AUSCERT

Allies in Cyber Security

Year in Review 2025

Table of Contents

Foreword

When I sat down a year ago to write the Year in Review, I strongly leaned into the **2025 Annual Threat Assessment from ASIO**. One year later, not only do we find ourselves facing the same issues, but in many ways, they have **intensified and accelerated** beyond expectations.

Now, before I start, I want to share a message that one of my colleagues sent to me a few months ago. My colleague was using an AI chatbot to make recommendations for conference speakers and the bot returned this:

> “David Stockdale (UQ / AUSCERT Board): ...He has the "weary CISO" vibe that is incredibly relatable when arguing why we should just turn the internet off and go back to paper.”

Now I’m not sure where it gleaned its knowledge from but the “weary CISO” is certainly the truth. And I suspect that many of you feel the same way with an **intensifying and accelerating threat landscape**. Whilst we should be cautious around media hype associated with the latest AI developments, the world in which we operate is now firmly grounded in this **new technological era**, whether it is used for good or bad. And I would love to say there is a quick fix to these rapidly emerging threats, but there isn’t. At times like these, we need to rely on fundaments such as **knowing the threats** that exist against ourselves and our organisations, **know our assets**, especially the real target of data assets, and a **defence in depth** (multiple controls) strategy.

Working backward on this list, the frameworks we adopt e.g. NIST, ISO27001 etc. give that defence in depth approach so we should ensure our organisation picks one and follows it. The choice is individual and needs to be a good business fit to maximise the chance of successful adoption. Once it is chosen, AUSCERT can help with **assessing the company’s compliance and provide a roadmap to help with adoption.**

AUSCERT

Now when it comes to asset management, please let me know if you've got this one "really" sorted… because if you have, the rest of us would like to know how. We know that **understanding the assets is fundamental** to staying on top of the vulnerability problem, but how many organisations really understand the true target, their data assets? Again, no quick fix but **AUSCERT's Data Governance training** offering is attracting a lot of interest. This course is intended to assist organisations in getting started on this fundamentally important area.

The last point is threats. Now we are all familiar with **cyber threat intelligence (CTI)** and how automated feeds can help block bad IP addresses or domains, but how many organisations have a view to why they may be attacked and the **tactics that could be used against them?** These can be generic tactics but increasingly they are crafted to the organisation and/or the vertical within which you reside. Knowing your data (information) assets and then workshopping how an adversary may use them, including against you, is **fundamental to your cyber resilience**.

All of these areas, **threat intelligence, training, and GRC** (governance, risk & compliance) are key areas in the **2025 – 2030 AUSCERT strategy** and like all cyber security businesses, we are working hard to stay relevant to the needs of our community. Increasingly we see organisations needing to invest in their own capabilities. We strongly advocate and believe AUSCERT has a place in assisting with this, for example, through our **freshly launched internship program**: it is intended to assist The University of Queensland in giving real cyber security experience to some of the brightest young graduates in the country.

So, to conclude and referencing the AI chatbot again, you are **not on your own** and whilst we cannot "turn off the internet and go back to paper", we definitely need to be **stronger together.** I am confident the **AUSCERT community** can materially assist with this.

