

**CYBERSECURITY
GOVERNANCE &
OPERATIONS**



**CAPABILITY
MODELING**



CYBER





CYBER

Services Overview

Governance, Risk & Compliance

- Strategic alignment of organizational goals
- Gap analysis of existing enterprise dynamics

Security Program Integrity

- Policy alignment with standard implementation
- Exception management and risk evaluation

Application Security & Technical Advisory

- Consensus and exploration of the business impact
- Deviations from accepted organizational norms

IT Change & Metrics

- Qualitative inquiry into IT administration
- Analysis of tactical and technical changes

Operational Awareness & Skills

- Skills evaluation of the “human-in-the-loop”



Governance Risk Compliance

Theory & Practical Implementations

- Evaluation of applicable framework implementation
- Analysis of state from certification and accreditation

Risk Management

- Risk assessment, evaluation, and recommendations
- Security test and evaluation

Maturity Assessment

- Cybersecurity program integrity and growth

Compliance

- Evaluation of the trilogy: compliance, privacy, and security

Summary of the Current State Dynamics



Security Program Integrity

Policy

- Evaluate discursive changes to policy
- Policy creolization

Standards

- Evaluate strategic alignment with IT implementations and Cyber Governance

Exceptions

- Manage discursive change and control aligned to policy and standards

Application of Fuzzy
Logic & Analytic
Capabilities



Application Security & Technical Advisory

Vulnerability Remediation

- Patch and Configuration Management
- Prioritization by Criticality and Sensitivity

Identification & Authentication

- User and Entity Behaviour Analytics (UEBA)
- Audit

Incident Response

- Correlation between Asset Bill of Materials, UEBA, and Threat Surface

Analysis of Networks, Systems & Integrations



IT Change & Metrics

CISO Dashboard

- Metrics for Decision Making
- IT Change and Cyber Program Integrity

Network and Security Operation Centers

- Operational and Situational Awareness through tailored analysis
- Runbooks

Communication and Information Feedback

- Enterprise analysis through Fuzzy Logic

Integration of Administrative & Technical Data Sources



Operational Awareness & Skills

Human-In-The-Loop

- Man-Machine Analysis of Controls
- Evaluation of human security operators

Knowledge, Skills & Abilities

- Measure core competencies based on job duties, operational environment, and resiliency

Balanced Scorecards

- Evaluation of risk management capabilities in context of operational environment and cyber capabilities

Attestation of the Investments in Security



Human and Entity Relationship

The evaluation of human factor cybersecurity competency across the dynamic systems integrating functional departments support understanding the contextual environment and inherent risks.

The Duality of Cybersecurity Risk