EXECUTIVE SOFTWARE

EAP Cloud Security Assurance Programme

Independent annual security assurance for the EAP Cloud environment

Contents

Introduction

The EAP Cloud service supports organisations delivering employee assistance and mental health services across multiple regions.

Given the sensitivity of information managed within the EAP Cloud environment, and the increasing expectations from enterprise and government customers, Executive Software has established a formal Security Assurance Programme.

This programme is designed to ensure that security is not only implemented but independently validated and continuously maintained.

Why this programme is being introduced

Security expectations for cloud-based health, wellbeing, and employee assistance services continue to increase. Enterprise, government, and large organisational customers are placing greater emphasis on independent validation, formal evidence, and repeatable assurance processes.

The programme has been introduced so that customers are not required to rely solely on vendor self-attestation or manage fragmented assurance activities themselves. It provides a centrally managed, independently supported assurance model that can be used consistently across the EAP Cloud customer base.

What this means in practice

The EAP Cloud environment is now supported by an annual programme of independent security assessment, testing, and reporting.

- Recurring: delivered through an annual assurance programme.
- Independent: externally validated by cybersecurity specialists.
- Actionable: findings are identified, prioritised, and addressed.
- Shareable: assurance artefacts are made available for customers to use.

What changes for customers

The programme represents a material uplift from an ad hoc security response model to a structured, recurring assurance model.

Previous approach	**Security Assurance Programme approach**
Security information provided on request.	Standard assurance artefacts produced through each assurance cycle.
Customer questionnaires and RFP responses handled separately.	Reusable evidence supports security questionnaires, procurement, and audit processes.
Security posture primarily described by Executive Software.	Security posture independently assessed, tested, and reported.

Testing and review activity could be customer specific.	Independent annual testing and review is centrally coordinated.
Findings handled as individual issues.	Findings are prioritised, tracked, remediated, and incorporated into continuous improvement.

What customers receive

A key part of this programme is the delivery of tangible security outputs that customers can use directly. Each assurance cycle produces the following outputs.

- **Independent assurance outputs:** organisation-level security assessment aligned with ISO 27001, including validation of both design and operating effectiveness of controls.
- **Penetration testing outcomes:** testing across web portals, APIs, and Provider Manager, with vulnerabilities classified by severity and supported by prioritised remediation recommendations.
- **Cloud security review:** assessment of Azure configuration against CIS benchmarks and Zero Trust principles, including identification of configuration risks and recommended improvements.
- **Customer-facing artefacts:** executive summary of security posture, evidence of independent testing and validation, and documentation suitable for security questionnaires, procurement processes, and government or enterprise audits.

Included customer benefits

The programme is intended to provide practical benefits that customers can use directly in their own governance, procurement, and assurance activities.

- Access to annual independent security assurance outputs.
- Reusable evidence to support customer security reviews, questionnaires, procurement processes, and audits.
- Reduced need for separate customer-led penetration testing or assurance coordination.
- Greater confidence for boards, funders, government agencies, and enterprise stakeholders.
- Improved visibility of security posture and remediation activity.
- Ongoing strengthening of the EAP Cloud environment through a formal continuous improvement cycle.

Security findings and continuous improvement

The programme is designed to ensure that findings are not just identified but addressed.

- Prioritisation of findings based on risk.
- Structured remediation planning.

- Ongoing monitoring of improvements.
- Incorporation of outcomes into future development and operations.

This creates a continuous improvement cycle, rather than a one-off assessment.

Delivery model

Executive Software manages the Security Assurance Programme on behalf of all customers. This includes:

- Engagement of independent cybersecurity specialists.
- Definition of testing scope and coverage.
- Coordination of testing activities.
- Management of remediation.
- Production and distribution of assurance artefacts.

There is no requirement for customers to commission or manage their own testing.

Shared investment and customer value

The Security Assurance Programme represents a shared investment in the assurance, resilience, and trustworthiness of the EAP Cloud service. Rather than each customer commissioning separate reviews, testing, and reporting, Executive Software centrally manages the programme for the benefit of the customer base.

If undertaken independently, a comparable programme of independent security assurance, penetration testing across multiple application layers, cloud infrastructure review, remediation management, and enterprise-ready security reporting would typically cost in excess of NZD $100,000 per annum.

By delivering this centrally across the EAP Cloud environment, customers receive the benefit of a mature assurance programme at a significantly lower proportional cost than commissioning equivalent work individually.

- The cost of specialist assurance activity is shared proportionately.
- Duplicate customer-led effort is reduced.
- Assurance is standardised and reusable across common procurement and audit needs.
- Customers receive stronger evidence without needing to manage the assurance process themselves.
- Executive Software can respond to security requirements through a planned programme rather than repeated ad hoc activity.

Security control alignment

To support formal assurance outcomes, certain baseline controls are expected within the EAP Cloud environment.

For example, where customers wish to utilise assurance artefacts for procurement, audit, or government and enterprise requirements, alignment with controls such as multi-factor authentication may be required.

Executive Software will work with customers to support this alignment where necessary.

Supporting security architecture and controls

The Security Assurance Programme operates on top of an established set of controls within the EAP Cloud environment, including data encryption at rest and in transit, role-based access control and least privilege, network segmentation and firewall protection, monitoring, logging, alerting, vulnerability detection, and threat monitoring.

The underlying environment continues to operate on Microsoft Azure, with security controls aligned to industry standards.

Customer-specific assurance activities

The Security Assurance Programme is intended to reduce the need for customer-specific assurance activity by providing a standard set of independently validated artefacts that can be reused across common security, procurement, and audit requirements.

Customers may still choose to undertake their own testing or request additional support for security questionnaires, tenders, RFPs, or customer-specific assurance processes.

Where these activities extend beyond the standard assurance artefacts, Executive Software can support them as additional services, subject to appropriate scope and commercial alignment.

Resilience and continuity

The EAP Cloud environment is designed for resilience, including geo-redundant Azure infrastructure, automated backups and point-in-time recovery, and Azure Site Recovery failover capability. This supports continuity of service in the event of infrastructure failure.

Summary

The EAP Cloud Security Assurance Programme provides a material uplift in the assurance, validation, reporting, and security governance available to customers. It combines annual independent validation of security controls, penetration testing, cloud infrastructure review, remediation management, and customer-facing artefacts for audit and procurement use.

By delivering this programme centrally, Executive Software reduces duplication across the customer base, provides stronger assurance evidence, and supports a secure, independently validated, and continuously improving EAP Cloud environment.