CISO Assurance Series

Preservica Security Testing Overview

About the CISO Assurance Series

The Preservica CISO Assurance Series provides concise, factual briefings intended to support customer Legal, Privacy, Information Security, and Risk stakeholders when evaluating specific aspects of the Preservica platform. Each document in the series focuses on a defined topic and is designed to complement, not replace, formal contractual documentation and due diligence materials.

These briefings are provided for informational and assurance purposes only. They describe Preservica's approach, controls, and practices as of the date of publication and do not constitute legal advice, contractual commitments, or warranties. Customers should rely on their applicable agreements with Preservica, including any data processing agreements and service terms, for binding obligations.

This document forms part of the Preservica CISO Assurance Series and may be read independently or alongside other series publications, depending on customer needs.

Preservica

Preservica

1. About this document

Preservica provides a cloud-based digital preservation platform used by customers operating in regulated, public sector, and risk-sensitive environments.

This document is designed as a **customer-facing assurance overview** that can be shared internally with Legal, Privacy, Information Security, Compliance, and Risk stakeholders when evaluating or approving the use of Preservica's SaaS platform.

It explains:

- How Preservica tests and manages the security of its own platform on an ongoing basis
- The controls and methodologies Preservica operates internally to identify and remediate vulnerabilities
- How customers and their appointed third parties may request security testing of their Preservica environment
- What Preservica does not permit and why, and how operational coordination requirements protect both parties

This document is **informational in nature**. It supports customer understanding and internal assurance discussions and should be read alongside the applicable contract, Order Form, and Data Processing Agreement.

2. Preservica's security testing programme at a glance

Across all Preservica cloud deployments, the following core principles apply to security testing and vulnerability management:

- **Continuous internal testing –** Preservica operates continuous security testing activities throughout the software development lifecycle, not only at release boundaries.
- **Multiple testing layers –** Static, dynamic, and infrastructure-level testing methods are combined to provide broad coverage across code, application, and platform layers.
- **Risk-based vulnerability management –** Identified vulnerabilities are assessed, prioritised, and tracked to remediation in accordance with Preservica's documented vulnerability management policy.
- **Independent annual assurance –** Preservica commissions independent penetration testing of the platform on an annual basis.

- **Customer testing is available by request for dedicated environment customers –** Customers on the Enterprise Plus (EPC) and Enterprise Plus Perform (EPC-P) tiers may request security testing of their own Preservica environment subject to a structured coordination and approval process. Testing on multi-tenant environments is not permitted.

- **All testing is scoped and time-bounded –** Whether internal or customer-initiated, all active security testing is conducted within defined parameters to protect platform integrity and service availability.

3. Preservica's internal security testing programme

Preservica operates a layered security testing programme that spans the full software development and operational lifecycle. The programme is designed to identify vulnerabilities as early as possible and to ensure that Preservica's production environments remain secure on an ongoing basis.

3.1 Static Application Security Testing (SAST)

Preservica integrates static application security testing at two points in the development process. SAST tooling operates within developer integrated development environments (IDEs), providing real-time feedback during the writing of code. It is also enforced as an automated gate in the pull request (PR) process, prior to any code being merged into the main branch.

In addition to analysing first-party code, SAST tooling monitors third-party and open-source library dependencies for known vulnerabilities, ensuring that the security posture of Preservica's software supply chain is maintained alongside the security of the code Preservica writes directly.

This approach ensures that potential security defects — including injection vulnerabilities, insecure configurations, and vulnerable dependencies — are identified and addressed at the earliest practical point in the development process, before code reaches any deployed environment.

3.2 Dynamic Application Security Testing (DAST)

Preservica performs dynamic application security testing against all release candidates (RCs) and DAST forms part of the release gating process. Release candidates must meet defined security thresholds to proceed to production deployment; those that exceed acceptable thresholds are not released until findings are addressed. DAST exercises the running application to identify vulnerabilities that may not be visible through static analysis alone, including those arising from runtime behaviour, configuration, and component interaction.

DAST is conducted in controlled, non-production environments. It is not performed against live customer environments without explicit coordination and approval.

