Terms of Reference

1 BACKGROUND

ESM develops and maintains software across approximately 30 application portfolios held in Azure DevOps, and requires a cloud-hosted platform that automatically analyses that source code for defects and security vulnerabilities and enforces a centrally governed quality standard at the point of code review, so that changes falling short of that standard cannot be merged. In this context, ESM needs to procure the services laid out below.

1.1 Definitions and abbreviations

Every term, abbreviation and product name used in these Terms of Reference is listed below and has the meaning given to it here wherever it appears.

Term	Explanation
Acceptance	The ESM's acceptance of a Deliverable, on the criteria set out in section 2.
Acceptance Certificate	The written certificate by which the ESM records Acceptance, in the form annexed to the Contract.
AES	Advanced Encryption Standard, a symmetric encryption algorithm. AES-256 denotes the 256-bit key variant.
AI	Artificial intelligence.
Angular	A web application framework. ESM's frontend applications are built with it.
API	Application programming interface: a defined interface through which one system consumes another.
Azure DevOps	Azure DevOps Services, the cloud-hosted edition, as operated by ESM. Holds ESM's source repositories.
Azure Pipelines	The continuous integration and delivery component of Azure DevOps.
Azure Resource Manager	The Microsoft Azure deployment and management service. Its templates describe infrastructure declaratively.
Bicep	A declarative language for deploying Azure resources; an alternative syntax for Azure Resource Manager templates.
Candidate	An economic operator submitting an offer in response to this tender. The Candidate to whom the Contract is awarded becomes the Service Provider.
CEF	Common Event Format, a log interchange format.
CET	Central European Time.
CI/CD	Continuous integration and continuous delivery: the automated build, test and release process.
CISA	The United States Cybersecurity and Infrastructure Security Agency.
CLI	Command line interface.

Cobertura	A test coverage reporting format.
Conditional Access	The Microsoft Entra ID policy engine controlling the conditions under which sign-in is permitted.
Contract	The contract or framework agreement concluded between the ESM and the Service Provider, as defined in section 1.
coverage.py	A test coverage reporting format for Python.
CQ-…	Requirement identifiers. The three-letter code names the subsection — for example CQ-LNG language coverage, CQ-SEC security analysis, CQ-GOV governance. Identifiers are reproduced verbatim in responses, per CQ-SUB-002.
CSS	Cascading Style Sheets.
CSV	Comma-separated values, a tabular text format.
CVE	Common Vulnerabilities and Exposures, the public catalogue of disclosed vulnerabilities.
CVSS	Common Vulnerability Scoring System, a severity scoring scheme for vulnerabilities.
CWE	Common Weakness Enumeration, a catalogue of software weakness types.
CycloneDX	A software bill of materials format.
DAST	Dynamic application security testing: testing an application while it runs. Out of scope — see CQ-W-001.
Deliverables	The items the Service Provider is required to deliver, listed in Table A in section 2.
Delivery Dates	The dates by which Deliverables are due, stated in Table A in section 2.
Docker, Dockerfile	A container platform, and the file describing how a container image is built.
DPA	Data processing agreement.
EMU	Enterprise Managed Users: the GitHub account model in which user accounts are provisioned and controlled by the enterprise.
EU/EEA	The European Union and the European Economic Area.
FC, CC, CE, CD, CR, PC, NC, N/A	The compliance statements a Candidate uses to respond to each requirement, defined at X.2.2.
Finding	Any defect, weakness or violation reported by the Platform. Equivalent vendor terms are listed at X.2.3.
FQDN	Fully qualified domain name.
Framework Agreement	Where the ESM concludes a framework agreement rather than a single contract, that agreement. See section 1.
GA	General availability: a capability released for production use and covered by the standard support terms.
GDPR	The General Data Protection Regulation.
GitHub, GitHub Enterprise Cloud, GitHub Actions	A source repository platform, its enterprise cloud edition, and its continuous integration component. Relevant only to the forward-compatibility requirements CQ-INT-013 to CQ-INT-016.

Go	A programming language. Anticipated future use at ESM.
HCL	HashiCorp Configuration Language, the language in which Terraform definitions are written.
HTML	HyperText Markup Language.
HTTPS	HyperText Transfer Protocol Secure.
IDE	Integrated development environment: the application in which a developer writes code.
Incumbent Platform	The static analysis service ESM operates at the date of this tender, described at X.1.4.
IP	Internet protocol. An IP range is a block of network addresses.
ISO/IEC	The International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27001 is the information security management standard.
Istanbul	A test coverage reporting format for JavaScript and TypeScript.
JaCoCo	A test coverage reporting format for Java.
Java	A programming language. ESM's primary backend language.
JavaScript	A programming language.
JetBrains	A family of integrated development environments.
JSON	JavaScript Object Notation, a structured data format.
KEV	The Known Exploited Vulnerabilities catalogue published by CISA.
KPI	Key performance indicator. Those applying to this Contract are in section 4.
LCOV	A test coverage reporting format.
LOC	Lines of code.
LTS	Long-term support: a release designated for extended maintenance.
M, S, C, W	Requirement priorities under the MoSCoW convention, defined at X.2.1.
M1 to M7	The implementation milestones set out in section 2.
Markdown	A lightweight plain-text formatting syntax.
MATLAB	A numerical computing language. Deliberately excluded from the scope of this tender.
Maven	The build and dependency management tool, and package ecosystem, for Java.
MCP	Model Context Protocol, an interface by which AI coding agents consume external tools and data.
Microsoft Entra ID	Microsoft's cloud identity provider, formerly Azure Active Directory. ESM's Azure DevOps organization is federated to it.
Microsoft Power BI	Microsoft's business intelligence and reporting tool. ESM builds its own reporting with it.
Microsoft Sentinel	Microsoft's security information and event management service.
Microsoft Word	Microsoft's word-processing application and its document formats.
MoSCoW	The Must, Should, Could and Won't have prioritisation convention, defined at X.2.1.

