

**Request For Proposal**

Managed Network Operations Center & Managed Security Operations Center Services Tender Document

Contents

[1. Introduction and Background 3](#_Toc191893458)

[2. Scope of Work 4](#_Toc191893459)

[2.1 Managed Network Operations Center (MNOC) 4](#_Toc191893460)

[2.2 Managed Security Operations Center (MSOC) 4](#_Toc191893461)

[2.3 Additional Services 5](#_Toc191893462)

[3. Technical Requirements 6](#_Toc191893463)

[4. Service Level Agreements (SLAs) 6](#_Toc191893464)

[4.1 Uptime and Availability 6](#_Toc191893465)

[4.2 Incident Response and Resolution Times 6](#_Toc191893466)

[4.3 Disaster Recovery and Business Continuity 7](#_Toc191893467)

[4.4 Compliance and Reporting 7](#_Toc191893468)

[4.5 Escalation Procedures 7](#_Toc191893469)

[5. Vendor Qualifications 7](#_Toc191893470)

[6. Compliance and Security Standards 7](#_Toc191893471)

[8. Submission Guidelines 8](#_Toc191893472)

[9. Existing Environment and Site Breakdown 8](#_Toc191893473)

[9.1 Site Breakdown 8](#_Toc191893474)

[9.2 Current Topology and Services 9](#_Toc191893475)

[9.3 Services for All Sites 10](#_Toc191893476)

[10. Monitoring Platform Capabilities 10](#_Toc191893477)

[10.1 Core Capabilities 10](#_Toc191893478)

[10.2 Advanced Features and Best Practices 11](#_Toc191893479)

[10.3 Additional Functionalities 12](#_Toc191893480)

[10.4 Vendor Support and Platform Scalability 12](#_Toc191893481)

[11. Reports and Dashboards 12](#_Toc191893482)

[11.1 Types of Reports 13](#_Toc191893483)

[11.1.1 Incident Management Reports 13](#_Toc191893484)

[11.1.2 Performance and Availability Reports 13](#_Toc191893485)

[11.1.3 Security and Compliance Reports 13](#_Toc191893486)

[11.1.4 Disaster Recovery and Business Continuity Reports 14](#_Toc191893487)

[11.1.5 Environmental and Infrastructure Reports 14](#_Toc191893488)

[11.2 Types of Dashboards 15](#_Toc191893489)

[11.2.1 Executive Dashboard 15](#_Toc191893490)

[11.2.2 Security Operations Dashboard 15](#_Toc191893491)

[11.2.3 Network Operations Dashboard 15](#_Toc191893492)

[11.2.4 Incident Management Dashboard 15](#_Toc191893493)

[11.2.5 Disaster Recovery and Business Continuity Dashboard 15](#_Toc191893494)

[11.2.6 Environmental and Infrastructure Monitoring Dashboard 16](#_Toc191893495)

[A. Evaluation Criteria and Selection Process 16](#_Toc191893496)

[B. Instructions for Evaluation: 17](#_Toc191893497)

[C. Evaluation Criteria Table 17](#_Toc191893498)

[Evaluation Methodology 19](#_Toc191893499)

#### **Managed Network Operations Center & Managed Security Operations Center Services Tender Document** Lebanese Red Cross ICT Section

### 1. Introduction and Background

The Lebanese Red Cross (LRC) is a prominent humanitarian organization committed to delivering vital emergency and healthcare services. As part of its mission to maintain a resilient IT infrastructure and secure digital operations, LRC is seeking to engage a qualified vendor for Managed Network Operations Center (MNOC) and Managed Security Operations Center (MSOC) services.

This tender aims to enhance LRC’s operational capabilities by ensuring continuous monitoring, prompt incident response, and the protection of its IT infrastructure from evolving security threats. The selected vendor will provide comprehensive services to meet LRC’s high standards for uptime, security, and scalability, and will support the ongoing transformation of the organization’s IT operations.