Dr. David Stockdale

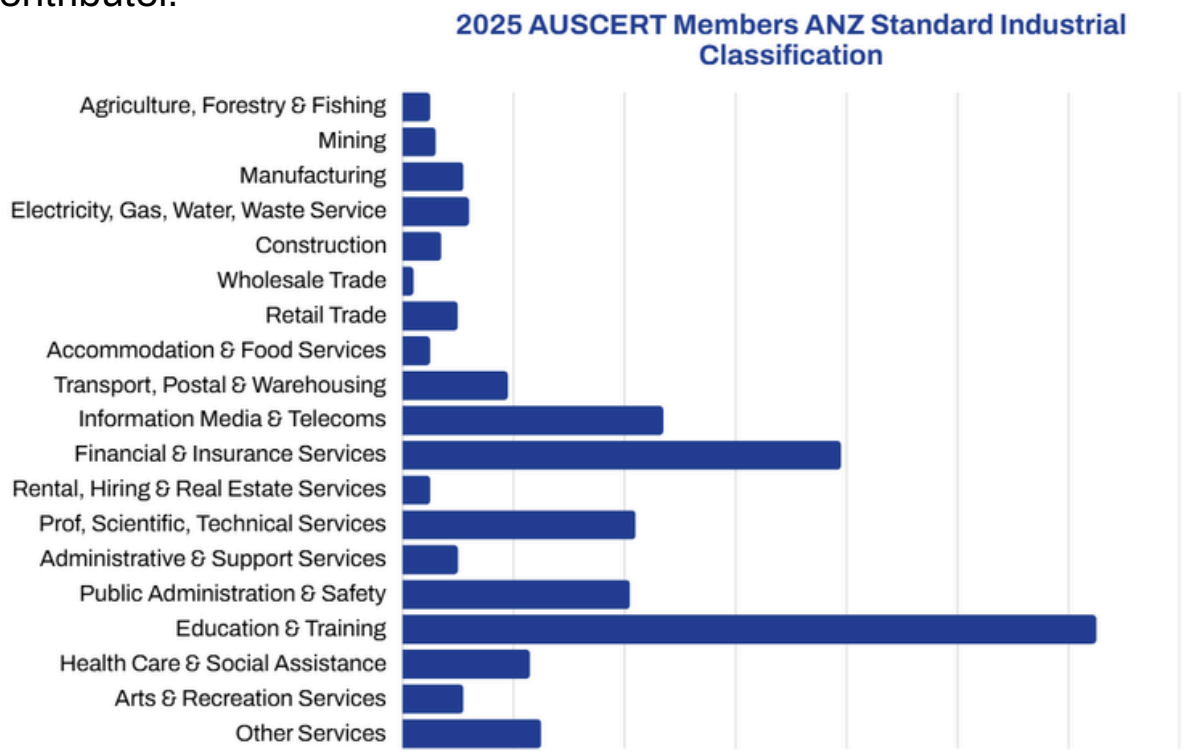
Director, AUSCERT

AUSCERT

Membership Overview

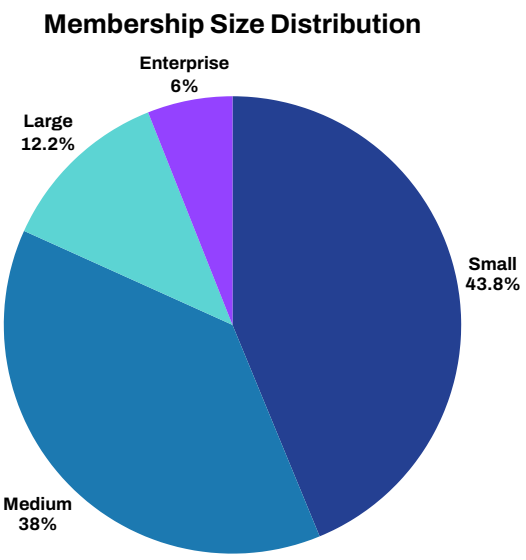
AUSCERT's membership base represents a diverse cross-section of industries, spanning organisations of all sizes. The **Education & Training** sector remains our most prominent member group, comprising of higher education institutions alongside primary and secondary schools.

The **Financial & Insurance Services** sector continues to be our second-largest membership segment, encompassing major banks. The **Information, Media & Telecommunications** sector is now the third-largest contributor to our membership base. In 2024, the Professional, Scientific & Technical Services industry was the third largest contributor.



Member Demographics

Throughout 2025, growth remained strong among small to medium-sized organisations. Our membership is geographically diverse across Australia, with Queensland, Victoria and New South Wales leading as the most represented states. In addition, we support a smaller number of international members, primarily from the South Pacific, as well as Fiji, India, Papua New Guinea, and the United States.



AUSCERT

Allies in Cyber Security

2025 Overview

7,850 Incidents Handled

9,382 Security Bulletins Distributed

27,553 Member Security Incident Notifications Sent

22,374 Sensitive Information Alerts Sent

12,601 Phishing Takedowns Handled

AUSCERT

Incident Support

In 2025, our analyst team managed **7,850** incidents. Each incident is identified and classified based on its characteristics to help determine the most common threats impacting our members. It is worthwhile noting that information requests are also classified under incidents.

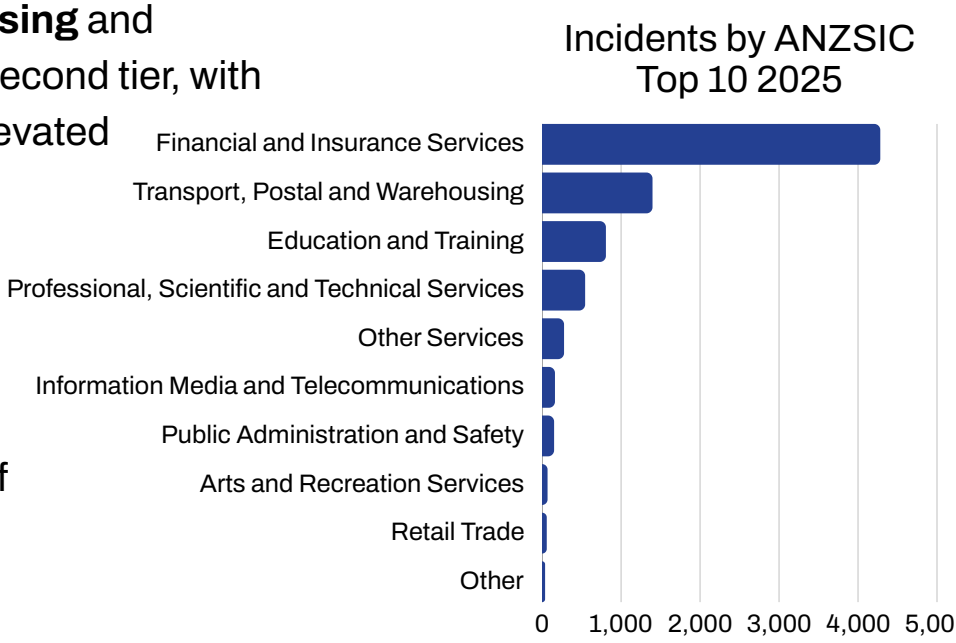
Top Incidents

- Phishing
- Info request
- Spam

Incidents by ANZSIC Top 10 2025

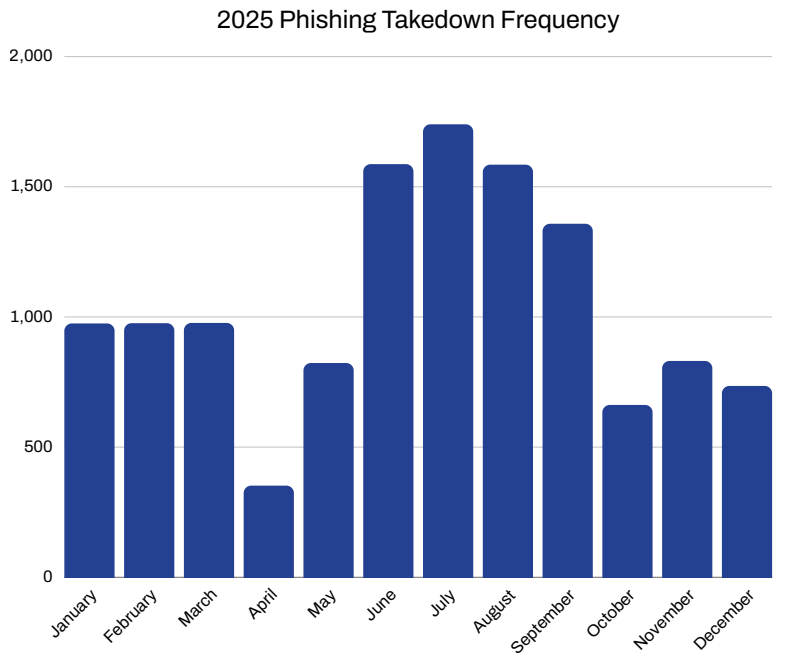
In 2025, **Financial and Insurance Services** experienced the highest number of incidents. **Transport, Postal and Warehousing** and **Education and Training** form a second tier, with notably fewer incidents but still elevated compared to other sectors.

Most remaining industries report comparatively low incident volumes, indicating that cyber activity in 2025 was heavily concentrated in a small number of high-value sectors.



