KUDELSKI SECURITY

Methodologies and Tools to Assess Cyber Risks

Large Private Sector Organizations

Agenda

- Challenges in the Private Sector
- The CISO Approach
- The Operations Center Approach
- How the CISO and Operations Relate

Risk Assessment Challenges in the Private Sector

Factors influencing methodologies in private sector

- Multiple standards to follow
- External audits (usually for compliance)
- Departmental regulatory requirements
- Mergers and Acquisitions / diversification / international footprint

Cost effectiveness of cyber controls

- Setting an appropriate risk appetite
- Correlation to business objectives

Alphabet Soup

Frameworks

- NIST CSF
- ISO/IEC 27001
- COBIT

Standards

- PCI DSS
- SOX / GLBA
- HIPPA / HITECH

Regulations

- Data Residency Requirements
- EU Privacy Regulations

The CISO Approach

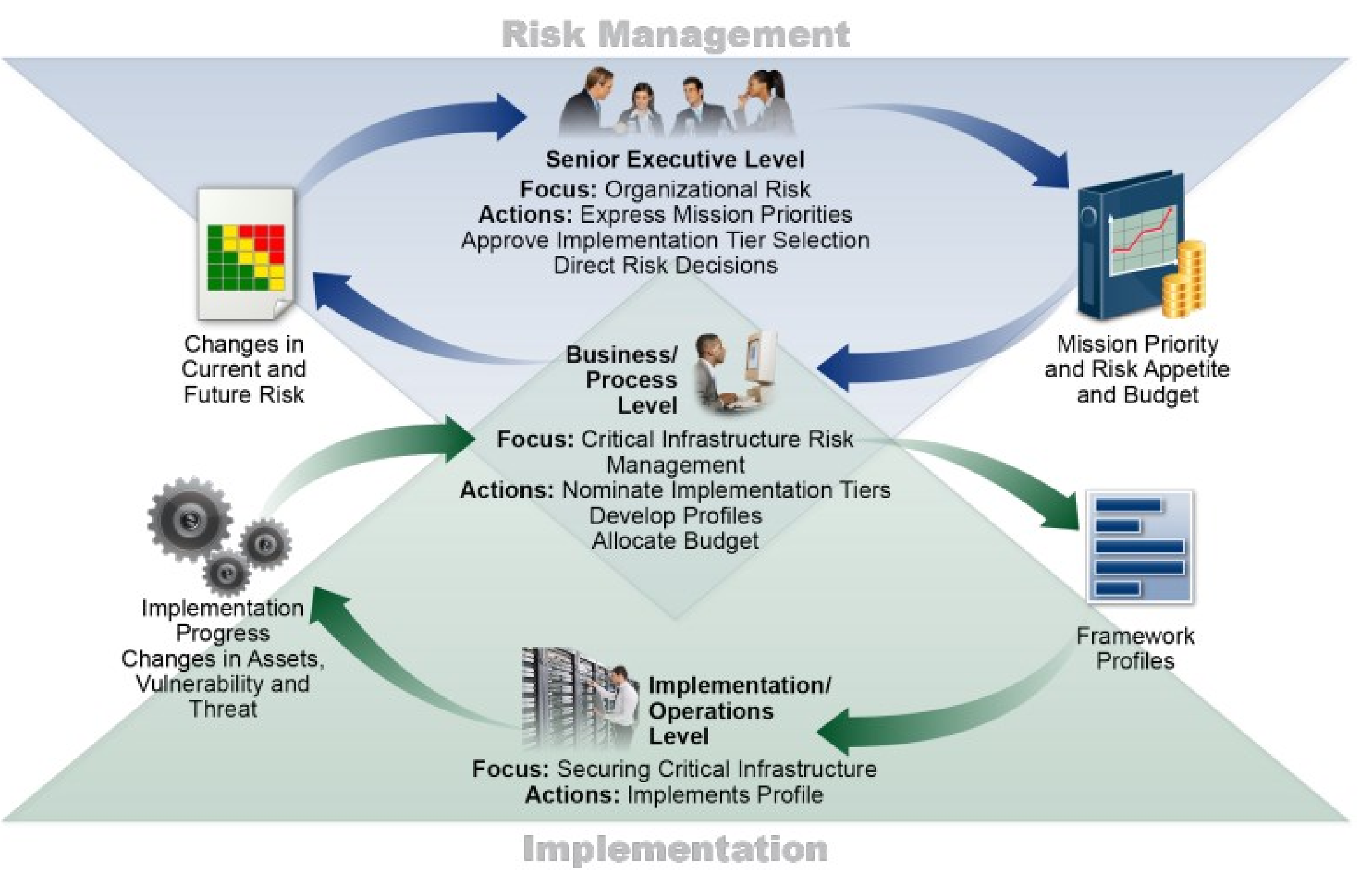
How do CISOs manage these influences

- Pick one or more methodologies to measure organizational risk
- Map controls to multiple standards
- Use governance, risk, and compliance (GRC) tools
- Use a metrics approach

