eurocom ci

T: +44 (0) 1372 886 920
F: +44 (0) 1372 351 219
info@eurocomci.co.uk

Wesley House, Bull Hill,
Leatherhead, Surrey, KT22 7AH

Service Definition – DBS Update Service Checker

1. Service overview

The DBS Update Service Checker is a cloud-based service that enables organisations to monitor the status of Disclosure and Barring Service (DBS) certificates that are registered with the DBS Update Service. The service performs automated daily checks to identify changes to certificate status and provides notifications when new information is identified or when an Update Service subscription expires.
The service supports employers in maintaining ongoing compliance and safeguarding assurance without the need to request repeat DBS checks unless required.

2. How the service works

Customers add DBS certificate details to the platform once the individual has subscribed to the DBS Update Service. The service then performs automated daily status checks against the Update Service.

The platform:

- monitors certificates daily
- identifies status changes or new information
- alerts customers when updates are identified
- notifies customers when Update Service subscriptions expire or are due to expire
- provides dashboard visibility and reporting of all monitored certificates

Results and monitoring history are available through the user interface and exportable for audit purposes.

3. Hosting, deployment and locations

The service is delivered as a Software as a Service (SaaS) solution hosted on Amazon Web Servers (AWS). The service is accessed securely over the internet using a supported modern web browser. No local software installation is required.

4. Backup, restore and disaster recovery

The service uses automated resilience and data protection controls, including:

- automated incremental backups
- backups stored in a separate data centre environment
- documented restore procedures to support service recovery

These measures support business continuity and recovery in the event of service disruption.

5. Resilience and availability

The platform is designed to scale with demand and uses cloud-native infrastructure to maintain availability. Service health and performance are monitored, with alerting in place to support timely response to incidents.

6. Onboarding support

Customers are supported through a structured onboarding process. This includes:

- an onboarding meeting to confirm user access requirements and reporting needs
- setup of the customer workspace and user permissions
- Initial upload of certificate information
- online training covering certificate management, alerts, dashboards, and reporting

Customer-specific user guidance is provided via the support helpdesk.

7. Offboarding and access to data on exit

Customers can export certificate monitoring data throughout the contract and at contract end. Monthly reports are provided during the contract summarising certificates monitored, updates identified, and subscriptions that have expired.

At contract end, certificate data can be exported directly from the platform. Once extraction is confirmed, access is disabled and data is retained or securely deleted in line with contractual and regulatory requirements.

8. Service constraints and customisation

The service supports configuration of:

- user roles and access levels
- notification recipients and alert preferences

Core monitoring logic is standardised to ensure consistency and integrity of Update Service checks. Changes that could affect monitoring accuracy are controlled.

9. Service levels and support hours

Support is provided during standard business hours (09:00–17:00, Monday to Friday, excluding UK public holidays). Support covers platform use, certificate management, alerts, reporting, and issue resolution.

Service availability is monitored continuously, and issues are prioritised based on impact and severity.

10. Outage and maintenance management

The service uses monitoring and alerting to detect outages or degradation. Customers are notified of confirmed outages through agreed communication channels, with updates provided until resolution.
Planned maintenance is managed through change control processes and communicated in advance where practicable.

11. Technical requirements

Customers require:

- a supported modern web browser
- internet connectivity
- authorised user accounts provisioned by a customer administrator

Users authenticate using multi-factor authentication (2FA).

12. Security

Security controls include:

- encryption in transit using TLS 1.2 or higher
- encryption at rest provided through AWS security controls
- role-based access control and least-privilege permissions
- multi-factor authentication
- vulnerability management and patching processes
- defined incident management and response procedures
- protective monitoring and audit logging

Access to management interfaces and support channels is restricted to authorised users.

13. After-sales support

Ongoing support is provided by a dedicated customer support team. Support includes:

- user assistance and troubleshooting

Co Registration No. 02387512 | VAT No 890 0227 39 | Data Protection : Z9753599

- guidance on certificate monitoring and alerts
- reporting and data export support
- escalation of technical issues where required

Co Registration No. 02387512 | VAT No 890 0227 39 | Data Protection : Z9753599