### 2. Scope of Work

### 2.1 Managed Network Operations Center (MNOC)

The MNOC service must ensure 24/7 proactive monitoring and management of LRC’s network infrastructure, providing the following services:

* **Proactive Network Monitoring**: Continuous monitoring of network health, identifying bottlenecks, hardware failures, and security vulnerabilities in real-time.
* **Performance Optimization**: Monitoring bandwidth usage, ensuring efficient utilization, and identifying areas for improvement in both network design and operational efficiency.
* **Incident Management**: Identification, escalation, and resolution of network incidents, aiming to restore normal operations swiftly with minimal impact on business activities.
* **Capacity Planning and Management**: Ensuring scalability of network infrastructure to handle future growth and changes in operational demands.
* **Configuration Management**: Maintaining a repository of configuration details for network devices and systems to streamline troubleshooting and change management.
* **Reporting and Analytics**

Regular performance and SLA compliance reports

Custom dashboards and predictive analytics

* **Quality of Service (QoS) Management**

Traffic prioritization for critical applications

Bandwidth allocation and latency reduction

### 2.2 Managed Security Operations Center (MSOC)

The MSOC service must provide 24/7 monitoring, detection, analysis, and response to cybersecurity incidents across all IT infrastructure and endpoints. Key services include:

* **SIEM (Security Information and Event Management)**: Real-time collection, aggregation, and analysis of security event data.
* **SOAR (Security Orchestration, Automation, and Response)**: "SOAR (Security Orchestration, UEBA, Automation, and Response): The vendor must leverage SOAR to implement advanced automation capabilities, including:
  + Dynamic Playbooks: Develop and deploy dynamic, pre-configured playbooks for common incident types (e.g., malware detection, phishing, brute-force attacks) that allow for automated detection, containment, and remediation.
  + Automated Threat Containment: Enable automated responses to high-confidence alerts, such as isolating compromised endpoints, blocking malicious IP addresses, and disabling suspicious accounts, without requiring manual intervention.
  + Machine Learning and AI Integration: Incorporate machine learning algorithms to refine automated workflows based on incident trends and threat patterns, improving detection and response over time.
  + Customizable Workflows: Provide flexibility for LRC to define and customize workflows based on organizational requirements, ensuring tailored responses to specific threat scenarios.
  + Continuous Improvement: Include mechanisms to analyze past incidents and refine automation processes, ensuring SOAR remains effective against evolving threats.
  + Seamless Integration: Ensure SOAR integrates with existing tools, including SIEM, endpoint protection, and ticketing systems, to enable end-to-end automation of the incident lifecycle."
  + Detect deviations from baseline behavior, such as unusual login patterns, access to sensitive data, or unauthorized data transfers.
* **Endpoint Detection and Response (EDR)**: Continuous monitoring and response to security incidents on endpoint devices, ensuring the protection of user devices and servers.
* **Threat Intelligence Integration**: Integration with global threat intelligence providers to ensure proactive defense against emerging threats and zero-day attacks.
* **Vulnerability Management**: Ongoing vulnerability assessments, quarterly penetration testing (four per year), and timely remediation of identified risks. The process must include:
  + Comprehensive Testing: Internal and external testing of systems, applications, and network infrastructure.
  + Red Team/Blue Team Exercises: Annual exercises to simulate advanced persistent threats (APTs) and assess SOC detection and response capabilities.
  + Post-Test Validation: Follow-up testing to confirm remediation effectiveness and eliminate residual risks.
  + Detailed Reporting: Reports categorizing vulnerabilities by severity with actionable mitigation steps and timelines.
  + Standards Compliance: Adherence to OWASP, NIST, and other recognized frameworks."

### 2.3 Additional Services

* **Disaster Recovery Management**: Ensuring the organization’s systems are resilient to failures and can recover rapidly from disruptions.
* **Business Continuity Planning (BCP)**: Creating and maintaining plans to ensure that critical operations can continue in the event of a disaster.
* **Cybersecurity Awareness Training**: Training LRC staff on best practices for security hygiene, threat detection, and incident reporting.
* **Dark Web Monitoring**: Continuous scanning of dark web forums and marketplaces to identify any compromised data or threats related to LRC’s operations.
* **Incident Management Tool Integration**: Integration of an automated incident response tool to streamline workflows and ensure timely response to incidents.
* **Regulatory Compliance Audits**: Regular audits of infrastructure and practices to ensure compliance with relevant regulations, including GDPR, HIPAA, and ISO 27001.

### 3. Technical Requirements

The vendor must provide solutions that meet the following technical requirements:

* **Monitoring Platforms**: Cloud-based solutions for scalability and flexibility, with a preference for those hosted in Lebanon for data sovereignty compliance.
* **Multi-Site Monitoring**: Monitoring solutions that provide visibility across all sites, including remote offices and field operations.
* **Data Encryption and Security**: All communication between monitoring platforms and LRC infrastructure must be encrypted using industry-standard encryption protocols.
* **Integration Capabilities**: The solution must integrate seamlessly with existing LRC IT infrastructure, including ticketing systems, network management tools, and cybersecurity solutions.