Phishing Takedowns

Phishing takedown trends continue to evolve rapidly in the era of artificial intelligence. In 2025, AUSCERT analysts handled 24% more phishing takedown requests compared to the previous year, reflecting both the increasing scale and sophistication of phishing activity. In response, we continue to enhance our infrastructure to improve efficiency and better support our members amidst these evolving threats.

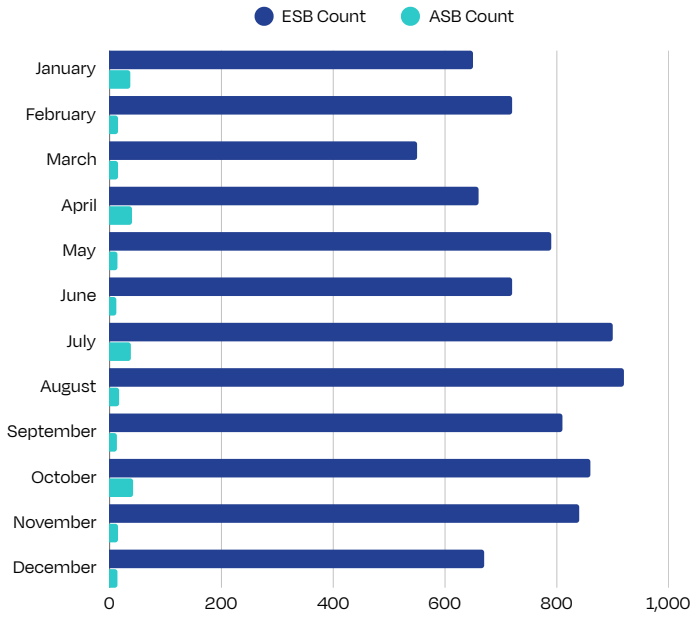


Vulnerability Management

Bulletins

In 2025, AUSCERT issued 9,382 Security Bulletins, marking a 16% increase from the previous year. Of that, 9,155 External Security Bulletins (ESB) were processed, as well as 227 AUSCERT Security Bulletins (ASB). AUSCERT continues to utilise the Exploitation Prediction Scoring System (EPSS) within our Bulletins and Critical Member Security Incident Notifications service, allowing members to effectively prioritise their vulnerability management.

ESB and ASB Bulletins by Time Year 2025

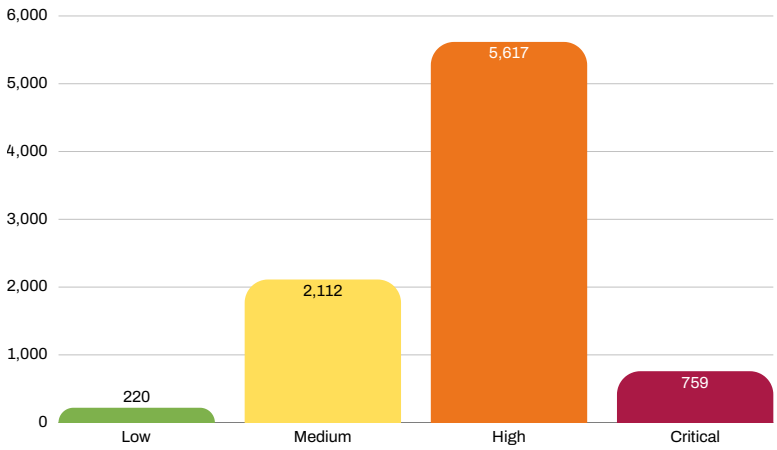


Bulletins by CVSS Rating

The Common Vulnerability Scoring System (CVSS) is an industry-standard framework used to evaluate and communicate the severity of security vulnerabilities, enabling organisations to prioritise remediation based on potential impact. AUSCERT identifies reported issues using Common Vulnerabilities and Exposures (CVE) identifiers to ensure consistent classification and tracking.

In 2025, most reported bulletins continued to be rated as High severity, reflecting an ongoing increase in threats capable of causing significant data breaches, financial impact, and operational disruption. Addressing high-risk vulnerabilities first supports improved risk reduction, regulatory compliance, and more efficient use of limited security and IT resources.

