Cyber as a Disrupter and Catalyst

SIFM – 20 March 2024

Cassandra Anderson

Ben Doane

Matthias Liermann

mazars

Cybersecurity program development

A Holistic Approach to Risk Mitigation

Security Risk Assessments

Comprehensive risk assessments against standard frameworks such as NIST CSF, ISO 27002, or CIS

Strategic Advisory & Policy Development

Strategic leadership services, program, policy development.

Industry Compliance & Sensitive Data

Ensuring your program meets industry-specific regulations and standards with the right controls & policies for sensitive data.

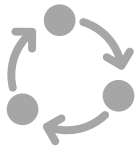
Penetration Testing

Technical assessment of the internal, external, web application, and physical environment.

24x7 Threat Prevention, Monitoring, & Response

Continuous security operations services for cyber threat prevention, identification, monitoring, and response.

Vulnerability Management



Comprehensive vulnerability scanning & reporting services for effective patching and remediation.

Digital Forensics & Incident Response

Ensuring swift and efficient response to any security breaches or incidents.

Security Awareness Training

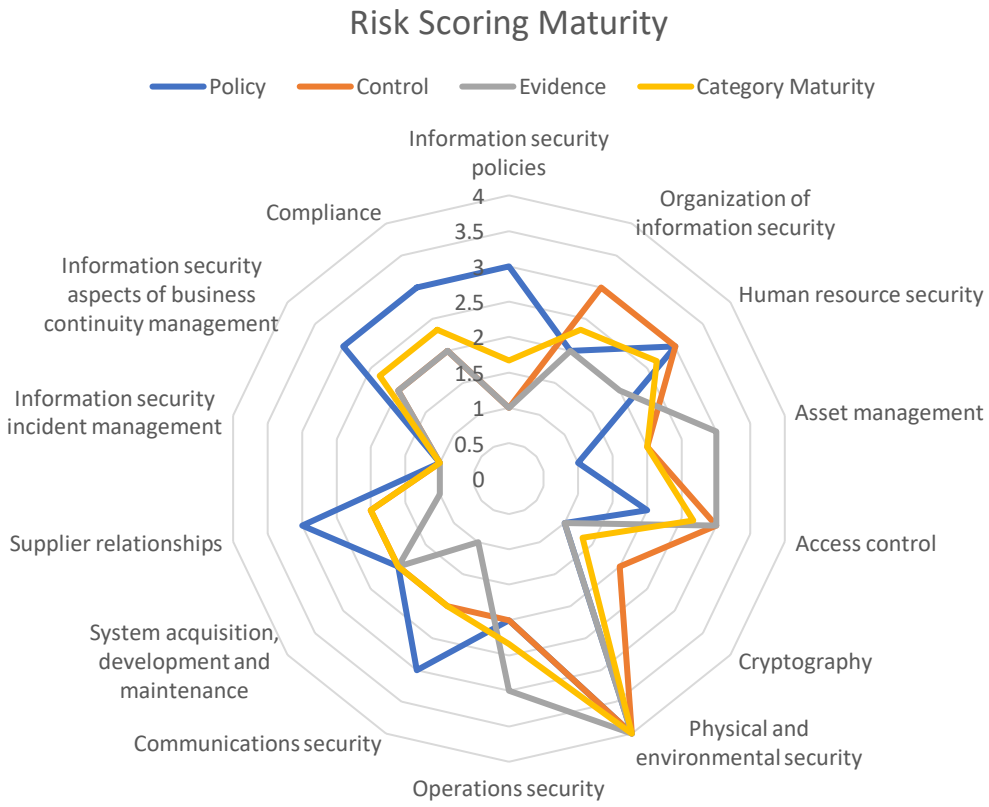
Robust curriculum to educate users for cyber resilience.

Organizational Risk Assessment **(Sample)**

Assessment Overview

- Goal:
  - Assess organizational risk against a standard security framework such as ISO, NIST, CMMC
- Workshop review:
  - Policies, Controls, Evidence
  - Risk and Compliance
- Workshop participants:
  - Security & Compliance
  - Business Managers
  - Technical Team
  - PMO
- Analysis & Reporting

14 Categories Assessed	114 Controls Assessed
Information security policies	2 controls
Organization of information security	7 controls
Human resource security	6 controls
Asset management	10 controls
Access control	14 controls
Cryptography	2 controls
Physical and environmental security	15 controls
Operations security	14 controls
Communications security	7 controls
System acquisition, development and maintenance	13 controls
Supplier relationships	5 controls
Information security incident management	7 controls
Information security aspects of business continuity management	4 controls
Compliance	8 controls