At this level, the CISO focuses on strategic risk to business objectives

It is challenging to relate operational measurements with strategic metrics

Methodology Example – NIST CSF



Risk Management

Senior Executive Level

Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Changes in Current and Future Risk

Framework Profiles

Implementation/ Operations Level

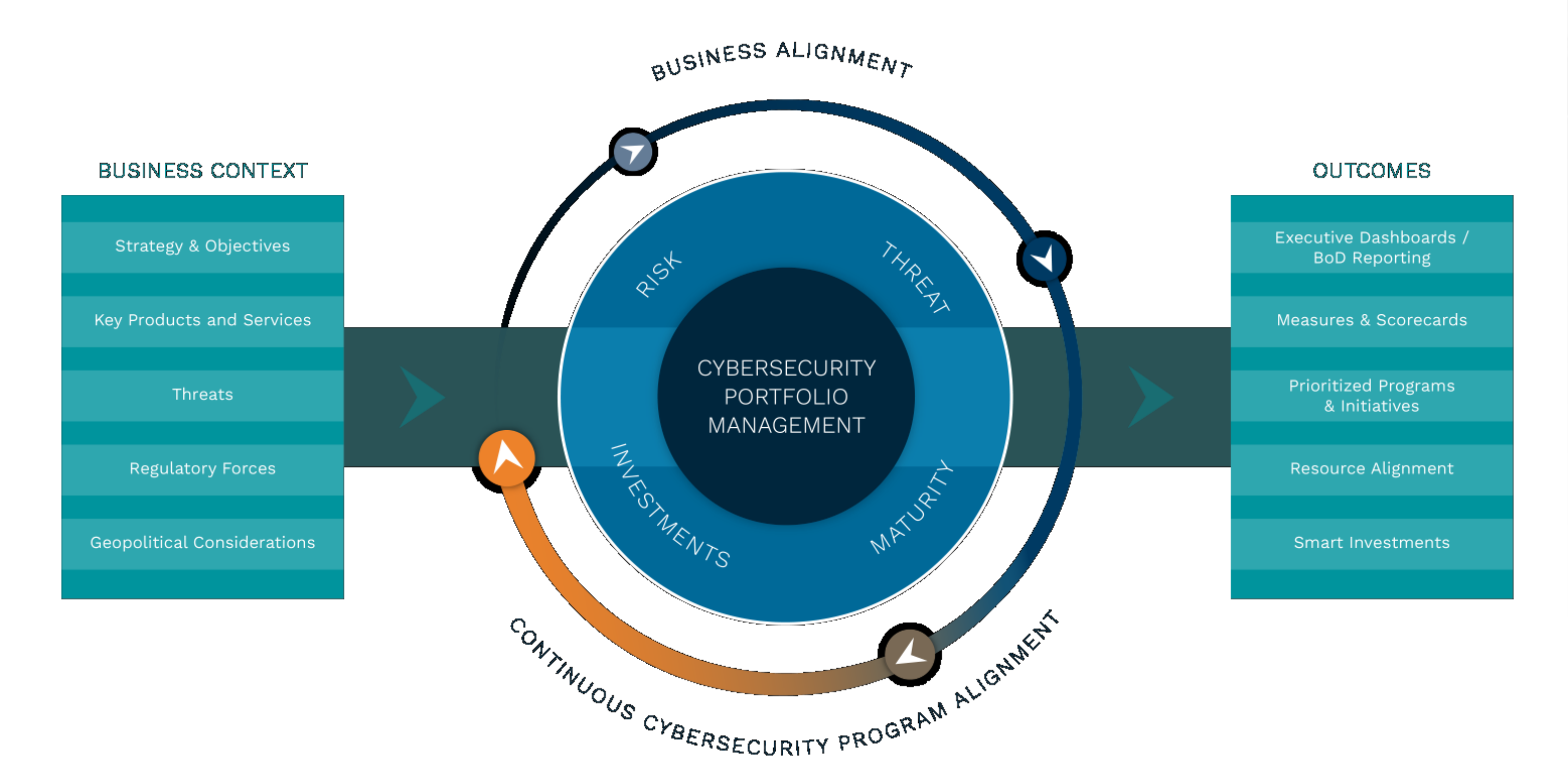
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation Progress Changes in Assets, Vulnerability and Threat