### 4. Service Level Agreements (SLAs)

The SLAs must include the following performance metrics and benchmarks, based on global best practices for similar-sized organizations:

### 4.1 Uptime and Availability

* **Service Availability**: 99.9% uptime for all critically managed services, including both NOC and SOC operations. Downtime beyond this threshold must be compensated as per the penalty clause.
* **System Monitoring**: Continuous monitoring of critical systems with alerts and automatic failover for redundancy in the event of failure.

### 4.2 Incident Response and Resolution Times

* **Penetration Testing** Frequency and Reporting: Vendors must ensure regular penetration testing is conducted, with:
  + Scheduled tests are performed at least every 3 months.
  + Reports delivered within 10 business days post-testing, including identified risks and mitigation plans.
  + Critical vulnerabilities addressed within 25 days of identification, with penalties for delays in resolution."
* **Incident Detection**: The ystem must detect critical incidents (e.g., security breaches, service outages) within 5 minutes of occurrence.
* **Initial Response Time**: Acknowledgment of critical incidents within 15 minutes of detection.
* **Incident Resolution**:
  + High Priority Incidents (e.g., cybersecurity breach, critical network downtime): Resolution or mitigation within 2 hours.
  + Medium Priority Incidents (e.g., non-critical system performance issues): Resolution or mitigation within 6 hours.
  + Low Priority Incidents (e.g., minor issues with no immediate impact on operations): Resolution within 24 hours.

### 4.3 Disaster Recovery and Business Continuity

* **Recovery Point Objective (RPO)**: The maximum acceptable amount of data loss is 1 hour.
* **Recovery Time Objective (RTO)**: The maximum allowable downtime for critical systems is 4 hours.

### Compliance and Reporting

* **Audit Reporting**: Monthly and quarterly audit reports, including security posture reviews, compliance checks, and recommendations for improvements.
* **Compliance Audits**: Annual external compliance audits with ISO 27001, HIPAA,

GDPR, and relevant cybersecurity regulations.

### 4.5 Escalation Procedures

* **Tiered Escalation Process**: Defined escalation levels with clear response times for unresolved issues at each tier.
* **Major Incident Review**: All major incidents (security breaches, critical system downtime) will be reviewed within 48 hours of resolution, with a report detailing actions taken and lessons learned.

### 5. Vendor Qualifications

Vendors must meet the following qualifications:

* **Industry Certifications**: Cisco Gold Partner, ISO 27001 certification, and a recognized SIEM MSSP partner.
* **Experience**: Proven experience working with NGOs or large humanitarian organizations. References from at least 4 similar organizations (at least 1 NGO).
* **Certified Staff**: A team of certified professionals, including CCIE, CISSP, CEH, and ITIL certifications, with a minimum of 3 years of experience in NOC/SOC operations.

### 6. Compliance and Security Standards

The vendor must comply with the following standards:

* **ISO 27001**: Information security management.
* **GDPR**: General Data Protection Regulation compliance.
* **ITIL**: Adherence to ITIL best practices for service management.
* **NIST CSF**: Compliance with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

### 8. Submission Guidelines

Proposals submitted include the following:

* **Technical Proposal**: Details of services offered, technical specifications, and integration capabilities.
* **Financial Proposal**: Detailed cost breakdown for a 3-year contract, including options for annual increases.
* **Vendor Qualifications**: Certifications, references, and staff CVs.
* **SLA Document**: A detailed SLA, including uptime, incident response times, escalation procedures, and reporting frequency.

### 9. Existing Environment and Site Breakdown

The following tables outline the updated infrastructure and assets across all LRC sites, which will be included in the scope of the tender for Managed Network Operations Center (MNOC) and Managed Security Operations Center (MSOC) services. This includes proactive monitoring for critical systems such as UPS and temperature sensors at key locations.