Bulletins by CVSS Rating Year 2025



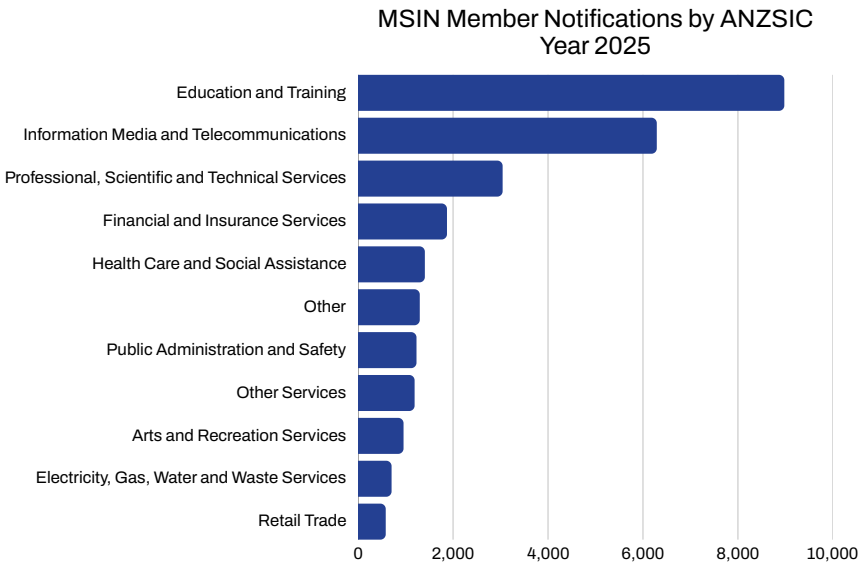
2025 CVSS Score Severity Ratings

0.01 - 3.9: Low
4.0 - 6.9: Medium
7.0 - 8.9: High
9.0 - 10.0: Critical

Vulnerability Management

Member Security Incident Notifications

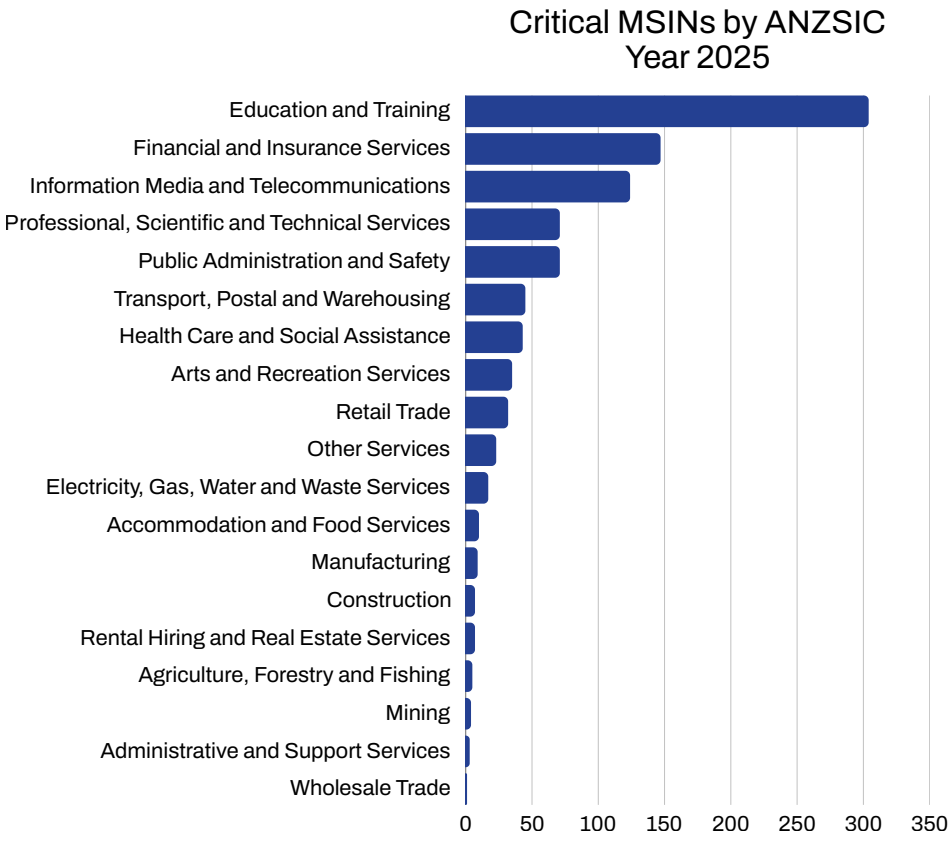
Member Security Incident Notifications (MSINs) are sent when incidents are observed in member's public facing infrastructure that could be directly impacting their organisation.



In 2025, a total of **27,553** MSINs were issued to AUSCERT members. **Education and Training** received the highest number of MSINs, continuing a consistent trend observed in the previous year. The **Information, Media and Telecommunications** sector ranked second, followed closely by **Professional, Scientific and Technical Services** in third, reinforcing their ongoing exposure to cyber threats due to high connectivity, data volumes, and reliance on digital infrastructure.

Critical Member Security Incident Notifications

In 2025, AUSCERT issued a total of 1,050 Critical MSINs, representing an 18% increase compared to 2024. This growth highlights a continued rise in high-impact threats, particularly in the **Education and Training** sector, requiring immediate attention.

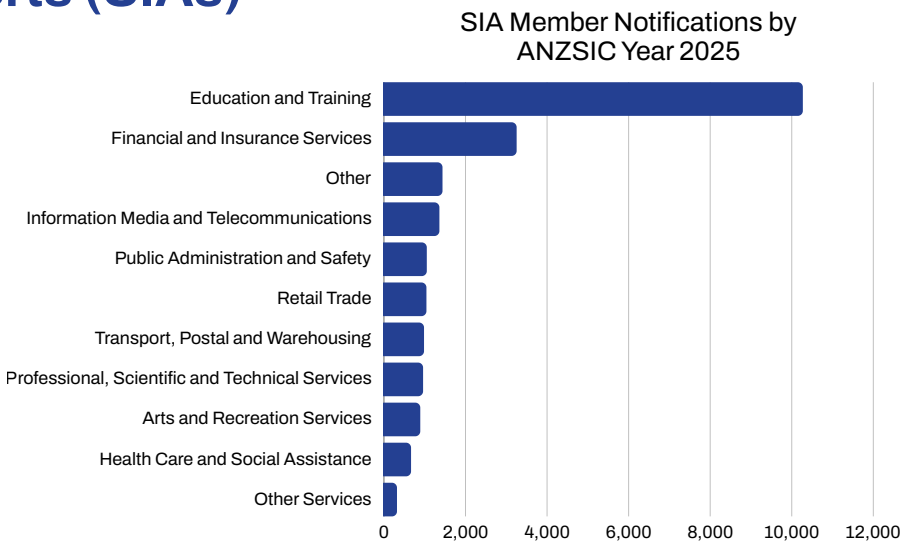


Financial and Insurance Services followed as the second-highest recipient, reflecting the attractiveness of the financial sector.

Threat Intelligence

Sensitive Information Alerts (SIAs)

Sensitive Information Alerts (SIAs) are issued to members via email when our analysts detect exposed credentials or other sensitive information, providing actionable details that enable organisations to rapidly assess risk and respond.



Reflecting the composition of our membership base, the **Education and Training** sector receives the highest volume of alerts, highlighting both its exposure to cyber risk and the critical importance of continuous monitoring and timely intelligence for this community. This is followed by the **Financial and Insurance Services** sector, which receives alerts at a frequency broadly comparable with other sectors, displaying the consistent threat landscape faced across industries.

Infrastructure Update - SIAs API

We're excited to share that our update to the Sensitive Information Alert (SIA) service is now available for members via the **Member Portal.**
This update:

- Returns structured credential data such as user, password, and URL.
- Filter and query results based on standard REST API principles.
- Mark SIAs as "actioned" once handled, enabling better tracking and integration with internal workflows.

AUSCERT

Governance, Risk & Compliance

Tabletop Exercises

Maturity Assessments

Cyber Incident Response Plans

NEW! Policy & Procedure Development

Maturity Assessment Success Story

Maturity assessments help organisations understand their current security posture by identifying gaps and areas of risk across the business.

A Brisbane-based high school has engaged our Governance, Risk and Compliance Maturity Assessment service on three occasions since 2023. Over this period, the school has demonstrated strong commitment and measurable progress in strengthening its cyber security posture and protecting critical assets.