Implementation

Governance and Risk Software Example – Secure Blueprint

OUR APPROACH to designing compreh business program



BUSINESS ALIGNMENT

BUSINESS CONTEXT

- Strategy & Objectives
- Key Products and Services
- Threats
- Regulatory Forces
- Geopolitical Considerations

RISK

THREAT

CYBERSECURITY PORTFOLIO MANAGEMENT

INVESTMENTS

MATURITY

OUTCOMES

- Executive Dashboards / BoD Reporting
- Measures & Scorecards
- Prioritized Programs & Initiatives
- Resource Alignment
- Smart Investments

CONTINUOUS CYBERSECURITY PROGRAM ALIGNMENT

The Security Operations Approach

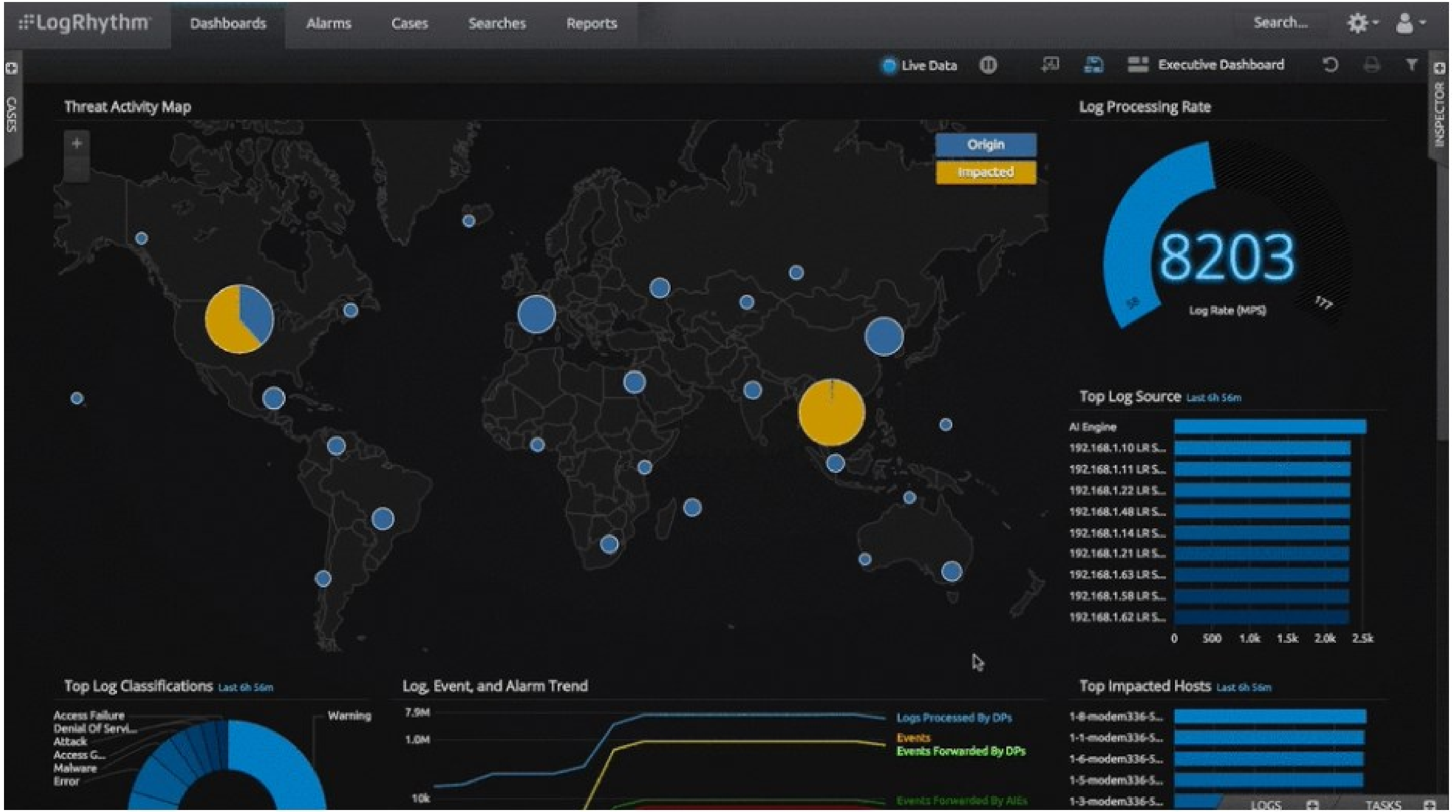
How does operations manage these influences

- Traditional focus on tools vs. methodology
- Tracking software/countermeasure coverage to identify gaps
- A measurement approach to security compliance
- Focus on threats (Malware, Hackers, Insider Threat, etc.)

