Managed.sa

Cybersecurity Orchestrator

Cybersecurity
Maturity Assessment

Security Governance
Program Development

Governance

Management Services

Managed.sa
Cybersecurity Orchestrator

Cybersecurity Maturity Assessment

Cybersecurity maturity Assessment will help your organization understand current cybersecurity posture, identify gaps and areas for improvement, and develop a roadmap for achieving higher levels of cyber maturity. Our service goes beyond standard cyber maturity assessments by considering more than just technical readiness. It provides a holistic perspective that includes people, processes, and technology.

By defining the cyber capabilities that need the board's attention and transforming them into a practical, business-enhancing function, our Service will assist you in advancing business goals, mitigating risks, fostering trust, and evaluating performance – converting information risk into a business asset.

Managed.sa
Cybersecurity Orchestrator

Key Features

The Maturity Assessment Service is a comprehensive evaluation of your organization's current cybersecurity posture compared to standards and regulatory requirements.

A. Our service identifies gaps in your existing controls and provides actionable recommendations to achieve compliance and enhance your security framework.

B. This assessment will provide your management and relevant stakeholders with a clear understanding of your current security posture and precisely where you stand regarding relevant standards and regulatory requirements.

Managed.sa
Cybersecurity Orchestrator

Benefits of Maturity Assessment:

1 Weakness Identification

Discover gaps and areas requiring enhancement in your current cybersecurity setup.

2 Compliance Assurance

Ensure your organization complies with relevant regulatory standards (e.g., NCA, SAMA, CST) to avoid fines and legal complications.

3 Security Enhancement

Improve your overall security stance by implementing best practices and addressing identified weaknesses.

4 Industry Peer Comparison

Utilize industry insights to benchmark against peers.

5 Cyber Maturity Evaluation

Assess cyber maturity on a site-by-site basis or at the company level.

6 Alignment with Industry Standards

Map cyber practices against recognized standards like NIST and ISO 27001.

7 Priority Setting

Identify key areas for a management action plan.

Cybersecurity Standards

NCA
National Cybersecurity Authority Standards

CST
Communications, Space, and Technology Commission Cybersecurity Standards

SAMA
Saudi Central Bank Cybersecurity Standards

ISO 27K
International Organization for Standardization ISO/IEC 27001

Managed.sa
Cybersecurity Orchestrator

Maturity Assessment Methodology

Our Maturity Assessment Methodology is based on the CMMI Cybermaturity Platform. Managed.sa methodology provides organizations with a structured and comprehensive approach to evaluating and enhancing their cybersecurity capabilities.

This methodology is grounded in the Capability Maturity Model Integration (CMMI) framework, which is widely recognized for its effectiveness in assessing and improving process maturity across various domains, including cybersecurity.

Step 01
Information Gathering

A

Customized Questionnaire

In this phase, we begin by crafting a customized questionnaire tailored to your specific requirements. The primary goal of this questionnaire is to simplify the process for you, especially for non-cybersecurity stakeholders, and to gain a comprehensive understanding of your current compliance level.

B

Interactive Workshops

We then conduct workshops with all relevant stakeholders to discuss existing processes and gather the necessary input. These workshops are designed to go beyond simply sharing a list of questions, providing an opportunity to clarify any ambiguities and ensure a clear understanding of the requirements.

Maturity Assessment Methodology

Step 02

Gap Assessment

A

Compliance Evaluation

We evaluate your current compliance status by comparing your implemented controls with the required controls based on the relevant regulations or standards you aim to comply with, such as NCA ECC, SAMA CSF, CST CRF, etc.

B

Maturity Level Identification

Next, we meticulously identify the maturity level of each control and the overall domain, categorizing them as implemented, partially implemented, or not implemented, in accordance with our defined criteria.

Maturity Assessment Methodology

Step 03

Reporting

A

Comprehensive Reporting

In the final phase, we prepare a detailed gap assessment report. This report comprehensively captures observations from the previous phases, outlining the compliance status of each control. It includes actionable recommendations and corrective actions necessary to achieve compliance, covering aspects such as technologies, policies, and processes.

B

Executive Summary Report

In addition to the detailed gap assessment report, we provide a high-level executive summary dashboards that highlights key findings, strategic insights, and essential recommendations for senior management, offering a clear vision of the current security compliance status and required actions that fit your unique business needs and operational environment.

Benefits of Maturity Assessment:

1 Comprehensive Cybersecurity Evaluation

The CMMI Cybermaturity Platform evaluates an organization's cybersecurity capabilities across several domains, including risk management, incident response, threat intelligence, asset management, and more. This comprehensive assessment ensures a holistic understanding of the organization's cybersecurity posture.

2 Maturity Levels

The assessment methodology uses a maturity model that defines different levels of cybersecurity maturity, ranging from Level 1 (Initial), where processes are ad hoc and reactive, to Level 5 (Optimizing), where processes are well-defined, proactive, and continually improved. Each level represents a more sophisticated and effective set of cybersecurity practices.