New code	Code added or changed since the baseline defined at CQ-GOV-003.
npm	The package manager and ecosystem for JavaScript and TypeScript.
NuGet	The package manager and ecosystem for .NET.
OAuth	An authorization delegation protocol. OAuth 2.0 is the current version.
OIDC, OpenID Connect	An identity layer built on OAuth 2.0.
OWASP	The Open Worldwide Application Security Project. The OWASP Top 10 lists the most critical web application security risks.
PDF	Portable Document Format.
Platform	The code quality and code security analysis platform to be provided under the Contract.
Portfolio	An Azure DevOps team project grouping related repositories. ESM operates approximately 30.
PowerShell, PowerShell Gallery	A scripting language used by ESM for automation, and its package ecosystem.
PR	Pull request. Used in this abbreviated form only in the vendor-terminology table at X.2.3.
Pull request	A proposed change to a repository, submitted for review before it is merged.
PyPI	The package manager and ecosystem for Python.
Python	A programming language. Used by ESM for backend services and data processing.
Quality policy	The set of conditions the Platform evaluates to produce a pass or fail result. Equivalent vendor terms are listed at X.2.3.
R	A statistical computing language. Deliberately excluded from the scope of this tender.
RASP	Runtime application self-protection. Out of scope — see CQ-W-002.
Receiving Function	The ESM department to which the Service Provider reports, named in section 5.
REST	Representational state transfer, an architectural style for web APIs.
RPO	Recovery point objective: the maximum data loss, measured in time, acceptable after an incident.
RTO	Recovery time objective: the maximum time to restore service after an incident.
Rust	A programming language. Anticipated future use at ESM.
S1 to S4	Support incident severities, defined in Table 3 in section 4.
SAML	Security Assertion Markup Language, a federated authentication protocol.
SAST	Static application security testing: analysing source code for security weakness without executing it.
SBOM	Software bill of materials: a machine-readable inventory of the components in a piece of software.
SCA	Software composition analysis: identifying third-party dependencies and their known vulnerabilities.

SCIM	System for Cross-domain Identity Management, a protocol for automated user provisioning and de-provisioning.
SCSS, SASS	Preprocessor dialects of CSS.
Service Provider	The Candidate to whom the Contract is awarded, as defined in section 1.
Services	The services the Service Provider performs under the Contract, described in section 2.
SKU	A distinct commercial product code; used here to mean a separately priced product variant.
SLA	Service level agreement. That applying to this Contract is in section 4.
SOC 2	Service Organization Control 2, an attestation of a service organisation's controls. Type II covers operating effectiveness over a period.
SPDX	A software bill of materials format.
Spring Boot	A Java application framework used by ESM.
SSO	Single sign-on.
Syslog	A standard for message logging.
T0	The effective date of the Contract.
Terraform	HashiCorp's tool for managing infrastructure declaratively as code. ESM manages its infrastructure with it.
TLS	Transport Layer Security, the protocol securing data in transit.
TypeScript	A programming language. ESM's primary frontend language.
URL	Uniform resource locator, a web address.
UTF-8	A character encoding for text.
VEX	Vulnerability Exploitability eXchange, a format for stating whether a vulnerability is exploitable in a given product.
Visual Studio Code	An integrated development environment.
XLSX	The Microsoft Excel workbook format.
XML	Extensible Markup Language.
YAML	A human-readable data serialisation format, used for pipeline and application configuration.
ZIP	A compressed archive format.

1.2 Subject matter of the procurement

ESM seeks a code quality and code security analysis platform: a service that automatically inspects source code held in ESM's Azure DevOps repositories, without executing it, and reports defects in reliability, maintainability, and security. The platform must enforce a centrally governed quality policy at the point of code review, so that changes failing ESM's standards cannot be merged.
The platform is a development-time control. It is **not** a runtime security product, **not** a penetration-testing service, and **not** a replacement for ESM's existing operational monitoring.