3.3 Vulnerability Management, Detection and Response (VMDR)

Preservica operates continuous vulnerability management, detection, and response (VMDR) across its platform infrastructure. This programme provides ongoing visibility into vulnerabilities affecting the underlying infrastructure, operating systems, and third-party components used to deliver the Preservica service.

Identified vulnerabilities are assessed against recognised scoring frameworks, prioritised by risk, and tracked through to remediation in accordance with Preservica's documented patching and vulnerability management policy. The effectiveness of this programme is subject to independent oversight as part of Preservica's ISO 27001 and SOC 2 Type II assurance.

3.4 Annual independent penetration testing

In addition to its continuous testing activities, Preservica commissions an independent penetration test of the Preservica platform on an annual basis. Testing is conducted by a CREST-certified independent third-party security firm and covers the application, API, and infrastructure layers of the service.

Results are reviewed by Preservica's Information Security team, and findings are assessed and remediated in accordance with Preservica's vulnerability management policy. The penetration test summary report, accompanied by a cover letter from Preservica's CISO summarising the current status of any findings, is available to customers and prospects on request. Existing customers may request this directly; prospects will be asked to sign a Non-Disclosure Agreement prior to disclosure. Requests should be directed to Information.Security@preservica.com.

4. Customer-initiated security testing

Preservica understands that customers — particularly those operating in regulated, public sector, or risk-sensitive environments — may have an internal requirement to conduct or commission their own security testing of third-party systems, including those used to process or store their data.

4.1 Eligibility

Customer-initiated security testing is available **exclusively** to customers on Preservica's dedicated infrastructure tiers: **Enterprise Plus (EPC)** and **Enterprise Plus Perform (EPC-P)**. These customers operate on infrastructure provisioned specifically for their organisation.

Security testing of any multi-tenant Preservica environment is **not permitted under any circumstances**. This applies to all other Preservica product tiers, including Starter Free, Starter Plus, Professional, Professional Plus, and Enterprise. The shared nature of multi-tenant infrastructure means that testing activity cannot be scoped in a way that adequately protects other customers sharing that infrastructure.

Customers on eligible tiers who wish to initiate security testing should note that their dedicated environment remains hosted on and interconnected with Preservica's broader cloud infrastructure. Testing must therefore be scoped strictly to the customer's own environment and must not extend to shared platform components.

4.2 What customers may request

Customers may request the following types of security testing against their own Preservica environment:

- **Vulnerability scanning** – Automated scanning to identify potential vulnerabilities without active exploitation
- **Penetration testing** – Structured testing including manual and automated techniques, with the option of authenticated or unauthenticated approaches, and black-box, grey-box, or white-box knowledge levels

Testing may be conducted directly by the customer's internal security team or by a third-party security firm appointed on the customer's behalf.

4.3 The customer security testing request process

All customer-initiated security testing must be requested in advance using Preservica's **Customer Security Testing Request Form**. Testing may not commence until written approval has been received from Preservica's Information Security team.

The request process requires customers to provide:

- The specific targets to be tested (fully qualified domain names and/or IP addresses)
- The source IP addresses or ranges from which scanning traffic will originate
- The proposed testing window (start and end dates and times)
- The type of testing, authentication method, knowledge level, and any automated tools to be used

A minimum of **30 days' notice** is required between form submission and the proposed start date. This lead time is required to allow Preservica to coordinate with its Security Operations Centre (SOC), Cloud Operations team, network operators, and cloud service providers (CSPs) as appropriate given the nature and scope of the proposed activity.

At the conclusion of testing, customers are required to share results with Preservica's Information Security team. Both parties review findings jointly before any remediation timelines are discussed or agreed.

The Customer Security Testing Request Form is available from Preservica's Information Security team at Information.Security@preservica.com.

4.4 Operational coordination requirements

Preservica operates a managed SaaS environment with active security operations monitoring, web application firewall (WAF) controls, rate-limiting, and intrusion detection capabilities. Any external scanning activity — regardless of its source — needs to be coordinated with Preservica's operational teams prior to commencement.

