

Service Definition – Eurocom CI Screening Service

1. Service overview

Eurocom CI provides an online screening service that enables organisations to request, manage, and receive screening outcomes for candidates as part of recruitment and onboarding processes. The service supports configuration of screening levels per job role and provides secure access to screening progress updates and reports.

Candidates complete required screening steps through Eurocom CI's platform. HR users can monitor progress and access completed screening reports and supporting evidence.

2. Service features and how it works

The service supports the following high-level workflow:

1. Customer administrators configure screening requirements for job roles (screening levels and checks).
2. HR users initiate screening requests for candidates, either directly in the platform or via HR system integration (where configured).
3. Candidates complete screening steps through the Eurocom CI platform.
4. Eurocom CI completes the required checks and generates screening outcomes and reports.
5. Results and reports are made available in the platform and can be returned to the customer's HR system via integration (if enabled).

3. Onboarding support

We support customers to start using the service through an onboarding process that includes:

- an onboarding meeting with customer stakeholders to confirm screening requirements and job roles
- configuration of access for relevant users and setup of role-based screening levels
- online training for users covering how to initiate screenings, monitor progress, and access reports
- customer-specific user documentation made available through our helpdesk platform

4. Offboarding support and data access on exit

Customers can export screening information during the contract. Each completed screening generates an exportable record, including outcomes and associated reports.

At contract end, customers may undertake a full export of historical screening data if required. We confirm completion of any agreed exports before disabling access. Data is retained or securely deleted in line with the customer's retention requirements and contractual obligations. Confirmation of deletion can be provided on request.

5. Data export formats

Screening outcomes and reports are provided in **PDF** format. Supporting documents supplied during screening may be provided in their **original format** (for example JPEG/PNG images or office documents), where applicable.

6. Hosting, locations and deployment model

The service is delivered as a cloud-hosted SaaS solution hosted on **Google Cloud Platform (GCP)**. The service is accessed securely over the internet using modern web browsers.

7. Backup, restore and disaster recovery

We operate automated resilience measures and backup controls to support service continuity. This includes:

- automated incremental backups
- backups stored in a separate data centre environment
- documented restoration processes to support recovery following service disruption

8. Resilience and performance

The service is designed to scale with demand. Infrastructure is configured to autoscale where required and multiple instances can be run to support availability during periods of higher load.

We monitor service health and performance to identify and respond to incidents and ensure users are not adversely impacted by demand from other organisations.

9. Outage and maintenance management

We use monitoring and alerting to detect service degradation or outages. Customers are informed of confirmed outages via agreed communication channels (email and telephone for major incidents where required). Updates are provided until the incident is resolved, and an incident summary can be provided on request.

Planned maintenance is managed through change control processes. Where maintenance may impact service availability, customers are notified in advance where practicable.

10. Service availability and support hours

We aim to provide continuous service availability and operate support during standard office hours: **09:00–17:00 Monday to Friday** (excluding UK public holidays).

Support response and fix targets are:

- **Full service unavailability:** response within 2 working hours; fix within 10 working hours
- **Major functionality unavailability:** response within 5 working hours; fix within 20 working hours
- **Minor functionality issues:** response within 10 working hours; fix within 10 working days

Full service and major issues should be reported by telephone to meet response timelines.

11. Service constraints and customisation

The service can be configured to support customer requirements, including:

- different screening levels for different job roles
- the ability to add or remove checks within a screening package (where applicable)
- customer preferences for candidate communications and reporting format

Customisation is managed through the customer service team or account manager to ensure changes are controlled and auditable. Some changes may be restricted once a screening is in progress to maintain data integrity and compliance.

12. Technical requirements

Customers require:

- a supported modern web browser
- internet connectivity
- an authorised organisational account and configured user access
- for integrations: an agreed integration setup between the customer HR platform and Eurocom CI (where applicable)

Users authenticate with multi-factor authentication (2FA) and must be provisioned by the customer administrator.

13. Security

Security controls include:

- encryption in transit using TLS 1.2+
- encryption at rest provided through Google Cloud encryption mechanisms
- role-based access controls and multi-factor authentication
- defined incident management processes
- change control and vulnerability management processes to address risks and patching
- protective monitoring and alerting to detect abnormal events

Administrative access changes are restricted and verified. Support access is restricted to authorised customer contacts.

14. Penetration testing and vulnerability management

We maintain a vulnerability management process to identify potential threats, apply patches based on risk and severity, and track remediation actions through change management. Vulnerability assessments are completed at least annually, and external testing may be commissioned where appropriate.

15. After-sales support

Ongoing support is provided by our customer service team and account manager (where applicable).

Support includes:

- user support and troubleshooting
- onboarding of additional users
- configuration changes to screening levels and role-based screening packages
- reporting support and export assistance (where applicable)