# **Assessment Scope:**

The scope of this engagement outlines a comprehensive, multi-layered Vulnerability Assessment and Penetration Testing (VAPT) program designed to evaluate the security posture of MOPH’s digital infrastructure, applications, and personnel. Covering external and internal assets, web and mobile applications, APIs, ERP systems, network configurations, and user behavior, each activity is tailored to simulate real-world threat scenarios using objective-based methodologies.

The engagement also includes deployment of a centralized Risk Management Platform and supporting services such as product assurance, detection and response validation, and post-assessment clean-up. All components are structured for annual execution over a period of up to three years, ensuring continuous visibility, risk tracking, and improvement across the enterprise environment.

| **Assessment Stage** | **Activity** | **Scope and Methodology** |
| --- | --- | --- |
| **STAGE 1 (ONSITE)** | **External Penetration Testing (Black Box) - 700 Public IPs** | **External Penetration Testing**  Cytomate will perform annual black-box penetration testing on up to **700 public-facing IPs**, targeting all internet-exposed services and infrastructure. The engagement will follow an objective-based methodology focused on identifying and validating real-world threats such as authentication bypass, data exposure, injection flaws, privilege escalation, and data exfiltration. Each activity will be mapped to defined test objectives, with detailed documentation of attempted attack paths, techniques, and outcomes.  Testing will combine automated reconnaissance with manual exploitation to uncover exploitable vulnerabilities and misconfigurations, using advanced tactics where necessary to simulate sophisticated threat actors. All findings will be thoroughly validated, risk-ranked, and aligned with business impact.  In parallel, Cytomate will support the deployment and integration of a centralized **Risk Operations Center (ROC)** platform to consolidate vulnerability data, testing activities, remediation tracking, and compliance reporting. The platform will integrate with existing scanners, asset inventories, and ticketing systems to provide a unified view of enterprise risk. |
| **STAGE 2 (ONSITE)** | **Internal Penetration Testing (Grey Box) - 3000 Internal IPs including Active Directory, Azure AD, Microsoft Exchange/O365, IIS/Apache, SQL, ERP, File Services, NAC/Endpoint Security Bypass, IAM/PAM** | **Internal Penetration Testing**  Cytomate will conduct annual internal penetration testing across up to **3,000 internal IPs**, covering core infrastructure components including Active Directory, Azure AD, Microsoft Exchange/O365, IIS/Apache, SQL databases, ERP systems, file services, IAM/PAM solutions, and endpoint security controls. The objective is to identify internal misconfigurations, lateral movement paths, privilege escalation vectors, and domain takeover scenarios through a structured, objective-based approach.  Testing will simulate insider threats and compromised user scenarios using a combination of automated enumeration and manual exploitation techniques. Activities will be aligned with defined objectives such as authentication bypass, privilege abuse, and data exfiltration, with each attack path documented in detail to assess impact and risk.  All validated findings will be risk-ranked and mapped to business impact, with detailed reporting of methodologies and outcomes. Additionally, Cytomate will support the integration of a centralized **Risk Operations Center (ROC)** platform within three months to consolidate internal testing data, remediation tracking, and compliance reporting, with real-time integration into existing scanners, asset inventories, and ticketing systems. |
| **STAGE 3 (ONSITE)** | **Wi-Fi Security Testing (Black Box) - 7 SSIDs (Head Office)** | **Wi-Fi Security Testing**  Cytomate will conduct annual Wi-Fi security assessments across **seven SSIDs** at the MOPH’s head office, focusing on evaluating wireless infrastructure for encryption strength, rogue access points, unauthorized access attempts, and misconfigurations. The testing will simulate real-world attack scenarios to assess the effectiveness of wireless security controls, including attempts to bypass network access restrictions and exploit weak authentication mechanisms.  The engagement will include active and passive reconnaissance and controlled exploitation techniques to identify vulnerabilities that could lead to unauthorized access or data leakage. All findings will be validated, risk-ranked, and documented with detailed descriptions of attack methods and outcomes.  Identified vulnerabilities will be onboarded to the centralized **Risk Operations Center (ROC)** platform for tracking, remediation, and compliance reporting. Testing will be conducted **once per year**, with all activities aligned to minimize disruption to business operations. |