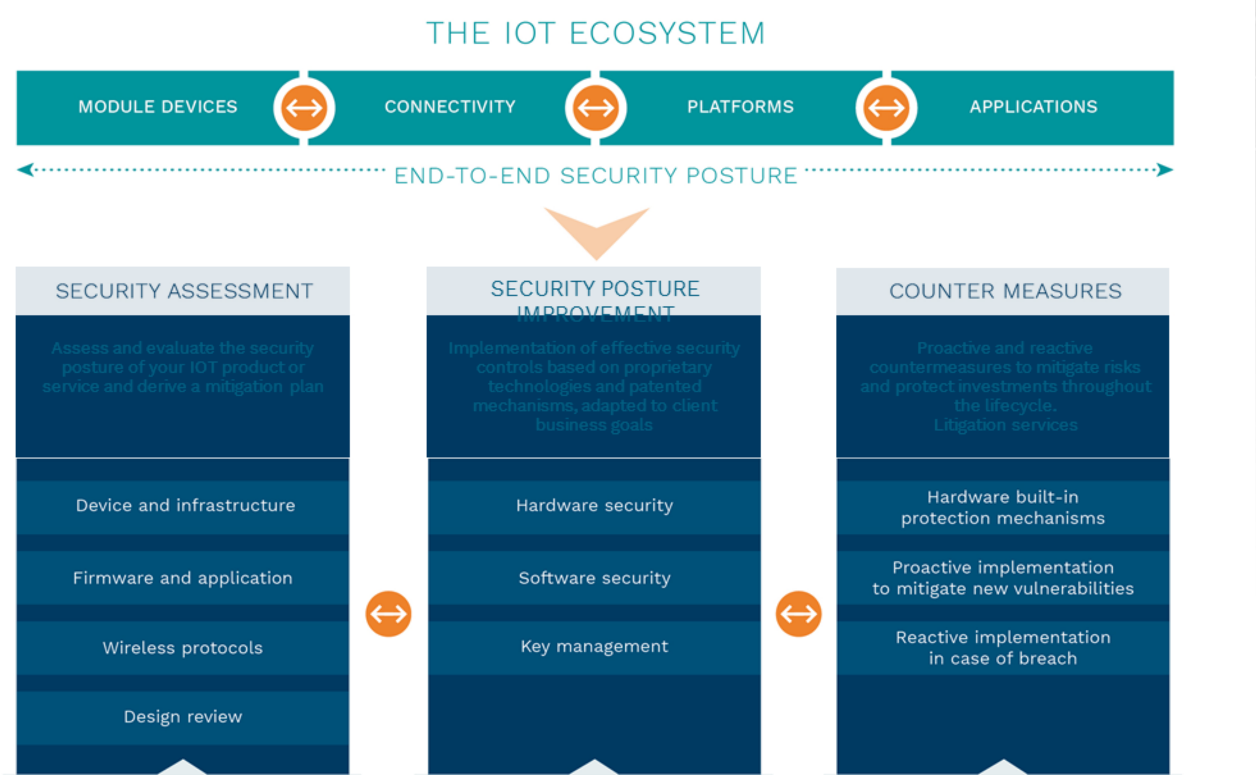
At this level, operations cares about tactical risk to business assets

It is a challenge to map business assets to business objectives

Tactical Risk Detection Tool Example – LogRhythm SIEM



Vulnerability Management Example – IoT End-to-End Security



THE IOT ECOSYSTEM

MODULE DEVICES ↔ CONNECTIVITY ↔ PLATFORMS ↔ APPLICATIONS

END-TO-END SECURITY POSTURE

SECURITY ASSESSMENT

Assess and evaluate the security posture of your IOT product or service and derive a mitigation plan

- Device and infrastructure
- Firmware and application
- Wireless protocols
- Design review

SECURITY POSTURE IMPROVEMENT

Implementation of effective security controls based on proprietary technologies and patented mechanisms, adapted to client business goals