Maturity Improvement Over Time

- September 2023: 15% – Very Weak
- September 2024: 36% – Average
- September 2025: 58% – Good

This consistent upward trend reflects sustained effort and targeted initiatives implemented over a 24-month period. As a result, the school now ranks at the upper end of the maturity spectrum, based on comparative assessments conducted by AUSCERT across the education sector.

Maturity	Score range
World	84-100%
Excellent	68-83%
Good	51-67%
Average	34-50%
Weak	18-33%
Very weak	0-17%

Members receive 15% off all GRC services!

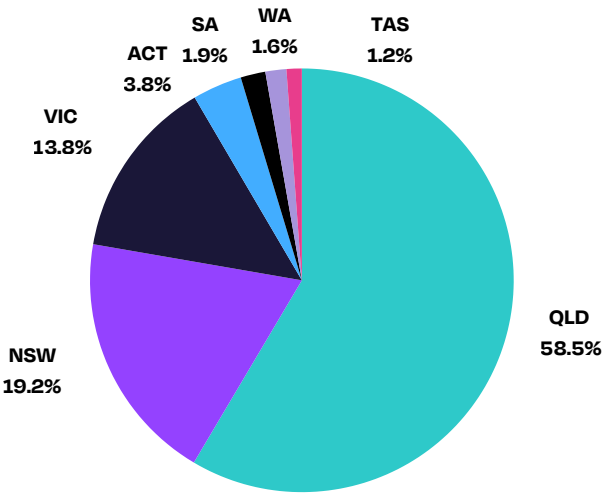
Contact us for a quote today
grc@auscert.org.au

AUSCERT Conference

AUSCERT2025 was a standout edition! Guided by the theme “Evolve and Thrive,” our exceptional speakers and attendees explored emerging security technologies, shared insights, and challenged conventional thinking.

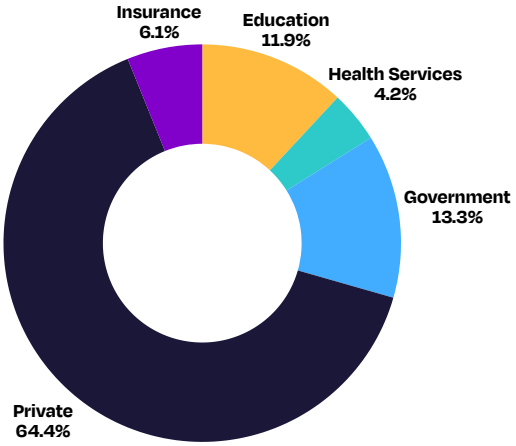
The AUSCERT Conference continues to grow each year, attracting delegates from across Australia. While attendance is national in reach, we maintain strong local engagement, with 58% of delegates based in Queensland.

Demographics by Location

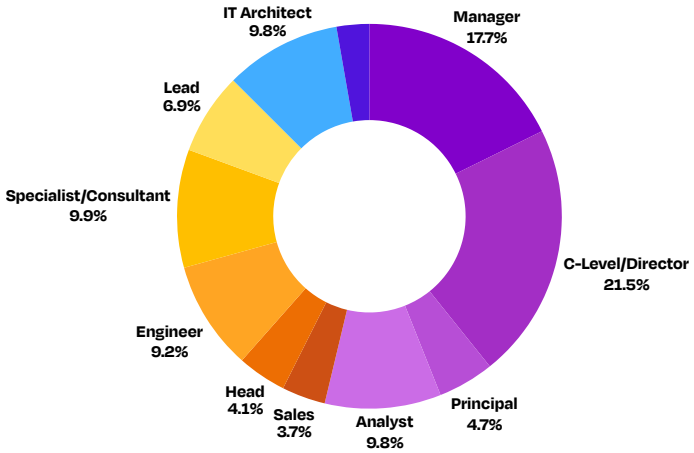


The conference has fostered an inclusive community that spans a wide range of industries and roles. Attendance data shows that private enterprise represents the largest segment of participants, followed by the education sector, then government and utilities, with most attendees holding manager or director-level positions.

Demographics by Industry



Demographics by Position



Community Outreach

AUSCERT's industry engagement reflects more than three decades of operational experience and a commitment to sharing that expertise with the wider community. These relationships enable faster, more coordinated responses to cyber threats and help build long-term resilience across interconnected digital environments.

In 2025, AUSCERT continued to strengthen its connections with the global cyber security community through knowledge sharing and collaborative initiatives. This included the publication of the white paper **Computer Emergency Response Teams in 2026: Now and Beyond**, which explores how CERT models and coordination mechanisms must evolve to meet future challenges.

In collaboration with **IDCARE**, AUSCERT also contributed to delivering the Cyber and Critical Tech Co-operation Program, providing cyber crime and online scam response assistance to micro businesses and individuals in Papua New Guinea and Fiji.

AUSCERT also worked closely with **ETHIO-CERT**, Ethiopia's national CERT, to help enhance and expand its cyber security capabilities. Through regular knowledge-sharing sessions, the teams collaborated to design and implement a service modelled on AUSCERT's Member Services Incident Notifications, providing timely threat alerts and actionable insights.

As a CERT serving all industries in Australia and neighbouring regions, AUSCERT's global partnerships remain vital to building a resilient and connected cyber security ecosystem.

Conclusion

In the last year, a lot of change has happened at AUSCERT! We introduced our five-year strategy and a renewed focus on long-term growth, resilience, and innovation. The team and I are immensely proud of the progress we have made so far. We are also excited about the journey ahead as we continue to evolve alongside a rapidly changing technology and threat landscape.