| **STAGE 4 (ONSITE)** | **External Web Application Security Assessment (Black Box) - 100 External Web Apps** | **External Web Application Security Assessment**  Cytomate will perform annual security assessments on up to **100 external-facing web applications**, using a combination of manual and automated techniques to identify vulnerabilities aligned with the **OWASP Top 10** and business logic flaws. The assessment will simulate real-world attack scenarios, including website scraping, defacement attempts, and exploitation of authentication, session management, and input validation weaknesses.  Each application will be tested against defined objectives, with detailed documentation of attack paths, methodologies, and outcomes to assess security posture and potential impact. Findings will be validated, risk-ranked, and mapped to business risk, with all vulnerabilities onboarded to the centralized **Risk Operations Center (ROC)** platform for tracking, remediation, and compliance reporting. Structured vulnerability data will also be provided in Excel format with parsing support for seamless integration.  Testing will be conducted **once per year**, ensuring minimal disruption to operations while maintaining continuous visibility into application-layer risks. |
| **STAGE 5 (ONSITE)** | **API Security Assessment (Black Box) - Publicly Exposed APIs** | **API Security Assessment**  Cytomate will conduct annual black-box security assessments of publicly exposed APIs to identify misconfigurations, insecure endpoints, and logic flaws. The engagement will focus on uncovering vulnerabilities related to access control, data exposure, and improper input handling, with in-depth testing aligned to the **OWASP API Security Top 10** and business logic abuse scenarios.  Testing will simulate real-world attack patterns to evaluate how APIs handle authentication, authorization, and data processing under adversarial conditions. Each vulnerability will be validated and mapped to its corresponding test objective, with detailed documentation of attack vectors, techniques, and outcomes.  All confirmed findings will be onboarded to the centralized **Risk Operations Center (ROC)** platform for tracking, remediation, and compliance reporting. Structured vulnerability data will also be provided in Excel format with parsing support. Testing will be conducted **once per year for up to three years**, ensuring continuous visibility into API-layer risks. |
| **STAGE 6 (ONSITE)** | **ERP Security Assessment 2 ERP Applications** | **ERP Security Assessment**  Cytomate will conduct annual in-depth security assessments of two ERP applications, focusing on identifying vulnerabilities that could compromise the confidentiality, integrity, or availability of critical business processes. The assessment will evaluate ERP-specific security controls, including user access management, segregation of duties, authorization mechanisms, and configuration weaknesses.  Testing will follow an objective-based approach, combining automated analysis with manual techniques to uncover exploitable flaws and misconfigurations. Each finding will be validated, risk-ranked, and mapped to its corresponding test objective, with detailed documentation of attack paths and outcomes.  All confirmed vulnerabilities will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking, remediation, and compliance reporting. Structured outputs will also be provided in Excel format with parsing support. Testing will be conducted once per year for up to three years, ensuring continuous visibility into ERP-layer risks. |
| **STAGE 7 (ONSITE)** | **Internal Web Application Security Assessment 10 Internal Applications** | **Internal Web Application Security Assessment**  Cytomate will conduct annual security assessments on up to 10 internal web applications, focusing on portals and custom services critical to internal operations. The engagement will simulate real-world attack scenarios, including website scraping, defacement attempts, and exploitation of business logic flaws, access control weaknesses, and input validation issues.  Testing will follow an objective-based methodology aligned with OWASP standards, combining automated scanning with manual techniques to uncover exploitable vulnerabilities and misconfigurations. Each finding will be validated, risk-ranked, and documented with detailed descriptions of attack paths and outcomes.  All confirmed vulnerabilities will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and remediation, with structured outputs provided in Excel format to support parsing and integration. Testing will be conducted once per year, ensuring continuous visibility into internal application-layer risks. |