1.2.1 Use in the ESM software delivery process

The platform will be embedded at the following points in the delivery lifecycle:

#	Point of use	Purpose
1	**Developer workstation (IDE)**	Surface findings before commit, using the same rules as the server, to avoid late rework.
2	**Pull request**	Analyse the changed code, annotate the pull request inline, and publish a pass/fail status that acts as a blocking Azure DevOps branch policy.
3	**Main-branch build**	Maintain the authoritative quality and security baseline per repository and feed historical trend data.
4	**Portfolio reporting**	Give engineering management and the architecture function an aggregated view of quality, security and technical-debt exposure across all applications.
5	**Programmatic access by AI coding agents**	A fifth, increasingly important use is programmatic access by AI coding agents, which form part of ESM's development toolchain. Agents must be able to retrieve findings and policy status directly so that defects are remediated within the development session rather than after the fact.

1.2.2 Current estate and baseline

Dimension	Figure	Basis
Repositories under analysis	373 (current), ≥ 1000 to be supported	Current incumbent project count; headroom for growth over contract term
Lines of code, as measured by ESM	Just over 1,000,000	Source lines under analysis, excluding third-party dependencies
Lines of code, as counted for licensing today	2,000,000	The entitlement ESM must currently hold. Roughly double the measured figure — see the note below
Application portfolios	Approximately 30	Azure DevOps team projects
Source repository platform	Azure DevOps Services (cloud)	Single organization, federated to Microsoft Entra ID. GitHub Enterprise Cloud must also be supported.
CI/CD platform	Azure Pipelines, self-hosted and managed agents	—
Contributing developers (code authors whose changes are analysed)	75	Drives per-developer or per-LOC licensing metrics
Named platform users (require login to the web interface)	35 currently provisioned	Drives per-seat licensing. Measured from the current platform's organization membership. Includes architects, QA and management readers as well as developers
Read-only / reporting users	50	Not separately provisioned today.

1.2.3 Current state (baseline for comparison)

ESM currently operates a cloud-hosted static analysis service integrated with Azure DevOps. The following characteristics of the current installation are stated as **factual baseline only** and not as a specification to be replicated:

- 373 analysed repositories, all with private visibility; no public exposure.
- A single custom organisation-wide quality policy applied by default to all projects.
- The policy is evaluated predominantly against newly added or changed code rather than the whole codebase, with the baseline set to the previously released version.
- Repository naming mirrors the Azure DevOps structure using the format ({PORTFOLIO}/{repository}).

1.2.4 Objectives

The platform will enable ESM to:

- Prevent defects and vulnerabilities from entering the main branch, enforced automatically rather than by reviewer discipline.
- Apply a consistent, centrally governed standard across all portfolios and all languages.
- Give developers actionable feedback early enough to act on it cheaply.
- Provide management with an evidenced, trended view of code quality and security exposure.
- Operate within EU data-protection constraints applicable to ESM.

2 DESCRIPTION OF THE SERVICES AND DELIVERABLES

2.1 Minimum technical and service requirements for the Platform

2.1.1 Terminology — technology-neutral drafting

The requirements are expressed in technology -neutral, capability-based terms rather than in the terminology of any specific product. This approach ensures that no Candidate is advantaged by ESM's familiarity with the incumbent platform. The neutral terms used in these Terms of Reference shall have the meanings set out below.

Term used in this ToR	**Commonly equivalent vendor terminology**
Quality policy	Quality gate, policy gate, build breaker, threshold profile
Finding	Issue, violation, defect, alert, smell
Maintainability finding	Code smell, technical debt item
Finding requiring manual review	Security hotspot, review item
Incremental analysis / new-code analysis	New code period, delta analysis, differential scan, clean-as-you-code
Rule set	Quality profile, rule pack, policy set, ruleset
Pull request annotation	PR decoration, inline comment, review comment

2.1.2 Mandatory Technical Requirements

Id	**Applicable to**	**Area**	**Description**
001	Platform	Languages	The platform will support all of the following languages / technologies: • Java • Python • Typescript • Javascript • HTML • CSS • XML • PowerShell
002	Platform	Functionality	The Platform will permit ESM to **exclude specified paths, files or generated code** from analysis and from metric calculation, configurable per repository.

003	Platform	Functionality	The Platform will perform **static analysis without executing the code** and without requiring the application to be deployed or running.
004	Platform	Functionality	The Platform will detect and report, as distinct categories: • **reliability defects** (code that is or may be functionally wrong) • **duplicated code** • **security weaknesses**.
005	Platform	Functionality	Every finding will identify the **file, line, and where applicable the code path**, and will carry a human-readable explanation of why it is a defect and how to remediate it.
006	Platform	Functionality	The Platform will **ingest externally produced test coverage reports** in at least one widely used open format per mandatory language (where applicable), and attribute coverage **per file and per line**.
007	Platform	Functionality	The Platform will support **multi-module and monorepo structures**, aggregating multiple build modules within one repository into a single reported result while retaining per-module detail.
008	Platform	Functionality	Analysis will be **deterministic**: the same commit analysed with the same configuration and rule set version will produce the same findings.
009	Platform	Functionality	The Platform will support **suppression of individual findings** with **mandatory justification, attribution to the suppressing user, and an audit trail**.
010	Platform	Security Analysis	The Platform will perform **static application security testing (SAST)** covering the **OWASP Top 10** and **CWE Top 25** for the following executable languages: • **Java** • **Python** • **TypeScript** • **JavaScript**
011	Platform	Security Analysis	Each security finding will be **mapped to a CWE identifier**, and to the relevant OWASP category where applicable.
012	Platform	Security Analysis	The Platform will detect **secrets and credentials** committed to source code: • API keys • Tokens • connection strings • private keys in the current checkout of every analyzed branch.
013	Platform	Security Analysis	The Platform will perform **software composition analysis (SCA)** of third-party dependencies, including **transitive** dependencies, for the ecosystems corresponding to ESM's mandatory languages: • **Maven** (Java), • **npm** (TypeScript/JavaScript) and • **PyPI** (Python).
014	Platform	Security Analysis	Dependency vulnerability data will be drawn from a **maintained vulnerability database updated at least daily**. The Candidate will name its data sources.
015	Platform	Security Analysis	Findings will carry a **severity** assigned per a documented and published scheme, and a **CVSS score** where one applies.