This coordination requirement exists to:

- Prevent legitimate scanning traffic from triggering SOC alerts, WAF blocks, or rate-limiting responses that could interrupt the testing activity or produce misleading results
- Ensure that Preservica's SOC is not responding to false-positive alerts generated by coordinated testing activity
- Protect service availability and the integrity of Preservica's monitoring baseline during the testing window — uncoordinated scanning activity has the potential to affect service availability and could place the customer in breach of contracted SLA obligations
- Allow Preservica to notify its CSPs and network operators where the nature or scale of planned activity warrants it

This is an operational and governance requirement, not simply a procedural formality. Preservica cannot approve testing activity that has not been subject to this coordination process.

5. What Preservica does not permit

The following activities cannot be approved under Preservica's customer security testing process, under any circumstances:

- **Continuous or open-ended scanning** – Scanning windows must be discrete and time-bounded. Preservica does not permit persistent, ongoing, or unscheduled scanning of its environments by customers or third parties.

- **DoS and DDoS testing** – Denial-of-service and distributed denial-of-service testing cannot be approved under any circumstances, regardless of the customer's environment type.

- **Expansion of scope beyond agreed targets** – Testing must remain within the specific targets, source addresses, and time window approved in the Customer Security Testing Request. Scope may not be expanded unilaterally during an active testing window.

5.1 A note on attack surface monitoring and OSINT tools

Some customers use automated attack surface monitoring or Open Source Intelligence (OSINT) tools as part of their third-party risk management (TPRM) programmes. Preservica acknowledges the legitimate intent behind such tooling, but customers should be aware of the following limitations when applying these tools to Preservica environments.

Such tools assess publicly visible infrastructure at the network and DNS layer. They do not have visibility into the specific configuration of an individual customer's Preservica environment, and findings may relate to shared platform infrastructure — including cloud provider services, content delivery networks, and other components — that are not relevant to the customer's contracted service.

Preservica may consider findings raised through OSINT tools but reserves the right to assess each finding in context and to formally accept risks with written explanation where a finding does not apply to the customer's specific environment or represents a false positive.

Customers who have read and understood the above and nonetheless wish to raise a specific finding from attack surface monitoring tooling may do so through their usual Preservica contact or via Information.Security@preservica.com.

6. Assurance and oversight

Preservica's security testing programme is embedded within its broader information security and compliance framework, which is subject to independent oversight and certification.

- **ISO 27001:2022** – Preservica's information security management system, including its vulnerability management and security testing controls, is certified against ISO 27001:2022.
- **ISO 9001:2015** – Preservica's quality management system is certified against ISO 9001:2015, supporting consistent and controlled processes across the organisation.
- **SOC 2 Type II** – Preservica's operational controls, including those relating to vulnerability management and change management, are independently audited as part of its annual SOC 2 Type II engagement. The SOC 2 Type II report is available to customers on request under NDA.
- **TX-RAMP** – Preservica holds TX-RAMP certification, recognising compliance with the Texas Risk and Authorization Management Program requirements for cloud services used by Texas state agencies.
- **AZRAMP** – Preservica holds AZRAMP certification, recognising compliance with the Arizona Risk and Authorization Management Program requirements for cloud services used by Arizona state agencies.

Customers may request access to Preservica's assurance materials, certifications, and audit reports through Preservica's Trust Center: https://preservica.com/trust-center

7. Next steps

Customers wishing to request security testing of their Preservica environment should contact Preservica's Information Security team at Information.Security@preservica.com to initiate the process.

Customers with additional security questions are encouraged to raise them through their usual Preservica contact or formal due-diligence process.

Preservica is committed to supporting customers with clear, accurate information to enable confident adoption of its cloud platform.

8. Frequently Asked Questions (FAQ)

The following FAQs are based on common questions raised by customer Legal, Information Security, and Compliance teams during due-diligence and procurement reviews.

8.1 Does Preservica perform its own security testing?

Yes. Preservica operates a continuous internal security testing programme comprising SAST integrated into developer IDEs and enforced at every pull request (including third-party library dependency scanning), DAST as a release gate against all release candidates, and continuous VMDR across the platform infrastructure. Preservica also commissions an independent annual penetration test.