### 9.1 Site Breakdown

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Department** | **Location** | **Devices End User** | **Routers** | **Switches** | **Firewalls** | **Physical Servers** | **VMs** | **Access Points** | **Wireless Controllers** | **Telephony Servers** | **Storage** | **UPS** | **Telular** |
| LRC HQ | Spears, Hadat, | 75 | 2 | 23 | 3 | 2 | 31 | 25 | 1 | 4 | 1 | 1 | 1 |
| 140 Dispatch Centers | HazmiehTebnineGamma Zahle DR | 30 | 3 | 4 | 3 | 4 | 4 | 7 | - | 11 | - | 1 | 1 |
| Hotline 170 and Backup Center | Spears  DR Site Antelias | 15 |  | 4 | 0 | 4 | 4 | 2 | 0 | 2 | - | - | - |
| Blood Bank Centers (13 BTS) | Antelias, Saida, Halba, Jbeil, NabatiehJounieh, Tyr, Rachaya, Zahle, Chouf, Tripoly | 52 | 13 | 13 | 1 | 1 | 3 | 13 | 1 | 1 | 1 | 13 | 1 |
| Medico-Social Services (MSS) | Aley Batroun Tripoli Jal Eldeib Msaytbeh Jbeil | 30 | 6 | 6 | 1 | 1 | 2 | 12 | 0 | 6 | 0 | 6 | - |
| Disaster Risk Reduction (DRR) | Hazmieh | 25 | 1 | 2 | 1 | 0 | 0 | 4 | 1 | 1 | 1 | 1 | - |
| Disaster Management Services | Hadad | 31 | 1 | 8 | 1 | 1 | 3 | 15 | 1 | 1 | 1 | 1 | - |
| Nursing University | Baabda | 9 | 1 | 5 | 1 | 1 | 3 | 7 | 1 | 1 | 1 | 1 | - |
| Total |  | 267 | 27 | 65 | 11 | 14 | 50 | 85 | 5 | 27 | 5 | 24 | 3 |

**Total Number of Locations: 36 LRC sites (includes HQ, Blood Bank, MSS, DRR, DMS, Nursing University, and Disaster Response sites)**

### 9.2 Current Topology and Services

* **Hotline 170 and Backup Center**: This site includes the critical emergency hotline and a dedicated backup center. It will receive active 24/7 monitoring of network devices, systems, and telecommunication infrastructure.
* **Blood Bank Centers (13 BTS)**: These centers are critical for blood collection and storage operations, requiring active 24/7 monitoring, especially for temperature sensors and UPS systems. Notifications via email and phone call should be triggered in case of any failures or anomalies.
* **Medico-Social Services (MSS)**: This service includes multiple facilities providing medical and social support, all of which need active monitoring and incident management for IT systems and infrastructure.
* **Disaster Risk Reduction (DRR) Centers**: Six locations focusing on disaster preparedness, response, and mitigation. Active monitoring of their critical systems, including UPS and environmental sensors, is essential.
* **Disaster Management Services (DMS)**: Eighteen sites dedicated to disaster management operations, each requiring 24/7 monitoring, incident response, and system alerts (including UPS and temperature sensor monitoring).
* **Nursing University (5 Locations)**: Monitoring of infrastructure at all five university locations, with active alerts for potential incidents affecting IT resources.

### 9.3 Services for All Sites

* **UPS and Temperature Sensors Monitoring**: Active 24/7 monitoring of Uninterruptible Power Supply (UPS) systems and temperature sensors at critical locations, including blood bank centers, disaster management centers, and other sensitive sites.
  + **Notification System**: Automated alerts via email and phone call in the event of power failures, temperature deviations, or other critical incidents.

### 10. Monitoring Platform Capabilities

The monitoring platform provided by the selected vendor must adhere to global best practices, ensuring robust and effective management of the entire LRC infrastructure. The platform must deliver the following capabilities to provide real-time insights, improve operational efficiency, and support proactive incident detection and response.