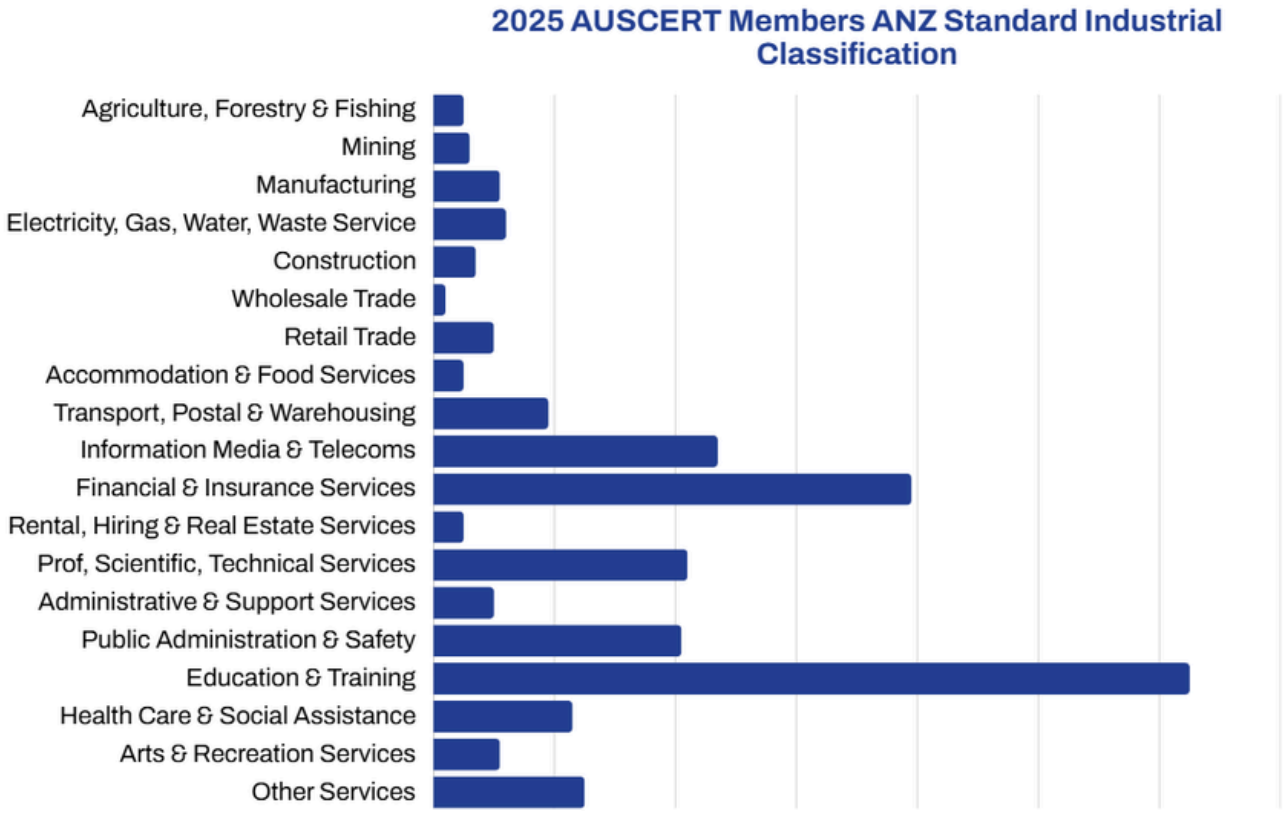
Our members have been fantastic: they offered us their feedback on our ideas, proofs-of-concept and renewed services. They demonstrate innovation, collaboration, and a strong commitment to cyber security maturity. Their engagement and trust are fundamental to our success.

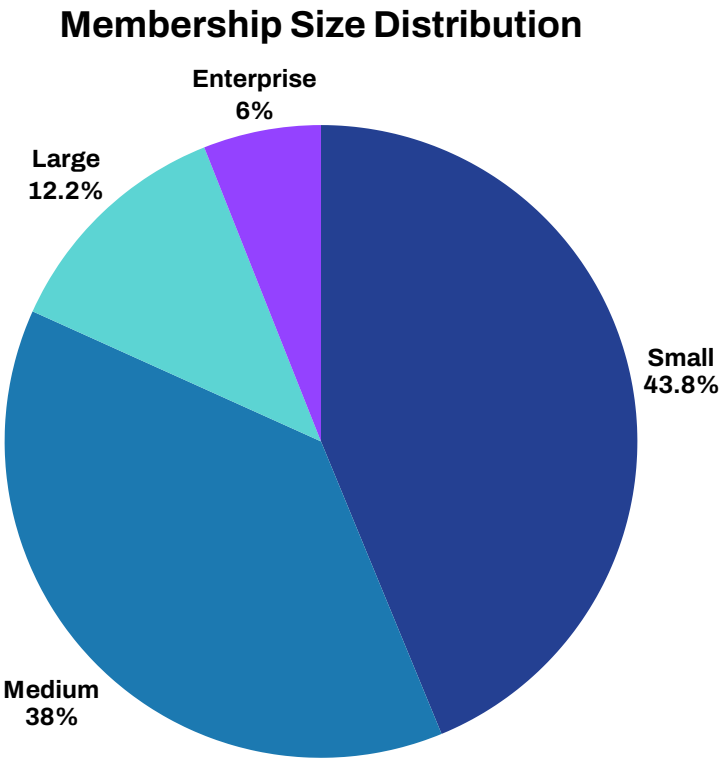
We look ahead with optimism and determination, confident that through strong partnerships, continued investment in our members, and a clear strategic direction, AUSCERT is well positioned to deliver lasting value in the years to come.

