Crystal Eye Compliance & Cryptographic Capability

Information and Response to Cryptographic Evaluations Report – June 2025

Company Name and ABN	Red Piranha Ltd 63 160 631 505
Years in business	12
Years providing ICT deliverables	9
Background	As part of ensuring Australian Signals Directorate (ASD) programs remain fit for purpose, Red Piranha offers this report to address standards used within the Crystal Eye platform on the ASD Cryptographic Evaluations (ACE) program and Crystal Eye cryptographic standards used within the platform. Crystal Eye provides backwards compatibility with respect to older encryption standards so locking down your Crystal Eye network to meet security controls will rely on end users understanding the needs and implementing the correct settings. This report aims to help end users understand some of these requirements, explain the formal position around cryptographic standards, and provide assurance to partners around cryptographic functionality.
Details of ability to deliver the offered categories	Red Piranha contributes to the Information Security and Cybersecurity Industries with its Crystal Eye Platform and numerous other services, both standalone and integrated with the Crystal Eye platform, including, but not limited to: • Vulnerability Assessments and Penetration Testing • Virtual Chief Information Security Officer (vCISO) and Crystal Eye Integrated Electronic Chief Information Security Officer (eCISO) engagements • Governance, Risk and Compliance (GRC) Audits and Consultancy • Digital Forensics Services • Managed Detection and Response • Threat Hunting and Threat Intelligence services • Incident Response Services • Threat Intelligence Analysis • Cyber Security Reviews and Assessment Services, and • Corporate and General Staff Security Awareness Training. At Red Piranha, all customers who have a Crystal Eye platform within their environment automatically communicate and engage with Red Piranha's Global Security Operations Centres. Licensed Crystal Eye platforms are continuously monitored and maintained by Red Piranha Limited's Global Security Operations Centre personnel. Each platform is also inclusive of Security Information and Event Management (SIEM) operations and functionality.

Details of Red Piranha's Risk Management Systems	The Red Piranha Risk Committee, chaired by Rosemary Milkins (Non-Executive Director, Chairperson), was established in 2022. The Risk Committee regularly advises and reports to the Board on enterprise and cyber risks, including monitoring of Red Piranha's Risk Management Systems.
	Within the domain of operational risk, Red Piranha is certified to ISO/IEC 27001:2022 and focuses on the continuous improvement of its Information Security practices.
	Red Piranha is also certified to ISO 9001:2015 for Quality Management, ensuring that its customers get consistent, good-quality products and services.
	Red Piranha aligns to IRAP and the Australian ISM and has undergone IRAP assessment. Red Piranha also aligns with the ASD's Secure by Design principles for secure software development.
	Red Piranha subscribes to the Defence Industry Security Program (DISP) and has achieved DISP membership. Projects are in place to achieve full compliance with Essential 8 Maturity Level 2 a per the latest DISP cybersecurity requirements. Additionally, we align to the DISP required areas of the Defence Security Principles Framework (DSPF).
	Red Piranha has been granted the Defence Export Permit by the Department of Defence, allowing it to export their technology to foreign governments (Defence Export Permit: DOD/DEP/20829572).
	Red Piranha regularly conducts vulnerability testing on its service delivery network. Internal vulnerability scans within the most recent quarter were conducted on 30/04/2025, 03/06/2025 and 27/06/2025. The results of these tests were analysed by the Compliance Team, the SecOps Team, and the CISO on submission, and requests for mitigation activities were made, based on the level of risk each vulnerability posed to Red Piranha at that time. As part of the ongoing process, vulnerabilities are monitored by the Infrastructure and Compliance teams on a weekly basis.
	In addition, penetration testing on product change control and on new product releases as per our internal policies are conducted. Penetration tests for Crystal Eye v5.0 were completed on 22/02/2024 and 09/04/2024. Testing on the Red Piranha Orchestrate platform was completed on 22/10/2024. Testing for the Crystal Eye v5.5 Beta was completed on 24/03/2025.
	Red Piranha has implemented an incident management system for both internal and client incidents. Measurable processes and metrics have been introduced for change control and vulnerability management. The outputs and mitigations from these processes are reviewed and managed by the Compliance Team in weekly risk meetings. Compliance attends weekly Infrastructure and SecOps management meetings to ensure vulnerabilities, changes and mitigations are tracked and managed in a timely fashion.
	Red Piranha maintains membership in CREST ANZ (Council of Registered Ethical Security Testers), providing assurance that testing conducted is of exemplary quality, conforms to industry best practices and meets the highest ethical standards in penetration testing services.
	Red Piranha have made a security report submission page available to the public for the reporting of security issues directly to the Internal Compliance Team ([Compliance Contact	Red Piranha](#)).