### 10.1 Core Capabilities

* **Proactive Monitoring**: The platform must provide 24/7 real-time monitoring of all IT infrastructure components, including network devices (routers, switches, firewalls), servers (physical and virtual), telecommunication systems, UPS systems, and environmental sensors (temperature, humidity, etc.).
* **Multi-Site and Distributed Architecture**: The platform should be capable of monitoring distributed environments across multiple locations, using remote probes or agents to provide visibility into LRC's geographically diverse sites. The platform should support seamless monitoring across all 36 LRC sites, including remote and field offices.
* **Performance Management**: The platform must continuously monitor and optimize the performance of IT systems, ensuring that all systems operate efficiently and meet established service levels. It should track key performance indicators (KPIs) to proactively identify potential issues, such as network latency, bandwidth consumption, CPU and memory utilization, and service availability.
* **Incident Detection and Alerts**: The platform must automatically detect incidents and anomalies, providing customizable alerts based on predefined thresholds. Alerts must be sent through multiple channels (email, SMS, phone calls, or integrated messaging systems) for critical incidents to ensure prompt response.
* **Threshold-Based Alerts**: The system should allow for flexible configuration of alert thresholds, enabling LRC to tailor the monitoring solution to their specific operational requirements. This ensures that system performance is always within the acceptable range, with proactive notifications when thresholds are exceeded.
* **Root Cause Analysis**: The monitoring platform should be able to perform automated root cause analysis for detected incidents, this tool should reduce the time required to gather relevant data, thus supporting experts in performing a thorough investigation and minimizing downtime. However, the RCA process remains dependent on expert input for accurate diagnosis and resolution.

### 10.2 Advanced Features and Best Practices

* **Distributed Monitoring Probes**: To monitor different locations efficiently, the platform must allow for the use of distributed probes or agents. This will provide granular visibility into network and system performance across all LRC sites, including remote locations and field offices.
* **Capacity Planning and Forecasting**: The platform should include advanced analytics capabilities for predicting future resource requirements based on historical trends and usage patterns. This will help ensure LRC’s infrastructure is properly sized to meet current and future operational demands.
* **Historical Data Analysis and Trend Reporting**: The platform should store up to 6 months of historical monitoring data for capacity planning, troubleshooting, and trend analysis. Detailed reports should be generated to help understand usage patterns, identify potential bottlenecks, and support decision-making.
* **Customizable Dashboards**: The platform should provide customizable, role-based dashboards that allow LRC’s IT staff to easily view real-time data, performance metrics, and incident statuses. Dashboards should be user-friendly, enabling efficient monitoring at a glance.
* **Automated Ticketing Integration**: The monitoring platform must integrate seamlessly with the vendor’s incident management system (e.g., ServiceNow, Jira) or any other existing ticketing systems to automatically generate and track incident tickets. This integration ensures that incidents are recorded, prioritized, and managed effectively.
* **Security Event Monitoring**: The monitoring solution must support integration with LRC’s Security Information and Event Management (SIEM) system. This allows for the aggregation of security-related data across all devices, providing a comprehensive view of potential threats and enabling quick identification of any security incidents or breaches.
* "The monitoring platform must include AI-driven analytics to enhance real-time detection and response, leveraging advanced algorithms for root cause analysis and anomaly detection."
* UEBA functionality must be integrated into the monitoring platform, enabling continuous behavior tracking and risk scoring of users and entities."
* **Compliance and Regulatory Reporting**: The platform must support automated compliance reporting for various regulatory requirements (e.g., ISO 27001, GDPR). It should have predefined templates for compliance reports, helping LRC meet industry standards and audits with minimal effort.
* **Integration with ITSM (IT Service Management)**: The platform should integrate with ITSM tools (e.g., ServiceNow, ITIL-based systems) for change management, incident management, and problem management. This ensures a unified approach to service delivery and enhances operational efficiency.
* **Virtualization and Cloud Monitoring**: Given the growing use of virtualized environments and cloud services, the platform must support monitoring of virtual machines (VMs), cloud-based workloads, and hybrid cloud infrastructures, providing visibility into both on-premise and cloud environments.
* **Automated Remediation**: The platform should include automated remediation features to address common incidents without manual intervention, reducing response time and ensuring that minor issues do not escalate into larger problems. This can include automated system restarts, service reroutes, or patch deployments.

### 10.3 Additional Functionalities

* **User and Role-Based Access Control**: The platform must allow for role-based access control (RBAC), ensuring that sensitive information is only accessible to authorized personnel. This is essential for maintaining confidentiality and security within the monitoring system.
* **Service Dependency Mapping**: The system should automatically discover and map service dependencies across the IT infrastructure. This mapping helps to understand how components interact and provides insights into the potential impact of incidents on business operations.
* **Automated Workflow Management**: The platform should support automated workflows for incident escalation, ticketing, and reporting. This streamlines the incident management process and ensures a faster, more efficient resolution.
* **Cloud and Hybrid Deployment Support**: The platform should support hybrid and multi-cloud environments, enabling LRC to monitor on-premises, private cloud, and public cloud systems from a single dashboard.
* **Data Security and Privacy**: All data transmitted and stored within the monitoring platform must be encrypted using the highest industry standards (e.g., AES-256). It should also comply with all relevant data protection regulations (e.g., GDPR, HIPAA).
* **Custom Reporting**: The platform should provide customizable reports that can be tailored to meet LRC’s operational needs. This includes generating reports for management reviews, compliance audits, and detailed incident analysis.
* **Integration with Threat Intelligence**: The platform should integrate with threat intelligence services to provide real-time alerts about new or evolving threats that may impact LRC’s IT infrastructure. This integration enhances LRC’s ability to proactively defend against cyber-attacks.

