- Engage Independent Auditors

  Obtaining third-party certifications, such as ISO/IEC 27001 or SOC 2, can significantly enhance the credibility of the self-assessment. Independent audits provide objective verification of the provider's security posture.

- Maintain Continuous Improvement

  Providers should integrate continuous monitoring mechanisms to ensure that their security controls remain effective over time. Regular reviews and updates to security practices are essential to meet evolving threats and regulatory changes.

- Transparency in Reporting

  Detailed and transparent reporting in the STAR Registry can build customer trust. Providers should ensure that all submissions are accurate, up-to-date, and reflective of their true security capabilities.

Case Study: Enhancing Trust Through the STAR Registry

A leading cloud services provider in the healthcare industry sought to build trust with potential clients by participating in the CSA STAR Registry. By undergoing rigorous third-party audits and publishing comprehensive security documentation, the provider was able to demonstrate adherence to HIPAA, ISO/IEC 27001, and the CCM. This transparency not only differentiated the provider in a competitive market but also led to increased customer confidence and a significant expansion of its client base in the healthcare sector.