	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

<b>Description of Request</b>	Information Security Scorecards Managed Services for a period of (5) five years. Solution implementation of 12 months and thereafter four year M&S.
-------------------------------	---


## 1. High level background

A cybersecurity scorecard for a company is a tool or framework that assesses and measures the organization's cybersecurity posture and provides an overall score or rating. It is designed to evaluate various aspects of an organization's security practices, controls, and vulnerabilities to determine the effectiveness of its cybersecurity program.

Critical cybersecurity applications and various IT security platforms being compromised due to attacks against critical network security infrastructure and business systems, cyber-security shortfalls or instability leading to severe business disruptions.

The requirement for a cybersecurity scorecard is driven by the increasing frequency and sophistication of cyber reporting to different stakeholder, the need to comply with industry regulations, the risk of reputational damage from data breaches, the importance of managing vendor and supply chain risks, the need for board and executive oversight, and the recognition that cybersecurity is an ongoing process.

Overall, a cybersecurity scorecard is a valuable tool for organizations to assess, monitor, and enhance their cybersecurity posture, align with industry regulations, and instil confidence in different stakeholders regarding the company's security practices. It enables proactive risk management, compliance, and continuous improvement in an increasingly complex and threat-prone digital landscape.

	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

## 2. Business Objective

To deploy a managed service that is scalable (i.e., meaning it should be able to accommodate Eskom size), AI-powered platform that continuously monitors, analyses, and reports on the enterprise's cybersecurity hygiene, risks, and compliance posture. The solution service should enable proactive threat mitigation, asset lifecycle management, and strategic decision-making through advanced analytics, customizable reporting, highly customisable dashboards, and integration with existing security ecosystems. The capability should afford the individual team members and or managers to report on their respective functional areas. The platform should be compatible to all operating system regardless of the platform (i.e., laptop, mobile device, etc)


## 3. Scope of work/Business requirements

A cybersecurity scorecard can help organizations to overcome these challenges by providing a clear picture of their security posture, identifying areas for improvement, and prioritizing security investments. By taking steps to improve their security posture, organizations can reduce their risk of data breaches and the associated costs and consequences. Cybersecurity scorecard business requirements core capabilities shall include but not be limited to the following:

### 3.1. AI/ML-Driven Risk Intelligence

- **AI Engine:** Deploy an AI/ML engine to generate dynamic risk cards, prioritized alerts, and predictive threat analytics.
- **Automated Remediation Guidance:** Provide AI-generated reports with actionable recommendations aligned with the organization's architecture and risk appetite.
- **API Ecosystem:** Enable seamless integration with existing tools (SIEM, EDR, ITSM) via RESTful APIs for bidirectional data exchange.
- **Data integration:** Integration with related data sources shall be done in a phased approach. All the data collected for analysis shall reside at Eskom predefined storage services (i.e., Eskom data centre or Eskom Cloud) which upon contract expiry shall be handed over to Eskom data custodians.

### 3.2. Real-Time Monitoring & Hygiene Management

	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

- **Continuous Asset Visibility:** Achieve near real-time monitoring of network security performance, vulnerabilities, and misconfigurations across on-premises, cloud, and hybrid environments.
- **Agentless Architecture:** Ensure full network and asset visibility without endpoint agent deployment, minimizing operational overhead.
- **Mobile Device Support:** Monitor security posture for mobile devices (iOS, Android) and integrate findings into unified dashboards.

### 3.3. Compliance & Reporting

- **Customizable Framework Alignment:** Generate reports mapped to NIST, ISO 27001, CIS, GDPR, PoPIA, and utility-specific regulations.
- **Regulatory Progress Tracking:** Track compliance status against mandated requirements and automate audit-ready documentation.

### 3.4. Asset Discovery & Classification

- **External/Internal Asset Inventory:** Continuously scan and catalog external-facing assets (e.g., web servers, APIs) and internal endpoints.
- **Dynamic Classification:** Auto-classify assets by criticality, exposure, and data sensitivity (e.g., PII repositories, public-facing services).
- **SSL Certificate Grading:** Evaluate SSL/TLS certificates, prioritize vulnerabilities (e.g., expiry, weak ciphers), and provide remediation steps.

### 3.5. Threat Intelligence & Response

- **Threat Actor Dashboard:** Aggregate external threat feeds (IoCs, TTPs, compromised assets) into a centralized view for proactive defence.
- **Malicious Asset Tracking:** Flag and isolate assets tagged as malicious (e.g., blacklisted IPs, domains).
- **Simulated Attack Validation:** Integrate automated attack scenarios (e.g., phishing, ransomware simulations) to validate security controls and metric accuracy.

### 3.6. Remediation & Playbooks


- **Technical Playbooks:** Provide standardized workflows for mitigating risks (e.g., patch management, incident response) aligned with MITRE ATT&CK.
- **Improvement Guides:** Deliver contextualized guidance to mature security practices (e.g., zero-trust adoption, encryption protocols).