8.2 Can we perform penetration testing of our Preservica environment?

Customer-initiated security testing is available only to customers on the Enterprise Plus (EPC) and Enterprise Plus Perform (EPC-P) product tiers. It is not available for multi-tenant environments. Eligible customers must submit a Customer Security Testing Request Form to Information.Security@preservica.com and receive written approval before testing commences. A minimum of 30 days' notice is required.

8.3 Can we appoint a third-party security firm to test on our behalf?

Yes. Customers may appoint a qualified third-party security firm to conduct testing on their behalf. The third party must be identified in the Customer Security Testing Request Form and is subject to the same scope, source, and timing constraints as directly conducted testing.

8.4 Why does Preservica require 30 days' notice?

The lead time allows Preservica to coordinate with its SOC, Cloud Operations team, network operators, and CSPs as appropriate. Without this coordination, legitimate scanning traffic may trigger SOC alerts, WAF rules, or rate-limiting responses that could affect both the testing activity and the availability of the service. This coordination requirement exists to protect both parties.

8.5 Can you disable WAF or rate-limiting controls for our test?

Preservica can discuss WAF exception requests as part of the testing coordination process. Customers should be aware that if scanning source IPs are excluded from WAF controls, test results will not reflect a real-world adversary and will show the application with its automated defences partially bypassed. Preservica recommends attempting scanning without an exception first and will advise on a case-by-case basis.

8.6 Can we use continuous attack surface monitoring tools against our Preservica environment?

Preservica does not permit continuous or open-ended scanning as part of the customer security testing process, and such tools are not a substitute for the coordinated testing described in this document. Customers should also be aware of the significant limitations of such tooling when applied to Preservica environments — see Section 5.1 for detail.

8.7 We have a finding from a security scoring tool — how do we raise it?

Findings from attack surface monitoring or security scoring tools should be raised with Preservica's Information Security team at Information.Security@preservica.com. Preservica will review each finding in context, assess its applicability to the specific customer environment, and provide a written response that may include an explanation of false positives, a risk-based remediation plan, or formal risk acceptance with rationale.

8.8 We are an Enterprise Plus (EPC) or Enterprise Plus Perform (EPC-P) customer — can we test our dedicated environment?

Yes. Enterprise Plus (EPC) and Enterprise Plus Perform (EPC-P) customers are welcome to request security testing of their dedicated environment through the standard Customer Security Testing Request process. Testing must be scoped to the customer's specific environment and must not extend to shared platform infrastructure. The same 30-day notice requirement and operational coordination obligations apply.

8.9 What happens to findings from our test?

At the conclusion of testing, customers are required to share results with Preservica's Information Security team. Both parties review findings jointly before any remediation timelines are discussed or agreed. Preservica will provide a written response that may include explanations of false positives, a risk-based remediation plan with mutually agreed timelines, or formal risk acceptance with rationale. No remediation timeline is agreed until both parties have jointly reviewed the applicable findings.

8.10 Can we see the results of the independent annual penetration test?

Yes. The penetration test summary report, produced by a CREST-certified independent third-party security firm, is available on request alongside a cover letter from Preservica's CISO summarising the current status of any findings. Existing customers may request this directly; prospects will be asked to sign a Non-Disclosure Agreement prior to disclosure. Requests should be directed to Information.Security@preservica.com.

8.11 Where can we find independent assurance?

Preservica makes security certifications, assurance materials, and audit reports available through its Trust Center: https://preservica.com/trust-center

About Preservica

Preservica is transforming the way organizations around the world protect and future-proof critical long-term digital information. Available in the cloud (SaaS) or on-premise, our award-winning Active Digital Preservation™ archiving software has been designed from the ground up to tackle the unique challenges of ensuring digital information remains accessible and trustworthy over decades.

It's a proven solution that's trusted by thousands of businesses, archives, libraries, museums and government organizations around the world, including the UK National Archives, Texas State Library and Archives, MoMA, Yale and HSBC.

preservica.com/about