Dr. Ivano Bongiovanni

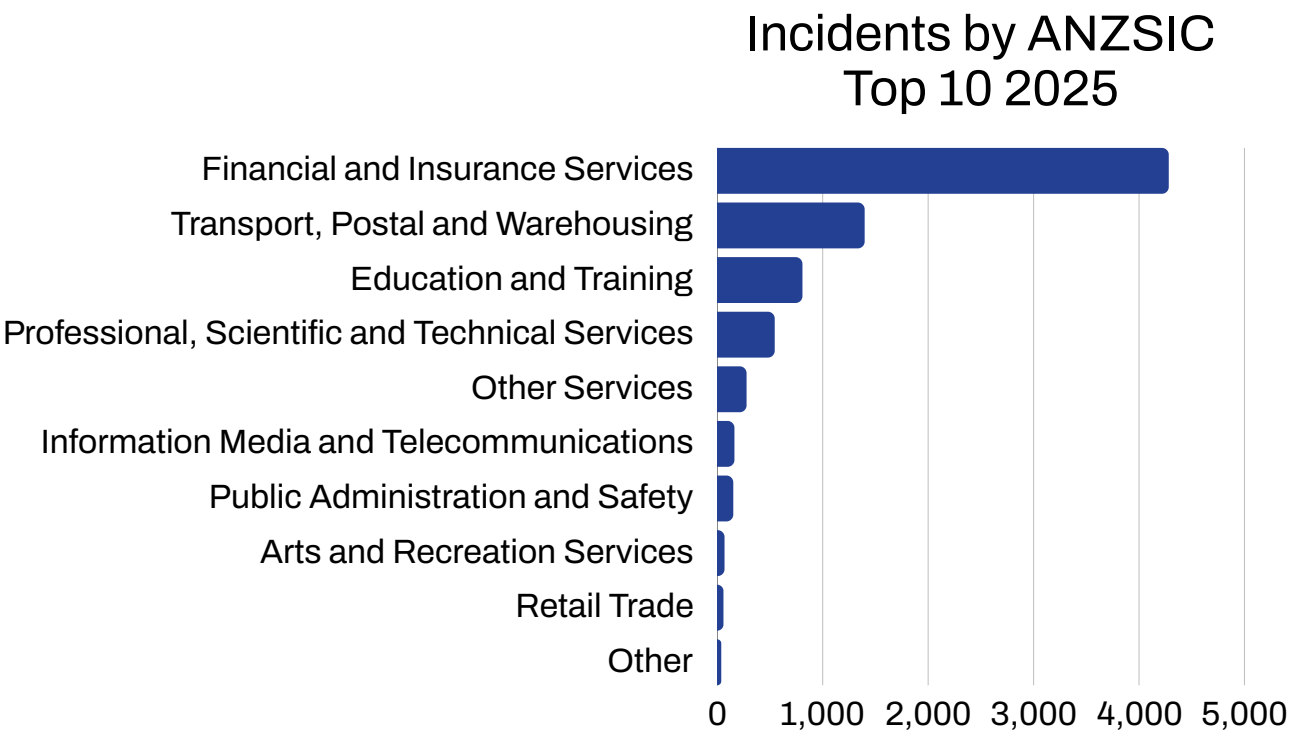
General Manager, AUSCERT

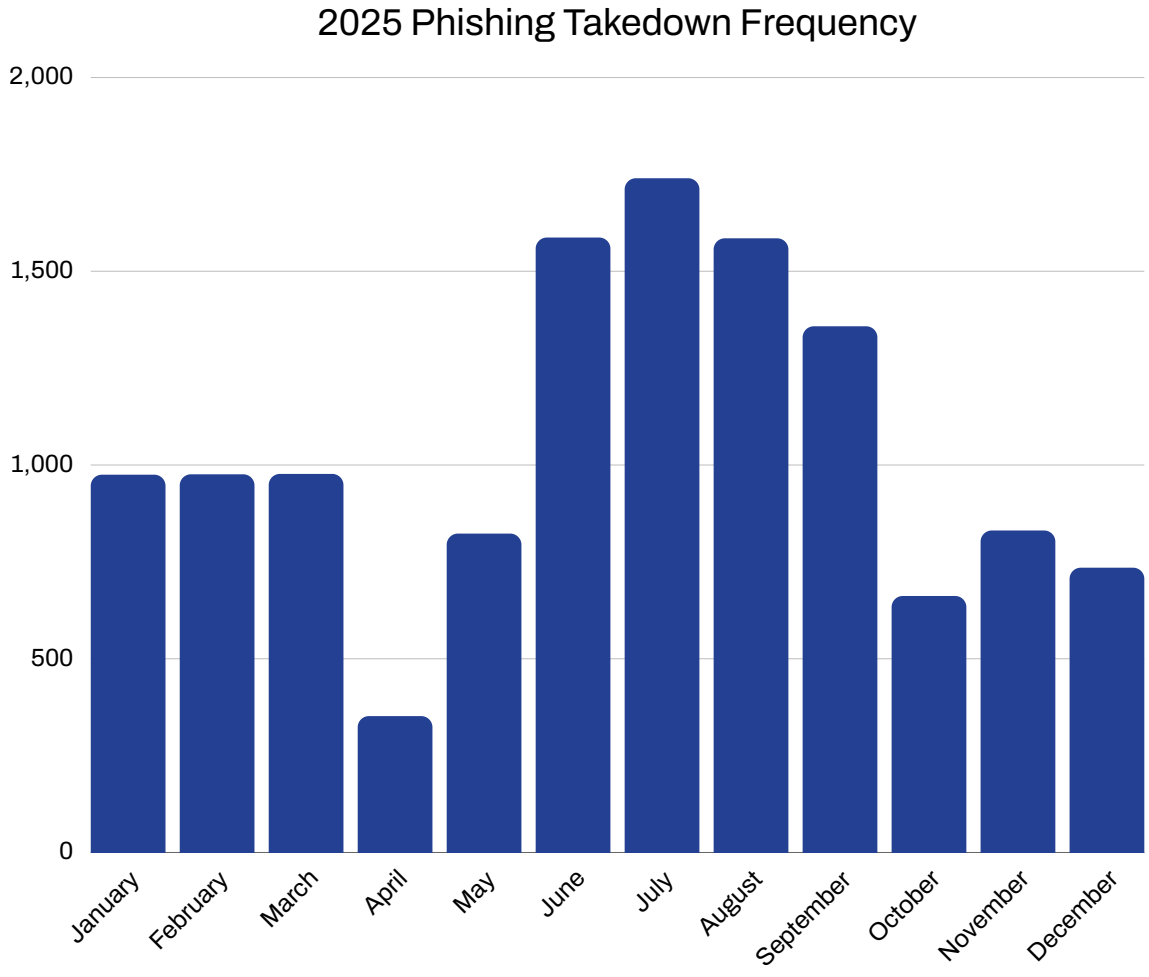
Appendix


2025 AUSCERT Members ANZ Standard Industrial Classification
Agriculture, Forestry & Fishing
Mining
Manufacturing
Electricity, Gas, Water, Waste Service
Construction
Wholesale Trade
Retail Trade
Accommodation & Food Services
Transport, Postal & Warehousing
Information Media & Telecoms
Financial & Insurance Services
Rental, Hiring & Real Estate Services
Prof, Scientific, Technical Services
Administrative & Support Services
Public Administration & Safety
Education & Training
Health Care & Social Assistance
Arts & Recreation Services
Other Services