016	Platform	Management	The Platform will support a **centrally defined quality policy** applied by default across all repositories, editable only by explicitly authorized administrators and **not overridable by individual project teams**.
017	Platform	Management	The quality policy will support, at minimum, conditions on the metrics listed #4, with **ESM-configurable thresholds and comparison operators**.
018	Platform	Management	The Platform will support **incremental analysis**: evaluating the policy against only code **added or changed since a configurable baseline**. The baseline will be selectable as at least **the merge base with the target branch**.
019	Platform	Management	The policy result will be exposed as an unambiguous **binary pass/fail** suitable for automated enforcement.
020	Platform	Integration	The Platform will provide **native integration with Azure DevOps Services (cloud) and Github**, including repository discovery and binding.
021	Platform	Integration	The Platform will **annotate Azure DevOps AND Github pull requests**, posting a summary and **inline comments on the specific changed lines** to which findings relate.
022	Platform	Integration	The Platform will operate correctly where the **Azure DevOps / Github organization is federated to Microsoft Entra ID for single sign-on** (OAuth application, Microsoft Entra ID service principal, workload identity federation, managed identity, or personal access token) **not depending on interactive end-user OAuth consent**, which a federated organization may be unable to grant.
023	Platform	Integration	The Platform will publish a **pull request status check** to Azure DevOps / Github that ESM can configure as a **required branch policy blocking pull request completion**.
024	Platform	Integration	The Platform will provide **ready-to-use Azure Pipelines tasks** (via the Visual Studio Marketplace) or a documented command-line interface usable within a container-based pipeline job.
025	Platform	Integration	Analysis will be invocable from **ESM-hosted and Microsoft-managed Azure Pipelines agents requiring outbound HTTPS connectivity only**, with **no inbound connectivity to ESM networks**.
026	Platform	Access Management	The Platform will support **single sign-on interoperable with Microsoft Entra ID** as the sole interactive authentication path for ESM users. ESM is **protocol-agnostic**: SAML 2.0, OpenID Connect, OAuth 2.0, or a native Microsoft Entra ID integration are all acceptable.
027	Platform	Access Management	The Platform will provide **role-based access control** that separates, at minimum, **administration** from **contribution** from **read-only access**, and permits quality policy administration to be restricted independently of general project administration.
028	Platform	Access Management	All ESM repositories and analysis results will be **private by default**.
029	Platform	Hosting	**All ESM data** — source code, analysis results, metadata, logs and backups — will be **stored and processed exclusively within the EU/EEA** in the normal operation of the Platform.
030	Platform	Hosting	Data will be **encrypted in transit** (TLS 1.2 or higher) and **at rest** (AES-256 or equivalent).

031	Platform	Hosting	ESM's data will be **logically isolated** from that of other customers.
032	Platform	Management	The Platform will expose a **complete, documented, versioned administrative API** sufficient to perform: (a) repository onboarding and per-repository settings; (b) quality policy definitions and their assignment to repositories; (c) rule set definitions and assignment; (d) user groups, roles and permission assignments; (e) integration bindings to Azure DevOps / Github
033	Service Provider	Hosting	The Service Provider will hold current **ISO/IEC 27001 certification and/or SOC 2 Type II attestation** covering the Platform.
034	Service Provider	Hosting	The Service Provider will provide a **GDPR-aligned data processing agreement**, a complete **sub-processor list**, and will commit to **breach notification within a stated maximum period**.
035	Service Provider	Hosting	On termination, the Service Provider will **delete all ESM data within a stated period** and provide written confirmation of deletion. Deletion obligations will extend to **backups, caches, replicas, search indexes and log stores**.
036	Service Provider	Maintenance	The Service Provider will maintain **compatibility with Azure DevOps Services and Github** as they evolve and will state its commitment and typical timescale for adapting to changes.

2.1.3 Additional Technical and Service Requirements

Id	**Applicable to**	**Area**	**Description**
101	Platform	Functionality	The Platform will support the following test coverage formats: JaCoCo XML, Cobertura, LCOV, coverage.py, and Istanbul.
102	Platform	Functionality	The Platform will report a **measure of duplicated code** across.
103	Platform	Functionality	ESM will be able to **author custom rules** in addition to the supplied rule set and distribute them centrally.
104	Platform	Functionality	Suppression will **additionally** be possible by annotation in the source code itself, so that the decision travels with the code under version control.
105	Platform	Functionality	Authority to suppress will be **restrictable by role**, so that ESM can require suppressions of security findings above a stated severity to be approved by someone other than the code author.
106	Platform	Security Analysis	The Platform will detect security-relevant weakness in the **configuration and markup languages** XML, YAML, HTML and Terraform/HCL — to the extent meaningful for each (for example insecure deserialization settings, exposed secrets in configuration, unsafe template constructs, permissive infrastructure rules).

Id	Applicable to	Area	Description
107	Platform	Security Analysis	Secret detection will additionally cover **reachable git history**, not only the current checkout, so that a credential committed and later removed is still surfaced
108	Platform	Security Analysis	The Platform will additionally perform SCA for **NuGet** and **PowerShell Gallery**.
109	Platform	Security Analysis	The Platform will provide a **triage workflow** for findings that require human confirmation, recording the reviewer, decision, justification and timestamp.
110	Platform	Security Analysis	The Platform will support **reachability or exploitability analysis** to distinguish dependency vulnerabilities that are actually invoked by ESM code from those that are not.
111	Platform	Security Analysis	The Platform will detect the **open-source licenses** of dependencies and allow ESM to define permitted and prohibited license lists.
112	Platform	Security Analysis	Regardless of the scope granted, the Platform will **never modify existing source code on a protected branch**, will never force-push, and will never delete branches it did not create.
113	Platform	Security Analysis	Every finding will carry **stable lifecycle metadata**: an identifier that persists across analyses and across code movement, first-detected date, age, current state, and the identity of the responsible team or code owner. Findings will not be re-identified as new when surrounding code is reformatted or relocated.
114	Platform	Security Analysis	The Platform will support **remediation deadlines** derived from finding severity — a target date computed and tracked per finding — and will report findings breaching their deadline.
115	Platform	Security Analysis	The platform will provide a maintained **emergency response process for actively exploited vulnerabilities** — for example a CISA KEV listing or a widely exploited zero-day in a common dependency — providing detection content and customer notification faster than the routine update cycle.
116	Platform	Security Analysis	The Platform will consume and/or produce **VEX (Vulnerability Exploitability eXchange)** statements, so that ESM's assessment that a vulnerability is not exploitable in its context can be recorded and carried forward rather than re-triaged each cycle.
117	Platform	Security Analysis	The Platform will flag **malicious, typosquatted, protestware or hijacked packages** in the dependency graph, distinctly from ordinary CVE findings.
118	Platform	Security Analysis	The Platform will provide **agent-based or equivalent deep security analysis** capable of identifying **logic-level vulnerabilities that structural analysis does not detect**, covering at minimum: (a) **broken access control** — insecure direct object references, missing or incorrect authorization checks, privilege escalation; (b) **business logic flaws** — skippable workflow steps, repeatable actions that should be idempotent, absent rate limiting; (c) **authentication and session management flaws** —

Id	Applicable to	Area	Description
			session fixation, non-expiring sessions, absent brute-force protection. Each such finding will carry an **auditable reasoning trace** — the path by which the conclusion was reached, including the code locations examined — sufficient for an ESM engineer to verify or refute the finding without re-deriving the analysis.
~~119~~	~~Platform~~	~~Security Analysis~~	
120	Platform	Security Analysis	Results will be **reproducible**: the same commit, analysed with the same configuration and version, will yield materially the same findings. The Candidate will state what governs reproducibility and what variance ESM can expect between runs.
121	Platform	Security Analysis	Findings will surface in the **same queue, triage workflow and API** as all other findings, distinguishable by source, rather than requiring a separate console or a parallel process.
122	Platform	Security Analysis	The analysis will be **independently scopeable and schedulable** — runnable against selected repositories, on demand or on a schedule, without being tied to every pull request — so that ESM can control both cost and review load.
123	Platform	Management	The baseline against which an analysis runs will additionally be selectable as **the previously released version** of the software.
124	Platform	Management	The Platform will support **multiple distinct policies**, assignable per repository so that differing standards can apply to (for example) production services versus internal tooling.
125	Platform	Management	All changes to policy definitions and rule sets will be **versioned and audit-logged**, recording actor, change and timestamp, and will be view- and exportable.
126	Platform	Management	Policy and rule-set definitions will be **exportable and importable as text**, so they can be held under version control and promoted between environments. Policy held as code will reside in an **ESM-controlled administrative repository**; the Platform will **not** honour policy overrides placed in the analyzed repositories themselves, which would defeat CQ-GOV-001.
127	Platform	Management	The Platform will allow ESM to **defer or pin rule-set updates**, so that a rule change delivered by the Service Provider does not cause previously passing repositories to fail without ESM's decision.
128	Platform	Management	The Platform's own configuration will be manageable **declaratively as code using HashiCorp Terraform**, covering at minimum: (a) repository onboarding and per-repository settings; (b) quality policy definitions and their assignment to repositories; (c) rule set definitions and assignment; (d) user groups, roles and permission assignments; (e) integration bindings to Azure DevOps / Github.