### 3.7. Strategic Posture Management

#### 3.7.1. Security Posture Benchmarking

- Measure organizational security maturity against industry benchmarks (e.g., peers, sector averages) to identify gaps and strengths.
- **Risk Prioritization:** Leverage AI-driven insights to prioritize investments based on criticality, business impact, and cost-benefit analysis.

#### 3.7.2. Progress Tracking & Reporting

	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

- **Historical Trend Analysis:** Track security posture improvements over time via visual timelines and KPI dashboards.
- **Executive Dashboards:** Provide a single-pane view of cybersecurity hygiene, performance, and alignment with business goals.

### 3.7.3. Data-Driven Decision Support

- **Cross-Service Data Interpolation:** Synthesize data from disparate tools (e.g., vulnerability scanners, firewalls) into actionable insights for strategic, tactical, and operational decisions.
- **Innovation Enablement:** Deliver clean, validated datasets to support AI/ML initiatives, threat modelling, and ROI calculations for security investments.

### 3.7.4. Stakeholder Communication

- **Customer/Partner Reporting:** Generate tailored reports to demonstrate compliance, resilience, and security maturity to external stakeholders.

### 3.7.5. Dashboards

- The executive dashboard reports
- IT and OT maturity assessments
- IT and OT security posture
- Overall information security posture in comparison with other similar sectors
- Trends analysis to show whether we are improving or not

## 4. Implementation Principles

Solution implementation of 12 months and thereafter (4) four-year M&S.

The Cybersecurity Scorecard initiative will adhere to the following foundational principles to ensure alignment with organizational objectives, operational continuity, and long-term sustainability:

### 4.1. Clearly Defined Deliverables:

The project will be structured around specific, measurable, and time-bound deliverables to ensure transparency and accountability throughout all phases of execution.

### 4.2. Well-Defined Milestones:


Progress will be tracked against explicit milestones, enabling stakeholders to monitor timelines, resource allocation, and critical decision points with precision.

### 4.3. Phased Integration with Existing Systems:

Integration of diverse data sources will be executed via a staged approach to minimize operational disruption, ensure compatibility, and validate system interoperability at each phase.

### 4.4. Post-Implementation Support & Expertise:

Upon project completion, dedicated, two highly skilled personnel will be assigned to maintain and update dashboards in real time. These resources will remain readily available to generate ad-hoc reports and provide analytical support to meet evolving business and compliance requirements.

	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

## 5. Professional Services

Professional consulting services post project execution during the four (4) years of the system operations and service support. This includes products specialists that will assist Eskom with the following:

- Project management for major products upgrades and enhancements
- Solution design
- Development, testing, configuration, documentation, and implementation of enhancements of products that are currently deployed including associated interfaces to Eskom applications
- Project Implementation shall only be for the first year and support will happen on the second year after proper optimisation of the service.
- Upon project completion, dedicated, two highly skilled, expert level personnel will be assigned to maintain and update dashboards in real time. These resources will remain readily available to generate ad-hoc reports and provide analytical support to meet evolving business and compliance requirements. The maximum capped hours of 1760 per year per resource shall be applied from second year to end of the contract.
- No Travelling shall be required except going to Eskom head office at Megawatt Park.


## 6. Training/Transfer of skills:

- Provide onsite, classroom-based and web-based training for end-users and system support staff on a pre-booked basis. The recommended method of training delivery would be required during the implementation phase.
- Solution training shall be provided for 10 people including exam certification. This shall cover train the trainer session. The training shall commence on project implementation to enable better comprehension of service support.
- Mentor 10 Eskom resources through the installation, configuration and deployment stages using a defined skills transfer program.
- The service provider will be required to train Eskom IT staff to provide first line support. This will be determined as part of the contract terms.

## 7. Service Level Agreement requirements

Below are the minimum requirements for SLA which shall be incorporated into the comprehensive and detail SLA upon identifying the successful nominated supplier.

Service Level	Description	Escalation to SP	Escalation to OEM
Critical	Business has stopped	Response within 1 (one) hour – Level 1 Response within 1 (one) hour – Level 2	Response within 1 (one) hour – Level 3
Major	Business severely impacted	Response within 1 (one) hour – Level 1	Response within 3 (four) hours – Level 3

	<b>TENDER SCOPE OF WORK</b>  <b>Group Information Technology</b>	<b>Template Identifier</b>	240-IT042	<b>Rev</b>	1
		<b>Effective Date</b>	April 2023		
		<b>Review Date</b>	April 2028		

		Response within 1 (one) hour – Level 2	
Normal	Minor business impact/product failure	Response within 1 (one) business day – Level 1 Response within 2 (two) business days – Level 2	Response within 1 (one) business day – Level 3
Low	No business impact but requires one or more updates	Response within 2 (two) business days – Level 1 Response within 2 (two) business days – Level 2	Response within 2 (two) business days – Level 3
Informational	Request for information	Response within 3 (three) business days – Level 1 Response within 3 (three) business days – Level 2	Response within 3 (three) business days – Level 3

## 8. Approvals: