**Project Requirements Document**

**1. Project Overview** Contoso, Ltd. is seeking to enhance its cybersecurity infrastructure with a comprehensive **Managed Security Services (MSS) solution**. The goal of this project is to implement a robust security framework that ensures **data protection, threat monitoring, and cybersecurity compliance**. The selected vendor will provide a scalable and cost-effective solution that aligns with Contoso's security policies and industry regulations.

**2. Business Need & Objectives**

* Strengthen **cyber threat detection** and mitigation capabilities.
* Ensure **continuous compliance** with industry standards such as **ISO 27001, SOC 2, and NIST**.
* Provide **24/7 monitoring** and rapid incident response.
* Implement **data encryption** and **penetration testing** methodologies.
* Support a seamless integration with Contoso’s existing **cloud infrastructure**.

**3. Scope of Work** The selected provider will deliver the following services:

* **Security Operations Center (SOC) Support**: Real-time monitoring and management.
* **Threat Intelligence & Detection**: Automated detection of security vulnerabilities.
* **Compliance & Risk Management**: Regular audits and adherence to **NIST, ISO, and SOC 2 standards**.
* **Incident Response & Remediation**: Framework for rapid security breach containment and mitigation.
* **Cloud Security Services**: Protection for Contoso’s **Azure-based** infrastructure.
* **Training & Awareness**: Security training for Contoso’s IT teams.

**4. Implementation Timeline**

* **Phase 1 (Month 1-2)**: Security assessment, gap analysis, and planning.
* **Phase 2 (Month 3-5)**: Solution deployment and integration.
* **Phase 3 (Month 6-9)**: Testing, compliance validation, and training.
* **Phase 4 (Ongoing)**: Continuous monitoring, reporting, and support.

**5. Budget & Pricing Considerations**

* Estimated budget: **$1.5M - $2.5M** over a **3-year contract**.
* Flexible **pricing model**: Fixed cost vs. usage-based.
* Volume discounts for extended engagements.
* Additional charges for premium support and advanced security features.

**6. Compliance & Security Standards** The provider must demonstrate adherence to:

* **ISO 27001** (Information Security Management Systems)
* **SOC 2 Type II** (Security, Availability, and Confidentiality)
* **NIST Cybersecurity Framework**
* **GDPR & CCPA Compliance** (if applicable)

**7. Quality Assurance & Performance Metrics**

* **Response Time SLAs**: Threat detection within **15 minutes**, remediation within **4 hours**.
* **Uptime Guarantee**: **99.9%** service availability.
* **Quarterly Security Audits**: Compliance reporting and policy updates.

**8. Vendor Selection Criteria** Proposals will be evaluated based on:

* **Technical Capability & Experience (30%)**: Previous deployments of similar solutions.
* **Pricing & Cost-effectiveness (25%)**: Transparent cost structure and competitive pricing.
* **Quality & Compliance (20%)**: Alignment with industry best practices.
* **Supplier Reputation & References (15%)**: Three references from enterprise clients.
* **Sustainability & Corporate Responsibility (10%)**: Environmentally responsible IT practices.

**9. Required Documentation** Vendors must provide the following:

* Company background and relevant case studies.
* Security architecture and technical specifications.
* Detailed pricing breakdown.
* Implementation and support plan.
* Compliance certifications.

**10. Additional Notes** This document serves as a preliminary guideline to collect necessary information for drafting a formal **Request for Proposal (RFP)**. Stakeholders should review and refine these requirements to align with Contoso’s evolving security needs before finalizing the RFP.