### 10.4 Vendor Support and Platform Scalability

* **Scalability**: The platform should be highly scalable, capable of accommodating future expansion as LRC’s network grows. This includes the ability to easily add new sites, devices, and systems without major overhauls.
* **Vendor Support**: The vendor must offer 24/7 support for the monitoring platform, including troubleshooting, updates, and patches. The support team should have deep expertise in the platform and be able to provide quick resolutions to issues that may arise.

### 11. Reports and Dashboards

As part of the managed services, the vendor is required to deliver a variety of reports and dashboards that will provide LRC with real-time insights, historical data, and actionable intelligence to manage its IT operations, security posture, and compliance efforts. These reports should be available through automated generation or on-demand requests, with clear visualization of key metrics.

### 11.1 Types of Reports

### 11.1.1 Incident Management Reports

* **Incident Summary Report**: A high-level report summarizing all incidents (security breaches, network issues, hardware failures, etc.) during a specified period. This report should include:
  + Number of incidents by severity (critical, high, medium, low)
  + Incident resolution times (average, by severity)
  + Incident response times (average, by severity)
  + Incident escalation rates
  + Root cause analysis summary
* **Incident Details Report**: A detailed report for each incident, including:
  + Incident type and description
  + Affected systems or services
  + Resolution steps taken
  + Incident resolution time
  + Lessons learned and preventive measures
* **Incident Response Times Report**: This report should analyze the time taken to detect, respond to, and resolve incidents, comparing it against predefined SLA targets.

### 11.1.2 Performance and Availability Reports

* **Network Performance Report**: A report detailing the performance of the network, including:
  + Bandwidth utilization
  + Latency and packet loss
  + Network device uptime and availability
  + Traffic flow analysis
* **Server Performance Report**: This includes performance metrics for physical and virtual servers, such as:
  + CPU and memory usage
  + Disk space utilization
  + Load balancing efficiency
  + System uptime
* **Service Availability Report**: A report showing the availability of critical systems and services, highlighting any downtime incidents or service interruptions.
* **Capacity Utilization Report**: A report assessing current capacity against the forecasted capacity needs. It should include:
  + Current and forecasted resource consumption (network, server, storage)
  + Trends and patterns of usage
  + Resource planning and optimization suggestions

### 11.1.3 Security and Compliance Reports

* **Security Events and Alerts Report**: A detailed report that includes:
  + Number of security events detected (based on SIEM data)
  + Severity and type of each event (e.g., intrusion attempts, malware detection)
  + Response actions taken and remediation details
  + Historical trend analysis of security events
* **Compliance Audit Report**: This report will include:
  + Compliance status with regulatory frameworks such as ISO 27001, GDPR, HIPAA, etc.
  + Results of any internal or external audits
  + Actionable items for maintaining or improving compliance
  + Timeline for compliance remediation and improvements
* **Vulnerability and Patch Management Report**: This report will track the current vulnerability status across the infrastructure, including:
  + Vulnerabilities identified (CVEs)
  + Patching status and remediation
  + Criticality and impact assessment
  + Historical vulnerability trends
* **Threat Intelligence Report**: A comprehensive report that analyzes threat intelligence feeds and correlates them with LRC’s security posture. It should include:
  + New and emerging threats relevant to LRC
  + Correlation between global threat intelligence and internal security events
  + Recommendations for proactive defense actions

### 11.1.4 Disaster Recovery and Business Continuity Reports

* **Disaster Recovery Test Report**: A report detailing the results of disaster recovery drills and tests, including:
  + Time to restore services (RTO)
  + Data recovery success (RPO)
  + Issues encountered during recovery tests
  + Suggested improvements for faster recovery in actual disaster situations
* **Backup and Restore Report**: A report on the backup status of critical systems, including:
  + Backup success rates
  + Frequency and scope of backups
  + Data integrity check results
  + Time taken to restore systems and data from backups