Id	Applicable to	Area	Description
~~129~~	~~Platform~~		
130	Platform	Management	Configuration applied as code will be **idempotent and drift-detectable**: re-applying an unchanged definition will produce no change, and configuration altered manually through the user interface will be detectable on subsequent reconciliation.
131	Platform	Management	Administrative automation will **not require long-lived administrative credentials to be stored** in ESM's Terraform state or pipeline definitions.
132	Platform	Integration	The Platform will support analysis of **long-lived branches** in addition to pull requests and the main branch.
133	Platform	Integration	The Platform will support **build-less analysis** (analysis from a source checkout without a compilation step) for at least the interpreted and markup languages.
134	Platform	Integration	The Platform will emit **webhooks or equivalent event notifications** on analysis completion and policy status change, to allow ESM to build downstream automation.
135	Platform	Access Management	The Platform will allow ESM to **disable all local and platform-native password authentication organization-wide**, so that federated sign-on is the only interactive route in.
136	Platform	Access Management	The Platform will **map identity provider group membership to platform roles** — via SAML attributes, OpenID Connect claims, Microsoft Entra ID group claims, or SCIM — so that access is governed by existing corporate group management rather than platform-local administration.
137	Platform	Access Management	**All interactive sign-in** will be subject to ESM's **Microsoft Entra ID Conditional Access policies**, including device-compliance and location-based conditions. No interactive path will bypass them — including local accounts, legacy authentication endpoints, and long-lived tokens usable in place of interactive login. Non-interactive machine credentials under CQ-IAM-008 are outside this requirement and are governed instead by expiry and revocation.
138	Platform	Access Management	The Platform will support **SCIM 2.0 automated user provisioning and, critically, automated de-provisioning**, so that a leaver removed from Microsoft Entra ID loses platform access without manual action.
139	Platform	Access Management	Roles will be granular enough to distinguish all five of: organization administrator, policy administrator, project administrator, contributor, read-only user.
140	Platform	Access Management	The Platform will maintain an **audit log** of authentication events, permission changes, policy changes and administrative actions, retained for a stated period and **exportable in machine-readable form**.
141	Platform	Access Management	The Platform will support **Microsoft Entra ID managed identities or workload identity federation** for service-to-service authentication, as an alternative to stored secrets.

Id	Applicable to	Area	Description
142	Platform	Access Management	The Platform will support **periodic access review**: producing, on demand or on schedule, a complete report of users, their roles, their group derivation and their last activity date, in a form suitable for attestation by a reviewer.
143	Platform	Access Management	The Platform will **stream or export security and administrative events** — authentication, permission change, policy change, administrative action, token issuance and revocation — in a form ingestible by **Microsoft Sentinel**, whether by native connector, a supported Common Event Format/Syslog output, a webhook, or a documented pull API.
144	Platform	Access Management	Exported events will carry a **stable schema with a documented change policy**, so that an ESM-built collector does not break silently when the Platform is updated.
145	Platform	AI	**ESM source code, analysis findings and platform configuration will not be used to train, fine-tune, retrain or otherwise improve any model operated by the Bidder or by any third party.** This condition will be capable of being made contractually binding.
146	Platform	AI	The platform supports to opt-out of any usage telemetry (feature usage counts, performance data, error reports) that is used for platform or model improvement.
147	Platform	AI	The Platform will provide a **documented, versioned, authenticated REST API** covering at minimum: retrieval of findings, policy status, and metrics; and modification of finding triage state.
148	Platform	AI	The Platform will provide an **interface consumable by AI coding agents** — for example a Model Context Protocol (MCP) server or equivalent documented agent interface— permitting an agent to query findings and policy status within a development session. The Bidder will state whether this interface is **maintained by the Bidder or by the community**.
149	Platform	AI	The Platform will provide **IDE integration** for **Visual Studio Code** and **JetBrains IDEs**, surfacing findings before commit.
150	Platform	AI	IDE analysis will use the **same rule set and rule set version** as server-side analysis, centrally distributed, so that local and pipeline results agree.
151	Platform	AI	The Platform will **automatically generate remediation fixes** for the findings it reports — that is, concrete proposed code changes, not merely textual guidance on how to fix the finding.
152	Platform	AI	Generated fixes will be deliverable through **at least one** of the following: (a) an automatically raised Azure DevOps / Github pull request; (b) a patch applied in the developer's IDE on acceptance; (c) a patch retrievable via API for ESM's own automation.
153	Platform	AI	**Where the Platform generates fixes**, those fixes will **never be committed to a protected branch, nor**