	Red Piranha undertakes management for product development in the ISO domain ISO/IEC 15408 and aims to attain Common Criteria (CC) certification.
	Red Piranha seeks to be listed on the Australian Government Evaluated Products List (EPL), subscribes to the ACE (ASD Cryptographic Evaluation) program, and aims to address Australian Signals Directorate (ASD) questions consumers may have around standards applied in its products in this report.
	Red Piranha Ltd complies with the ASX Risk Management Framework outlined in the ACH Clearing Rules Guidance Note No. 13.

FAQs - Standards and Cryptographic Position

Is Perfect Forward Secrecy (PFS) supported in all TLS Communications?	Yes, all proxy and SSL-VPN TLS communications supports PFS.
Does Crystal Eye support SNMPv3? Do we have the option to force disable SNMPv1 and SNMPv2 and are they disabled by default?	Crystal Eye does not support SNMP and so there is no requirement to disable SNMPv1 or SNMPv2.
Are all web and TLS components on Crystal XDR forced to TLS 1.2/1.3 only with TLS 1.0 and 1.1 both Client and Server disabled?	While backwards compatibility is supported, Crystal Eye has support to drop all TLS connections from clients with TLS 1.0, TLS 1.1, and TLS 1.2 allowing customers to force TLS 1.3 communications.
Is support for DES / 3DES and all other block ciphers with a 64-Bit Block Size disabled/blocked?	As AES has replaced DES and 3DES, the WebGUI still supports 3DES for backwards compatibility. Web Proxy and SSL communications has DES and 3DES disabled by default.
Are all weak ciphers disabled such as those that use RC4, MD5, or have key lengths of less than 128 bits or anonymous/unauthenticated DH Algorithms?	Yes, all weak ciphers are disabled.
Confirming all Telnet, FTP and TFTP services are disabled by default	In Crystal Eye these are not supported and are disabled
Confirming SSLv3 is forced disabled?	Yes, SSLv3 is disabled

Additional information

Red Piranha has a Security Operations team that can be called upon as required. Red Piranha operates 24/7/365 and has a maximum response time of 4 hours Monday 00:00 UTC to Saturday 00:00 UTC and 8 hours afterhours.

Red Piranha employs personnel outside of Australia; however, Data Sovereignty is maintained inside Australia when required.

Red Piranha implements Multi-Factor Authentication wherever possible.

Red Piranha's Crystal Eye Secure Edge also implements the cryptographic capabilities listed in this statement.

ISO 9001:2015

Red Piranha is certified to ISO 9001:2015 (Certificate number: 703236).

Last Internal Audit Completed November 2024

Last External Audit Date: 28 April 2025

Next Internal Audit Scheduled for October 2025

Next External Audit Scheduled for April 2026

ISO/IEC 27001:2022

Red Piranha is certified to ISO/IEC 27001:2022 (Certificate number: 781489)

Internal Audit Completed October 2024

Last External Audit Date: 28 April 2025

Next Internal Audit Scheduled for October 2025

Next External Audit scheduled for April 2026

ISO/IEC 15408

Red Piranha follows processes and guidelines outlined in ISO/IEC 15408.

IRAP

Red Piranha has undergone IRAP assessment and works to the Australian Signals Directorate's Information Security Registered Assessors Program (IRAP) alignment.

ISM

Red Piranha aligns with the Australian Government Information Security Manual (ISM).

DISP

Red Piranha received DISP membership on 17 February 2022.

Red Piranha has completed our Annual Security Report for the past year in July 2025.

Crystal Eye OS 5.5

Crystal Eye Enterprise v5.5 (Build 9) is the latest release of Red Piranha's Crystal Eye OS 5.5 as at 31/7/2025, this version supports Intel's GEN14 based systems.

Crystal Eye OS 5.0

Crystal Eye Enterprise v5.0 (Build 39) is the most recent release of Red Piranha's Crystal Eye OS 5.0 as at 31/07/2025, this version supports Intel's GEN14 based systems. Crystal Eye OS 5.0 will continue to be supported and updated throughout the Crystal Eye OS 5.5 lifecycle.

Change Control Testing

All penetration testing is conducted following our defined change control process, which follows 4 key stages:
- Change Acceptance
- Change Implementation
- Change Approval
- Change Deployment

Each internal team involved in the change control process follows set SLAs and uses a common repository for all change requests.

We perform 3 types of penetration testing each quarter to ensure the maximum level of assurance:
- Blind test – simulates a typical cyber-attack scenario

- Double-Blind – is an advanced version of the Blind test with particular attention on restricting information sharing
- Targeted/Lights-On – all personnel involved know that a test is being carried out

Statement of Accuracy

Red Piranha confirms the accuracy of the information provided in this document.

Ben Aylett
Product Manager

Anthony Blackman
Operations Manager