### 11.1.5 Environmental and Infrastructure Reports

* **Temperature and Environmental Monitoring Report**: A detailed report on the status of temperature sensors, humidity levels, and other environmental factors affecting critical infrastructure. This report should include:
  + Any deviations from the acceptable environmental thresholds
  + Notifications triggered by environmental sensor anomalies
  + Historical data and trends on environmental conditions
* **UPS Monitoring Report**: A report on the status of Uninterruptible Power Supply (UPS) systems, including:
  + Battery health and status
  + Power consumption and load balancing
  + Failures, anomalies, or alerts related to UPS performance
* **Asset and Configuration Management Report**: This report provides a detailed inventory of all hardware and software assets across the LRC infrastructure, including:
  + Asset health and performance status
  + Configuration compliance checks
  + System upgrades or changes

### 11.2 Types of Dashboards

### 11.2.1 Executive Dashboard

* A high-level view of the most critical performance and security metrics, designed for senior leadership. This dashboard should include:
  + Incident trends (by severity)
  + System uptime and availability
  + Compliance status summary
  + Key performance indicators (KPIs) for network, server, and application performance
  + Current and historical security event data

### 11.2.2 Security Operations Dashboard

* A detailed view for security operations teams, showing real-time data related to the security posture of LRC’s IT infrastructure. This should include:
  + Active security alerts and events
  + Current vulnerability status and patch management
  + Real-time threat analysis and incident management
  + Integrated SIEM data with ongoing investigation status

### 11.2.3 Network Operations Dashboard

* A dashboard for network operations teams providing insights into network performance and availability, including:
  + Real-time network traffic monitoring
  + Device uptime and performance metrics
  + Bandwidth and resource utilization data
  + Latency, packet loss, and network health overview

### 11.2.4 Incident Management Dashboard

* A dashboard that provides real-time updates on active and ongoing incidents, including:
  + Incident classification by severity
  + Time to resolution and SLA adherence
  + Incident escalation and resolution status
  + Root cause analysis and ongoing remediation efforts

### 11.2.5 Disaster Recovery and Business Continuity Dashboard

* A real-time view of LRC’s disaster recovery and business continuity readiness, including:
  + Current status of backup systems
  + Disaster recovery plan execution and test status
  + RTO and RPO compliance for critical systems
  + Data integrity and system restore times

### 11.2.6 Environmental and Infrastructure Monitoring Dashboard

* A dashboard displaying environmental conditions, particularly for temperature-sensitive locations such as blood banks, and UPS monitoring across LRC facilities. This dashboard should include:
  + Temperature and humidity levels across critical sites
  + UPS battery status and power usage
  + Alerts related to environmental anomalies

### Evaluation Criteria and Selection Process

Proposals will be evaluated based on the following:

* **Technical Expertise**: The vendor’s ability to meet LRC’s operational and security needs.
* **Service Flexibility**: Ability to scale services as LRC’s needs evolve.
* **References and Case Studies**: Demonstrated success in managing NOC/SOC services for similar-sized organizations.
* **Cost-Effectiveness**: Transparency in pricing and cost structure, with clear breakdowns.
* **Added Value**: Integration of advanced tools (e.g., SOAR, SIEM, EDR) and ability to provide value-added services such as cybersecurity awareness training and dark web monitoring.

### Instructions for Evaluation:

* **Compliant (Yes)**: The vendor fully meets the requirement as outlined in the RFP. The proposal includes appropriate documentation, evidence, or explanation demonstrating complete compliance.
* **Compliant (No)**: The vendor does not meet the requirement or cannot demonstrate compliance with the specified needs.
* **Page # in Bid**: The vendor should indicate the page number in their proposal where the response to this requirement can be found.
* **Comments**: Evaluators can add any relevant notes here regarding the compliance level or clarification needed for each requirement.