Id	Applicable to	Area	Description
			merged, without explicit human review and approval. Any capability to merge automatically will be capable of being disabled by ESM.
154	Platform	AI	Where a fix is delivered as a commit or pull request, it will be **clearly attributable as machine-generated** in the commit or pull request metadata, so that ESM can identify AI-authored code in its repositories after the fact.
155	Platform	AI	After a generated fix is applied, the Platform will **re-analyze the changed code** and confirm both that the original finding is resolved and that no new finding has been introduced.
156	Platform	AI	A generated fix will not be presented to ESM as ready for review until it has **passed the repository's configured build, its automated tests, and the quality policy** of CQ-GOV-001. Fixes that break the build or fail tests will be withheld or clearly marked as unvalidated.
157	Platform	AI	Automatic fix generation will be **scopeable** — capable of being enabled per repository, per portfolio and per finding category — so that ESM can pilot it narrowly before wider adoption.
158	Platform	AI	**Where fix generation relies on a third-party or hosted large language model**, **name the model provider, the model, and the geographic location of processing**, and will confirm that the prohibition for model training (see above) extends to this prover.
159	Platform	AI	All AI-enabled features, including automatic fix generation, will be **capable of being disabled organization-wide** by an ESM administrator.
160	Platform	AI	The Platform can **identify or attribute AI-generated code** and apply differentiated policy to it.
161	Platform	Reporting	The Platform will provide a **portfolio-level view** aggregating quality and security status across all repositories, with drill-down to portfolio, repository, file and finding.
162	Platform	Reporting	The Platform will retain **historical trend data for at least 24 months**, permitting analysis of quality and security posture over time.
163	Platform	Reporting	The Platform will provide **bulk export of metrics via API**, enabling ESM to build its own reporting, e.g., in Microsoft Power BI.
164	Platform	Reporting	The Platform will provide **exportable reports** in PDF and/or CSV suitable for distribution to management.
165	Platform	Reporting	The Platform will support **user-defined dashboards** combining metrics of ESM's choosing.
166	Platform	Reporting	The Platform will report **security findings in a form suitable for evidencing compliance activity**, filterable by severity, CWE and remediation status.
167	Platform	Performance	The Platform will support **at least 1000 repositories** and **at least 5,000,000 lines of code** under continuous analysis without degradation.

Id	Applicable to	Area	Description
168	Platform	Performance	The Platform will scale to **10,000,000 lines of code** without architectural change or migration to a different deployment model.
169	Platform	Performance	The Platform will sustain **at least 20 concurrent analyses**, bursting to **30**, without queuing.
170	Platform	Performance	**Pull request analysis feedback** will be returned within **10 minutes** for a repository of up to 100,000 lines of code.
171	Platform	Performance	The Platform will achieve a **monthly availability of at least 99.5%**.
172	Platform	Maintenance	**Platform updates, rule set updates and vulnerability database updates will be delivered without requiring action by ESM**, and will be included in the subscription price.
173	Platform	Maintenance	ESM will be able to **defer or pin rule set versions**, so that a rule change delivered by the Service Provider does not cause previously compliant repositories to fail without ESM's decision. Where deferral is not supported, the Bidder will state the **advance notice** given before behavior- changing rule updates.
174	Platform	Maintenance	**Planned maintenance** will be notified at least 5 business days in advance and, where it causes service interruption, scheduled outside 07:00–19:00 CE(S)T on business days.
175	Platform	Maintenance	The Platform will allow ESM to **monitor its consumption against its entitlement**, with warning before an overage threshold is reached.
176	Platform	Migration	ESM will be able to **export all of its data** — findings, triage decisions, metric history, policy definitions and configuration — **on demand, in documented machine-readable formats, at no additional cost**, throughout the contract term.

2.1.4 Service Requirements

Id	Applicable to	Area	Description
201	Service Provider	Functionality	The Service Provider will submit its platform to a **detection-quality benchmark** conducted by ESM on a supplied corpus of ESM-representative code containing seeded defects across **Java, Python, TypeScript and Terraform**, plus unmodified control code. The corpus, the seeded defect classes, the scoring method and the weighting will be published to all Candidates in advance and applied identically to every offer.

202	Service Provider	Security	The Service Provider will commission an **independent penetration test of the Platform at least annually** and make an executive summary available to ESM on request.
203	Service Provider	Hosting	The Service Provider will state **whether ESM source code is transmitted to and retained by the Platform**, or whether only derived metadata is retained. If source code is retained, state for how long, for what purpose, and how it is deleted.
204	Service Provider	Hosting	The Service Provider will confirm whether any **support personnel outside the EU/EEA** can access ESM data or systems, in what circumstances, from which jurisdictions, and under what controls.
205	Service Provider	Hosting	**Support and engineering access** to ESM data from outside the EU/EEA will not occur. Where the Service Provider cannot meet this absolutely, it will describe the **compensating controls** it applies to any non-EU/EEA access: named and vetted individuals, prior ESM approval per access, time-boxed and least-privilege sessions, session recording, and full audit logging available to ESM.
206	Service Provider	Hosting	The Service Provider will state its **routine retention policy for ESM source code and analysis artifacts during the contract** — how long transient copies persist after analysis completes, and whether ESM can configure a shorter retention.
207	Service Provider	Performance	The Service Provider will state **any hard limits** on analyses per day or per month, lines of code analyzed, or API request rates, within the licensed scope.
208	Service Provider	Performance	The Service Provider will operate a **public status page** and provide **proactive notification** of incidents affecting the Platform.
209	Service Provider	Performance	The Service Provider will state its **recovery time objective (RTO)** and **recovery point objective (RPO)** for the Platform.
210	Service Provider	Maintenance	The Service Provider will publish **release notes and a rule set changelog** for every update affecting analysis behavior.
211	Service Provider	Maintenance	The Service Provider will give **advance notice of any breaking change** to APIs, integrations, pipeline tasks or authentication mechanisms. ESM requires at least 90 days; the Bidder will state its committed notice period.
212	Service Provider	Maintenance	Documentation is sufficient for ESM to operate and reconfigure the Platform without the Service Provider's assistance. Administrator enablement has covered the configuration-as-code workflow.
213	Service Provider	Maintenance	The Service Provider will operate a **published deprecation policy** stating the minimum support period for a feature after deprecation is announced.
214	Service Provider	Maintenance	The Service Provider will provide a **product roadmap** covering at least the next 12 months and will state how customers can influence it.