3 Benchmarking and Gap Analysis

The methodology allows organizations to benchmark their cybersecurity capabilities against industry standards and best practices. By identifying gaps between their current state and desired maturity levels, organizations can prioritize areas for improvement and allocate resources effectively.

4 Actionable Insights and Recommendations

The assessment provides detailed insights into the organization's strengths and weaknesses, along with actionable recommendations for improvement. This helps organizations develop a clear and strategic plan for enhancing their cybersecurity capabilities.

5 Continuous Improvement

The CMMI Cybermaturity Platform emphasizes continuous improvement by encouraging organizations to regularly assess and refine their cybersecurity practices. This iterative approach ensures that organizations remain resilient in the face of evolving cyber threats and can adapt to changing regulatory requirements and business needs.

6 Alignment with Business Objectives

The maturity assessment methodology aligns cybersecurity initiatives with broader business goals. By integrating cybersecurity into the overall business strategy, organizations can ensure that security efforts support business growth, innovation, and risk management.

Managed.sa
Cybersecurity Orchestrator

Benefits of Using the CMMI Cybermaturity Platform:

1

Enhanced Cyber Resilience

By systematically assessing and improving cybersecurity capabilities, organizations can better protect against cyber threats and minimize the impact of potential breaches.

2

Improved Risk Management

The maturity assessment helps organizations identify and prioritize risks, enabling them to implement effective controls and reduce their overall risk exposure.

3

Increased Operational Efficiency

A mature cybersecurity program leads to more efficient processes, reduced downtime, and optimized use of resources.

4

Regulatory Compliance

The CMMI Cybermaturity Platform helps organizations ensure compliance with various regulatory requirements and standards, reducing the risk of fines and legal issues.

