Penetration Test Summary – Validation Manager

Dionach performed a penetration test for Ascentry (previously Finbiosoft Oy) between 7th and 19th January 2026, in line with recognised industry best practice. The objectives of the test were to find and highlight any potential security threats and vulnerabilities relating to Ascentry's Validation Manager web application and supporting Azure infrastructure. Please note that credentials were supplied for the purpose of testing.

All findings were classified as medium or lower-risk issues and the penetration test confirmed that the current security infrastructure is sufficient to prevent remote attackers from compromising the Validation Manager web application and underlying Azure environment. The tested application and cloud infrastructure have no critical or high severity vulnerabilities.

Security testing determined that Ascentry's Validation Manager incorporates appropriate and effective controls to safeguard user accounts and data from external compromise. The assessment confirmed the presence of robust account-protection mechanisms, stringent defences against unauthenticated attack vectors, properly implemented measures to mitigate injection attacks, and consistently enforced good access control practices throughout the application. Moreover, validation of the identified security controls is done through regular auditing and testing via independent third parties. Ascentry's security assessment procedures are included within the scope of its ISO/IEC 27001 certification.

Testing was performed in line with the OWASP Top 10 ASVS Level 1 testing methodology and a manual testing approach was to ensure appropriate security controls were in place to prevent unauthorised access to personal identifiable information (PII), account compromise and other security vulnerabilities.

Dionach are a CREST and CHECK accredited organisation, and perform over 1000 penetration tests annually and our consultants hold industry recognised certifications; such as CREST Registered Tester, CREST Certified Tester, OSCP, OSWE and ISO 27001 LA and LI.

Industry standard tools such as Burp Suite Pro, Nmap, FFUF, Nikto and Nessus Pro were used to test applications. ScoutSuite, Nessus, Nmap and NetExec as well a manual review of the Azure configuration was used as part of the Azure Technical Security Review.

Ascentry have been provided with a full technical report which contains all vulnerability information, relevant proof of concepts and remediation advice. This attestation letter provided by Dionach highlights the strong and robust security controls in place.

Test Details	
Application Name	Validation Manager and its Azure infrastructure
Dates test carried out	7th January to 19th January 2026
Attestation issue date	27/01/2026

For any questions relating to the detailed scope of this attestation or to obtain further security information, please liaise directly with Ascentry.