| **STAGE 8 (ONSITE)** | **Mobile Application Security Testing (3 Mobile Apps)** | **Mobile Application Security Testing**  Cytomate will conduct annual security assessments on up to three mobile applications across Android and iOS platforms. The engagement will focus on identifying vulnerabilities in mobile-specific components such as insecure data storage, API communications, reverse engineering exposure, and runtime manipulation risks. Testing will follow an objective-based methodology aligned with OWASP Mobile Security standards, simulating real-world attack scenarios to evaluate authentication, session handling, and access control mechanisms.  Each vulnerability will be validated, risk-ranked, and mapped to its corresponding test objective, with detailed documentation of attack paths and outcomes. All confirmed findings will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and remediation, with structured outputs provided in Excel format to support parsing and integration. Testing will be conducted once per year for up to three years, ensuring continuous visibility into mobile application security posture. |
| **STAGE 9 (ONSITE)** | **Configuration Review & System Hardening (Sample of up to 100 IPs from: - Microsoft/Linux Servers - Databases - Security/Netwo rk Devices - SIEM/SOAR, AD , azure cloud the list is not exhausted)** | **Configuration Review & System Hardening**  Cytomate will perform annual configuration reviews and system hardening assessments on a sample of up to 100 internal IPs, covering Microsoft and Linux servers, databases, network and security devices, SIEM/SOAR platforms, Active Directory, and Azure Cloud environments. The engagement will focus on identifying misconfigurations, unnecessary services, and deviations from industry-standard hardening benchmarks such as CIS and NIST.  Each system will be evaluated against defined security baselines to detect exploitable weaknesses that could impact operational integrity or expose sensitive assets. Findings will be validated, risk-ranked, and mapped to business impact, with detailed documentation of configuration gaps and recommended remediation steps.  All confirmed issues will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and compliance reporting, with structured outputs provided in Excel format to support parsing and integration. Testing will be conducted once per year for up to three years, ensuring continuous improvement of infrastructure security posture. |
| **STAGE 10 (ONSITE)** | **VoIP Security Assessment (1 VoIP Network)** | **VoIP Security Assessment**  Cytomate will conduct annual security assessments of the client’s VoIP network, focusing on protocol-level vulnerabilities across SIP, RTP, and related components. The engagement will simulate real-world attack scenarios to evaluate risks such as call spoofing, eavesdropping, unauthorized device registration, and misconfigurations that could compromise voice communication integrity and confidentiality.  Testing will follow an objective-based methodology, combining passive analysis and active exploitation techniques to uncover exploitable flaws. Each finding will be validated, risk-ranked, and documented with detailed descriptions of attack paths and outcomes.  All confirmed vulnerabilities will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and remediation, with structured outputs provided in Excel format to support parsing and integration. Testing will be conducted once per year for up to three years, ensuring ongoing visibility into VoIP infrastructure risks. |
| **STAGE 11 (ONSITE)** | **Advanced Social Engineering Assessment (2000 Staff incl. Vendors technology vetting)** | **Advanced Social Engineering Assessment**  Cytomate will conduct annual advanced social engineering assessments targeting up to 2,000 staff members, including vendors and privileged users. The engagement will simulate realistic attack scenarios such as phishing, baiting, USB drops, and remote exploitation attempts, with a specific focus on IT and application administrators. No whitelisting will be requested, ensuring an authentic threat simulation aligned with real-world adversarial tactics.  The assessment will follow an objective-based approach to evaluate user awareness, response behavior, and susceptibility to manipulation. All successful exploitation paths and behavioral patterns will be documented, risk-ranked, and mapped to business impact.  Confirmed findings will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and remediation, with structured outputs provided in Excel format to support parsing and integration. Testing will be conducted once per year for up to three years, supporting continuous improvement in human-centric security controls. |