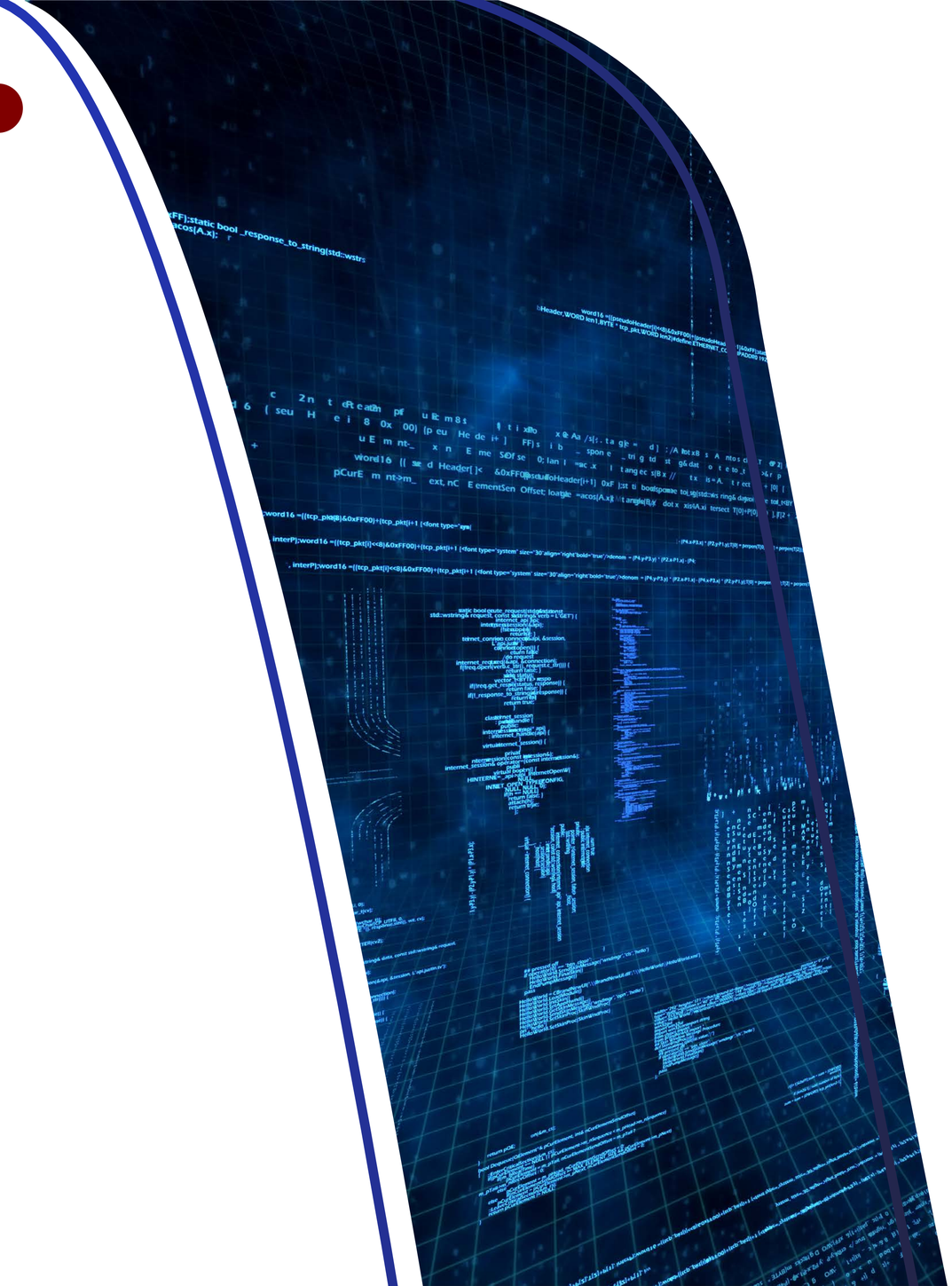
5

Strategic Decision-Making

With a clear understanding of their cybersecurity maturity, organizations can make informed decisions about where to invest in security and how to best protect their assets.

Security Governance Program Development

Our Security Governance Program Development service provides a comprehensive approach to establishing, maintaining, and enhancing an organization’s security governance framework. Security governance is the framework of tools, personnel, and processes that ensures effective risk management and aligns the security program with the organization’s overall business objectives. It encompasses the organizational structure, defi ned roles and responsibilities, metrics, processes, and oversight mechanisms that collectively enhance the security posture of the organization.



Managed.sa
Cybersecurity Orchestrator

Why

Information Security Governance Matters:

Information security governance is critical for safeguarding sensitive data, ensuring compliance with various regulations, effectively managing risks, and maintaining trust with stakeholders. A robust security governance framework helps organizations proactively address security challenges, minimize risks, and align security strategies with business goals. (Alignment with organization governance)

Managed.sa
Cybersecurity Orchestrator

Management • Governance • **Security Governance Program Development**

Our Services Include:

Development of Cybersecurity Policies, Procedures, and Standards

We help design and implement comprehensive cybersecurity policies, procedures, and standards that are aligned with business objectives and industry best practices and regulatory requirements. This includes establishing guidelines for data protection, access control, incident response, and more.

1

Conducting Regular Audits

Regular audits are essential to ensure that security policies and procedures are being followed and that controls are functioning effectively. We provide thorough audits to assess compliance, identify gaps, and recommend improvements.

2

Security Assessments and Gap Analysis

Our security assessments and gap analysis services help identify vulnerabilities within your current security program. We evaluate your organization's security posture against industry standards and regulatory requirements, highlighting areas for improvement.

3

Managing the Implementation of Security Controls

We assist in implementing as advisory and PMO to manage the end-to-end intiatiave
robust security controls designed to prevent data breaches and protect sensitive information. This includes technical controls (like firewalls and encryption) and administrative controls (such as user training and access management).
This service provided as a managed PMO
.

4

Managed.sa
Cybersecurity Orchestrator

Our Services Include:

Strategic Planning and Roadmap Development

Strategic planning is essential for the long-term success of a security program. We work with your team to develop a security roadmap that aligns with your organization's goals, ensuring that security initiatives are prioritized and resources are effectively allocated.

5

Expert Advice on Emerging Threats and Technologies

Our team of experts provides insights on the latest threats and emerging technologies. This ensures that your organization stays ahead of evolving security risks and takes advantage of new opportunities to enhance your security posture.

6

Strategic Advisory Services for Board Members and Executives

We offer strategic advisory services tailored for board members and executives to help them understand the importance of security governance, make informed decisions, and integrate security considerations into the broader business strategy.

7

Methodology based on Corporate Governance Framework

Managed.sa
Cybersecurity Orchestrator

Benefits of Maturity Assessment:

1. Enhanced Risk Management

By implementing a structured governance framework, your organization can better identify, assess, and mitigate security risks.

2. Regulatory Compliance

Our services ensure that your security program aligns with relevant regulations and standards, helping to avoid penalties and legal issues.

3. Improved Security Posture

With comprehensive policies, procedures, and controls in place, your organization will be better equipped to protect sensitive data and prevent breaches.

4. Alignment with Business Objectives

Our approach ensures that your security program supports and enhances your overall business strategy, fostering a security-conscious culture within the organization.

5. Informed Decision-Making

Our advisory services equip executives with the knowledge needed to make strategic security decisions, ensuring that security investments are aligned with business goals.

By partnering with managed.sa for Security Governance Program Development, your organization can build a strong foundation for managing security risks, ensuring compliance, and safeguarding assets.

Managed.sa
Cybersecurity Orchestrator

Managed.sa
Cybersecurity Orchestrator

3273 Anas Ibn Malik - Al Sahafah Dist.
Riyadh 13321 - 8347
Kingdom of Saudi Arabia

+966 11 4185222

managed.sa