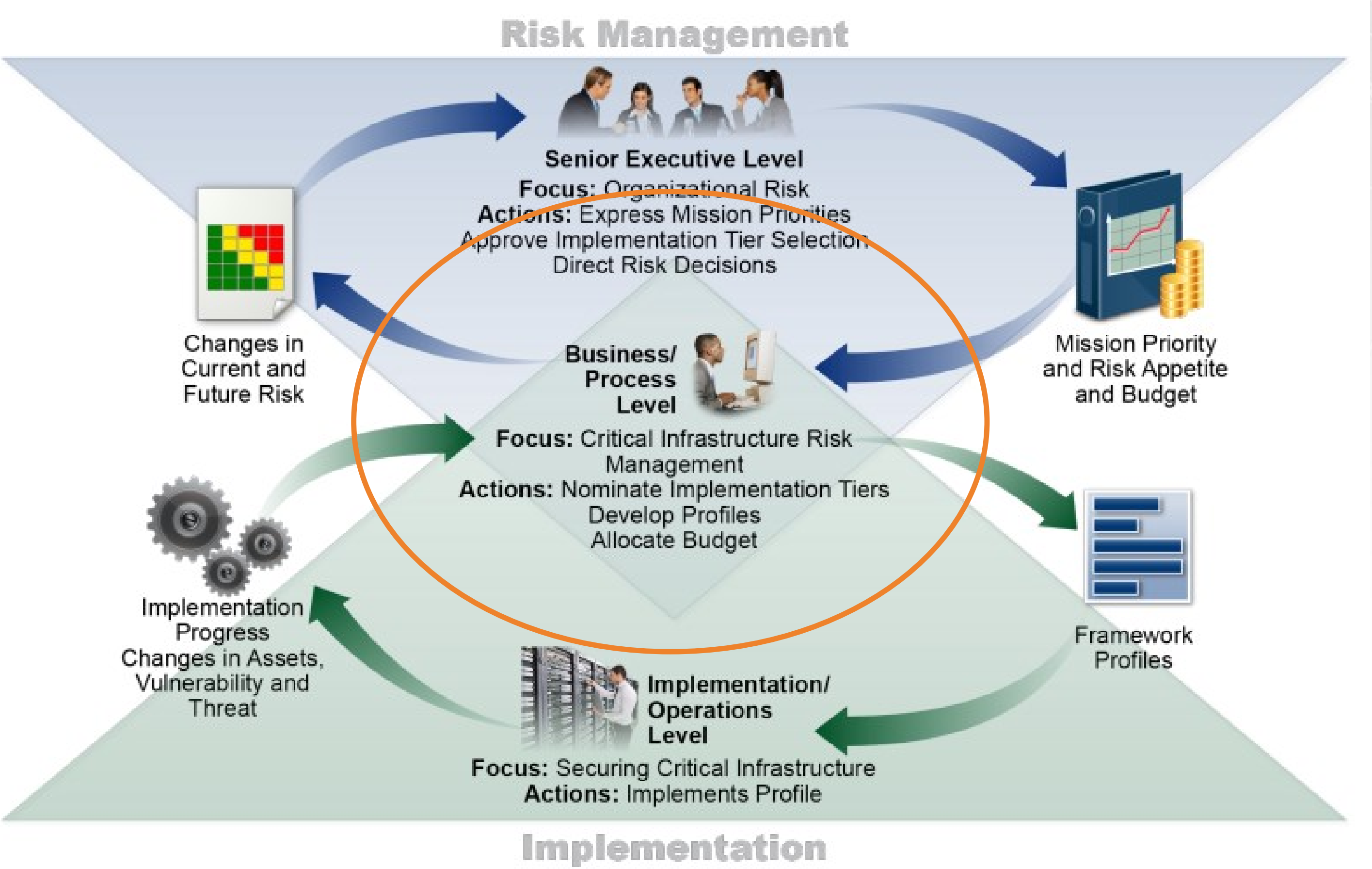
- Hardware security
- Software security
- Key management

COUNTER MEASURES

Proactive and reactive countermeasures to mitigate risks and protect investments throughout the lifecycle.
Litigation services

- Hardware built-in protection mechanisms
- Proactive implementation to mitigate new vulnerabilities
- Reactive implementation in case of breach

Combining Strategic and Tactical Risk Assessment



Risk Management

Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions

Changes in Current and Future Risk

Mission Priority and Risk Appetite and Budget

Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget

Implementation Progress
Changes in Assets, Vulnerability and Threat

Framework Profiles

Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation

Thank You

Ryan SPANIER
Director of Cybersecurity Research
Atlanta, GA USA
Phone: +1 404.665.8166
Email: ryan.spanier@kudelskisecurity.com