| **STAGE 12 (ONSITE)** | **Source Code Review 10 Applications (max 1.5M LoC)** | **Source Code Review**  Cytomate will conduct annual source code reviews for up to 10 applications, with a cumulative limit of 1.5 million lines of code (LoC). The assessment will include both static code analysis and manual review to identify logic flaws, insecure coding practices, and vulnerabilities that may impact application security. Special focus will be placed on authentication, input validation, access control, and error handling mechanisms.  The review will follow an objective-based methodology, mapping each identified issue to its corresponding security control failure. All findings will be validated, risk-ranked, and documented with detailed descriptions of code-level weaknesses and remediation guidance. Developer workshops will be conducted to discuss remediation strategies and promote secure coding practices.  All confirmed vulnerabilities will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and compliance reporting. Structured outputs will be provided in Excel format with parsing support, and SAST/DAST tools will be installed and operated on MOPH-provisioned laptops. Testing will be conducted once per year for up to three years, ensuring continuous improvement in code security posture. |
| **STAGE 13 (ONSITE)** | **Product Security Assurance Service Up to 2 Security Products (EDR, Proxy, etc.)** | **Product Security Assurance Service**  Cytomate will conduct annual independent security assurance assessments for up to two security products (e.g., EDR, Proxy), evaluating their detection and prevention capabilities against mapped MITRE ATT&CK tactics and techniques. This engagement is distinct from penetration testing and focuses solely on validating product effectiveness through controlled simulations of adversarial behavior.  Sensors will be deployed across all endpoints to monitor product response during attack emulation. The assessment will include onboarding to the centralized Risk Operations Center (ROC) platform, integration support, and training sessions for internal teams to ensure operational readiness and knowledge transfer.  Testing will be conducted once per year, ensuring continuous benchmarking of product performance and alignment with evolving threat landscapes. |
| **STAGE 14 (ONSITE)** | **Clean Up (All)** | **Clean-Up**  Cytomate will perform a comprehensive clean-up after each VAPT cycle, ensuring all temporary files, test artifacts, and simulated attack traces are removed from target systems and environments. This includes restoring configurations altered during testing, validating system stability, and confirming that no residual impact remains post-assessment. Clean-up activities will be documented in the final completion report, along with evidence of remediation and system integrity verification.  All findings and remediation actions will be onboarded to the centralized Risk Operations Center (ROC) platform for tracking and compliance reporting. Testing and clean-up will be conducted once per year, supporting secure and sustainable VAPT operations. |
| **STAGE 15 (ONSITE)** | **Risk Management Platform (Hosted In House 3000 Assets)** | **Risk Management Platform**  Cytomate will deploy and operationalize an in-house hosted Risk Management Platform to manage up to 3,000 assets, enabling real-time tracking, prioritization, and lifecycle management of identified vulnerabilities. The platform will integrate with existing vulnerability scanners, asset inventories, ticketing systems, and threat intelligence feeds to provide a unified console for enterprise risk visibility.  The solution will support secure onboarding of penetration testing activities, including project scoping, consultant collaboration, task assignment, and remediation tracking. It will also facilitate identification of externally exposed APIs, misconfigurations, and loopholes that may lead to data exposure or compromise of confidentiality, integrity, or availability.  Dashboards and reporting features will be provided for SLA monitoring, compliance tracking, and executive summaries. The platform will enable seamless collaboration between internal teams and external consultants through a secure portal and will be certified under the Qatar Common Criteria Scheme. Deployment and integration will be conducted once per year for up to three years, ensuring continuous improvement in risk governance. |
| **STAGE 16 (ONSITE)** | **Detection and Response (Hosted In House)** | **Detection and Response**  Cytomate will conduct an annual Red Team exercise to evaluate the effectiveness of in-house security monitoring solutions, such as SIEM platforms. The engagement will simulate advanced adversarial tactics across multiple attack stages, aligned with MITRE ATT&CK techniques, to assess detection coverage, alert fidelity, and incident response capabilities.  The exercise will be designed to replicate real-world threat behavior without prior notification, enabling a realistic evaluation of monitoring, correlation, and escalation workflows. Findings will be documented with detailed mappings to detection gaps and response delays, supporting continuous improvement of threat detection and operational readiness.  Testing will be conducted once per year, ensuring the organization’s detection and response posture remains aligned with evolving threat landscapes. |