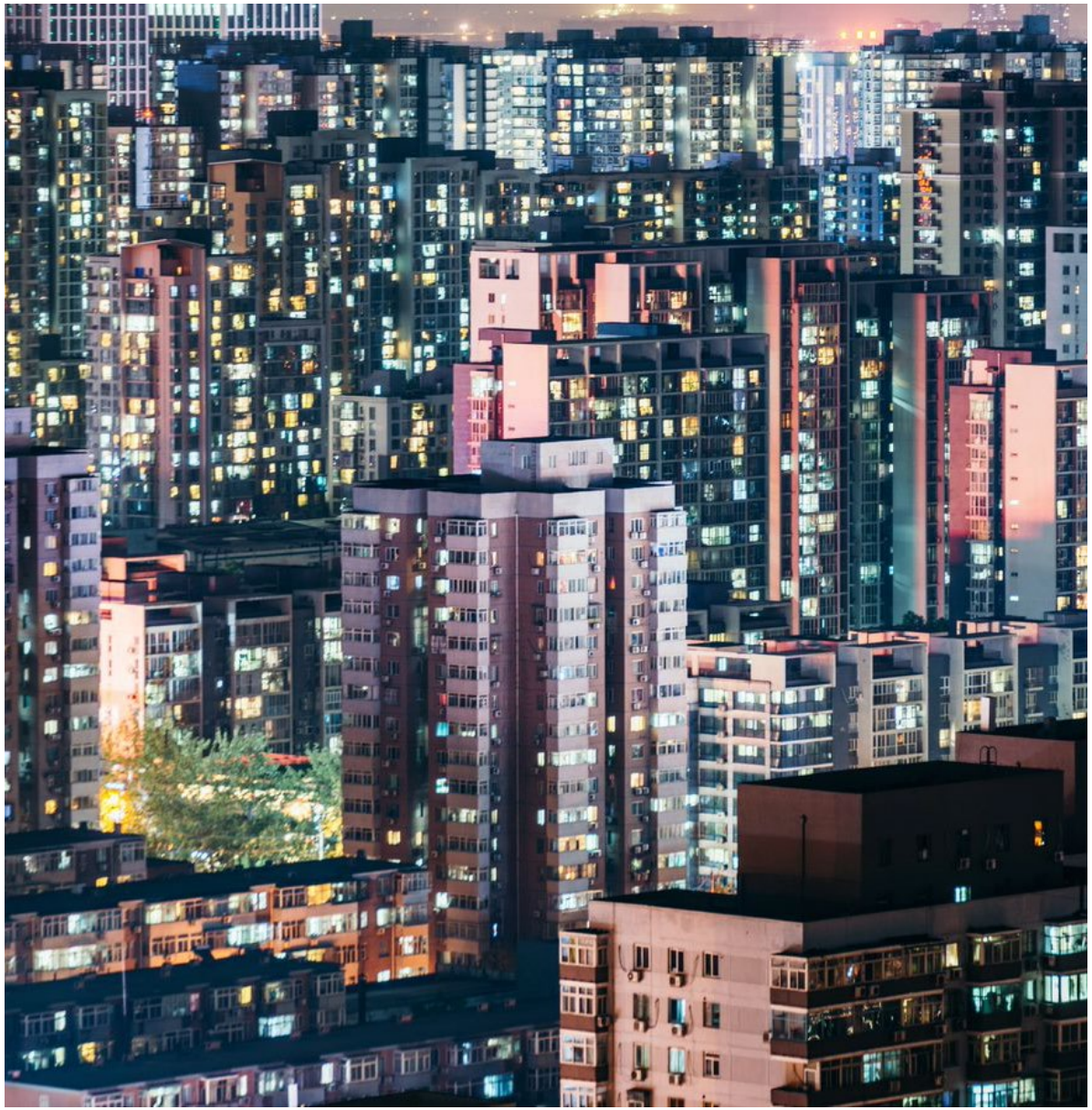
Managed security services
Data-driven. Expected outcomes.

1) **Data-centric**
   Leverage data to enable insightful analysis

2) **Tools to Platform**
   Evolve & leverage the right technology that enables a security platform from which to deliver consistent security operations

3) **Process Efficiency**
   Incorporate automation for scale & accuracy combined with human security operations expertise

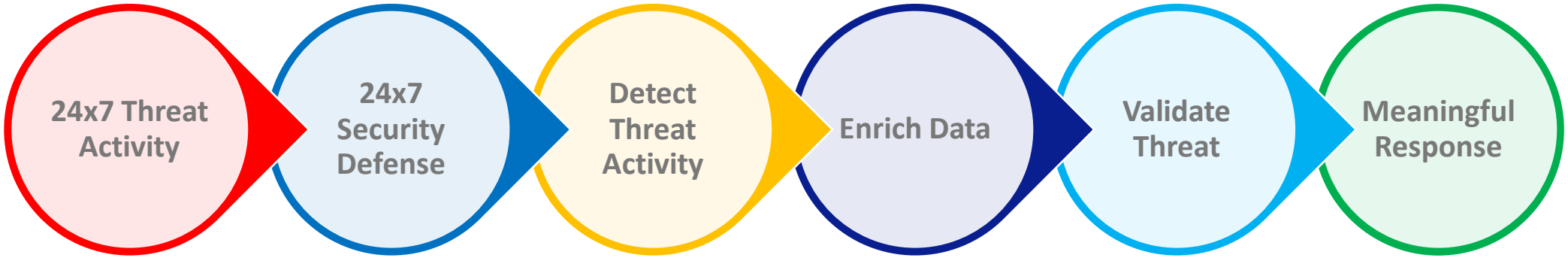
4) **Focused on Business Outcomes**
   The overall goal is daily risk mitigation & operational resiliency



24x7 managed security operations

Process: Mature & Consistent

Mazars managed security services provide a robust, comprehensive, and proactive approach for 24x7 security operations with the goal of security program maturity and overall risk mitigation.



Path to Security Operations Maturity
Phased Approach

Level 2: **Managed**
Processes characterized for projects and is often reactive

Level 4: **Quantitatively Managed**
Processes measured and controlled

Level 1: **Initial**
Process unpredictable, poorly controlled and reactive

Level 3: **Defined**
Processes characterized for the organization and is proactive

Level 5: **Optimizing**
Focus on process improvement

Mazars Goal: Quickly & systematically mature organizations from Level 1 to Level 4, then continue to grow