### Evaluation Criteria Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement** | **Compliant (Yes/No/ partially )** | **Page # in Bid** | **Comments** |
| Incident Response and Resolution Times | | | |
| **Uptime and Availability** | | | |
| The system must guarantee 99.9% uptime for critical services. |  |  |  |
| System monitoring includes redundancy with automatic failover mechanisms to ensure continuous availability. |  |  |  |
| Monthly performance reports on uptime, downtime incidents, and corrective measures. |  |  |  |
| **Incident Response and Resolution Times** | | | |
| Scheduled tests are performed at least every 3 months. |  |  |  |
| Reports delivered within 10 business days post-testing, including identified risks and mitigation plans. |  |  |  |
| Critical vulnerabilities addressed within 25 days of identification, with penalties for delays in resolution. |  |  |  |
| The system must detect critical incidents (e.g., security breaches, service outages) within 5 minutes of occurrence. |  |  |  |
| Acknowledgment of critical incidents within 15 minutes of detection. |  |  |  |
| High Priority Incidents (e.g., cybersecurity breach, critical network downtime): Resolution or mitigation within 2 hours. |  |  |  |
| Medium Priority Incidents (e.g., non-critical system performance issues): Resolution or mitigation within 6 hours. |  |  |  |
| Low Priority Incidents (e.g., minor issues with no immediate impact on operations): Resolution within 24 hours. |  |  |  |
| **Security Features and Compliance** | | | |
| Robust incident management with defined detection, escalation, and resolution workflows. |  |  |  |
| Integration with Security Information and Event Management (SIEM) for real-time threat detection. |  |  |  |
| Regular vulnerability assessments and automated reporting of risks. |  |  |  |
| Full compliance with ISO 27001, GDPR, HIPAA, and NIST standards. |  |  |  |
| **Monitoring Features** | | | |
| 24/7 monitoring of all network devices, servers, and telecommunication systems. |  |  |  |
| Configurable alerts for performance, security, and environmental anomalies. |  |  |  |
| Tool to assist experts in identifying the root cause of incidents (manual intervention required). |  |  |  |
| Support for monitoring multiple LRC sites, including remote offices and field locations. |  |  |  |
| **Scalability and Future Expansion** | | | |
| Ability to scale the platform to accommodate growth in sites, users, and infrastructure. |  |  |  |
| Capability to integrate with emerging technologies and future system upgrades. |  |  |  |
| **Disaster Recovery and Business Continuity** | | | |
| Development of comprehensive disaster recovery plans (DRP) with regular testing. |  |  |  |
| Ongoing maintenance and testing of BCP to ensure uninterrupted critical operations. |  |  |  |
| Recovery Point Objective (RPO): 1 hour. |  |  |  |
| Recovery Time Objective (RTO): 4 hours. |  |  |  |
| **Vendor Experience and Certifications** | | | |
| Proven experience with NGOs or humanitarian organizations of similar size. |  |  |  |
| Vendor holds ISO 27001, GDPR, and other relevant certifications. |  |  |  |
| **Reporting and Analytics** | | | |
| Monthly incident management, performance, and compliance reports. |  |  |  |
| Role-based dashboards for real-time monitoring and analytics. |  |  |  |

## Evaluation Methodology

|  |  |
| --- | --- |
| **Evaluation Criteria** | **Description** |
| **Technical Expertise and Solution Fit** | Assessment of the vendor's technical capabilities, proposed solution alignment with LRC’s needs, and technical approach. This includes platform compatibility, scalability, and overall solution architecture. |
| **Vendor Experience and Qualifications** | Evaluation of the vendor’s experience in providing similar services, especially in the NGO and humanitarian sectors. This includes references, certifications (e.g., ISO 27001), and staff expertise. |
| **Service Level Agreement (SLA) Compliance** | Evaluation of the proposed SLA, including uptime, incident response times, and adherence to critical SLAs for network and security operations. |
| **Security Features and Compliance** | Assessment of the vendor’s cybersecurity measures, including incident management, security event monitoring, SIEM integration, vulnerability management, regular penetration testing, and compliance with industry standards (ISO 27001, GDPR, etc.)." |
| **Platform Capabilities and Monitoring Features** | Evaluation of the monitoring platform’s features such as real-time monitoring, alerting, incident tracking, scalability, automated remediation, and integration with other systems. |
| **Support and Maintenance Services** | Evaluation of the vendor’s proposed support structure, including 24/7 availability, responsiveness, escalation procedures, and the qualifications of support staff. |
| **Cost and Value for Money** | Assessment of the total cost of the proposal, including long-term financial viability, scalability options, and cost-effectiveness in comparison to the value provided. |
| **Innovation and Use of New Technologies** | Assessment of the vendor’s ability to integrate and leverage emerging technologies like Artificial Intelligence (AI), Advanced Endpoint Behavior Analytics (AEBA), machine learning, and automation to improve security, efficiency, and system intelligence. |