215	Service Provider	Maintenance	The Service Provider will state its policy on **version currency** — whether ESM will always be on the current version, and whether ESM has any ability to defer platform upgrades.
216	Service Provider	Migration	On termination, the Service Provider will provide **read-only or export access for a stated period** to allow ESM to retrieve its data.
217	Service Provider	Migration	The Service Provider will deliver administrator enablement for ESM platform administrators, covering policy configuration, rule set management, access control, troubleshooting, and the declarative configuration-as-code workflow .
218	Service Provider	User support	The Service Provider will provide **technical support in English**, available at minimum during business hours in Central European Time.
219	Service Provider	User support	The Service Provider will operate a **documented severity classification** for support incidents and will commit to **response and resolution targets** per severity.
220	Service Provider	User support	The Service Provider will provide **at least two support channels**, one of which will be a ticketing system providing ESM with visibility of ticket status and history.
221	Service Provider	User support	The Service Provider will provide a **named escalation path** with defined escalation triggers and named contacts at each level.
222	Service Provider	User support	The Bidder will state whether a **named technical account manager or customer success contact** is included, and at what service level.
223	Service Provider	User support	The Service Provider will provide **publicly accessible product documentation** and a searchable knowledge base.
224	Service Provider	User support	Support will be available to **all ESM developers**, not solely to a limited number of nominated administrators. Where a limit applies, the Bidder will state it.
225	Service Provider	User support	The Service Provider will report **support performance against its committed targets** at agreed intervals.

2.2 Out-of-Scope

ID	Item	Priority
301	Dynamic application security testing (DAST) / runtime scanning of deployed applications.	**W**
302	Runtime application self-protection (RASP) or production workload protection.	**W**
303	Penetration testing services.	**W**
304	Container image and registry scanning at runtime (build-time Dockerfile analysis is covered by CQ-LNG-017).	**W**
305	Vulnerability management for infrastructure or endpoints outside the source code estate.	**W**
306	Migration	**W**
307	On-premises or ESM-tenant-hosted deployment. A cloud service hosted by the Service Provider is required.	**W**

3 KEY PERFORMANCE INDICATORS (KPIs)

The Service Provider will perform the Services in accordance with KPIs, provide values for at least the following:

#	KPI	Measurement method	Measurement period
1	**Service availability**	As measured and published by the Service Provider, on a stated basis with stated exclusions	Monthly
2	**Pull request analysis feedback time**	95th percentile elapsed time from analysis trigger to result published, for repositories up to 100,000 lines of code	Monthly
3	**S1 incident response**	Elapsed business hours from ticket raised to substantive response	Per incident, reported monthly
4	**S1 incident resolution or workaround**	Elapsed business days from ticket raised to resolution or accepted workaround	Per incident, reported monthly
5	**S2 incident response**	As KPI 3	Per incident, reported monthly
6	**S2 incident resolution or workaround**	As KPI 4	Per incident, reported monthly
7	**Vulnerability database currency**	Elapsed time from CVE publication to availability in the Platform's vulnerability data	Monthly
8	**Planned maintenance notice**	Advance notice given, and whether interrupting maintenance fell outside 07:00-19:00 CET on business days	Per occurrence
9	**Breaking change notice**	Advance notice given before a breaking change to APIs, integrations, pipeline tasks or authentication	Per occurrence
10	**Reporting**	The Service Provider will report performance against every KPI above at intervals in a format agreed with ESM	Monthly, Quarterly, Yearly

4 ADMINISTRATIVE ARRANGEMENTS (OFFICE SPACE, LAPTOPS ETC.)1

The Services are delivered as a cloud service hosted by the Service Provider; no Service Provider personnel are resident at the ESM's premises in the ordinary course. The Service Provider will report to the IT department. The Receiving Function is authorised to provide guidance, clarifications and instructions, as appropriate, to the Service Provider on the Services and Deliverables that fall under the scope of this Contract where required.
Implementation and enablement activities under section 2 may be delivered remotely, on-site at the ESM's premises in Luxembourg, or as a hybrid.

[1] This section is adapted for consultants but could be adapted further for other arrangements.

The ESM will not provide office space, laptops, administrative support or ESM system access to the Service Provider, save that the ESM will provide such access to its Azure DevOps organization as is strictly required to establish and operate the integration described in section 2, on the permission scopes disclosed under CQ-SEC-011.