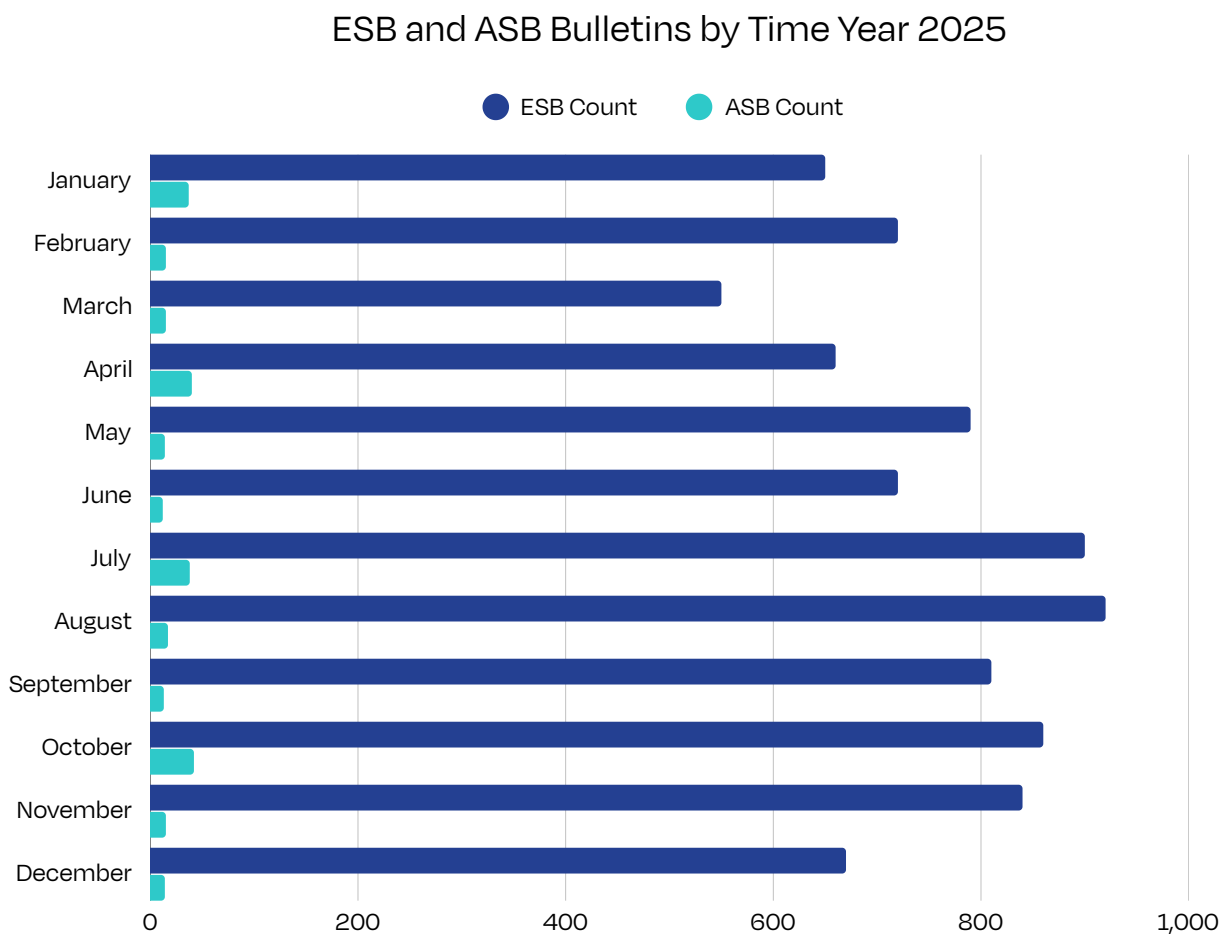

Membership Size Distribution
Enterprise 6%
Large 12.2%
Small 43.8%
Medium 38%

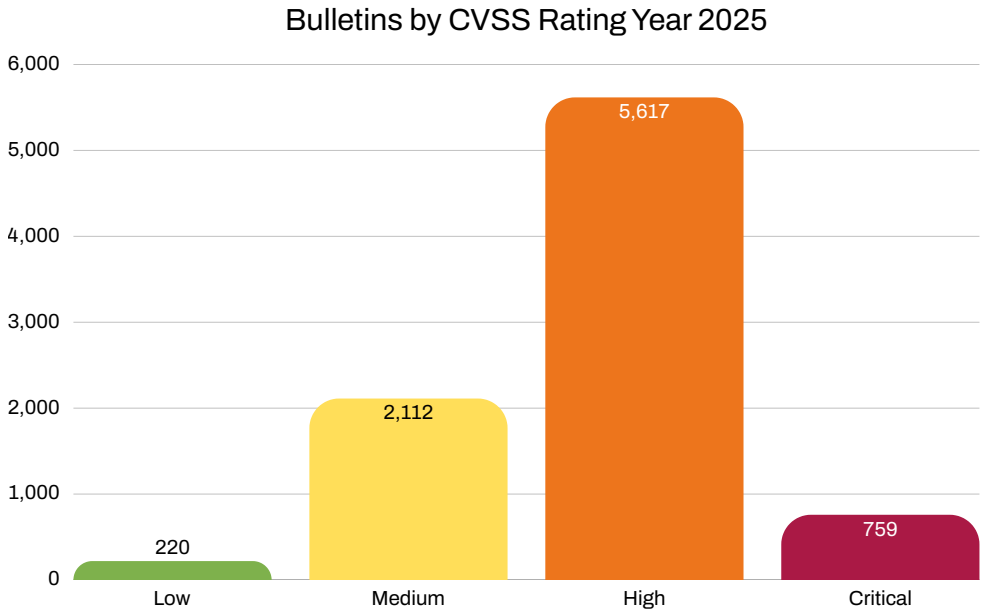
Appendix


Incidents by ANZSIC
Top 10 2025
Financial and Insurance Services
Transport, Postal and Warehousing
Education and Training
Professional, Scientific and Technical Services
Other Services
Information Media and Telecommunications
Public Administration and Safety
Arts and Recreation Services
Retail Trade
Other
0
1,000
2,000
3,000
4,000
5,000


2025 Phishing Takedown Frequency
2,000
1,500
1,000
500
0
January
February
March
April
May
June
July
August
September
October
November
December

Appendix

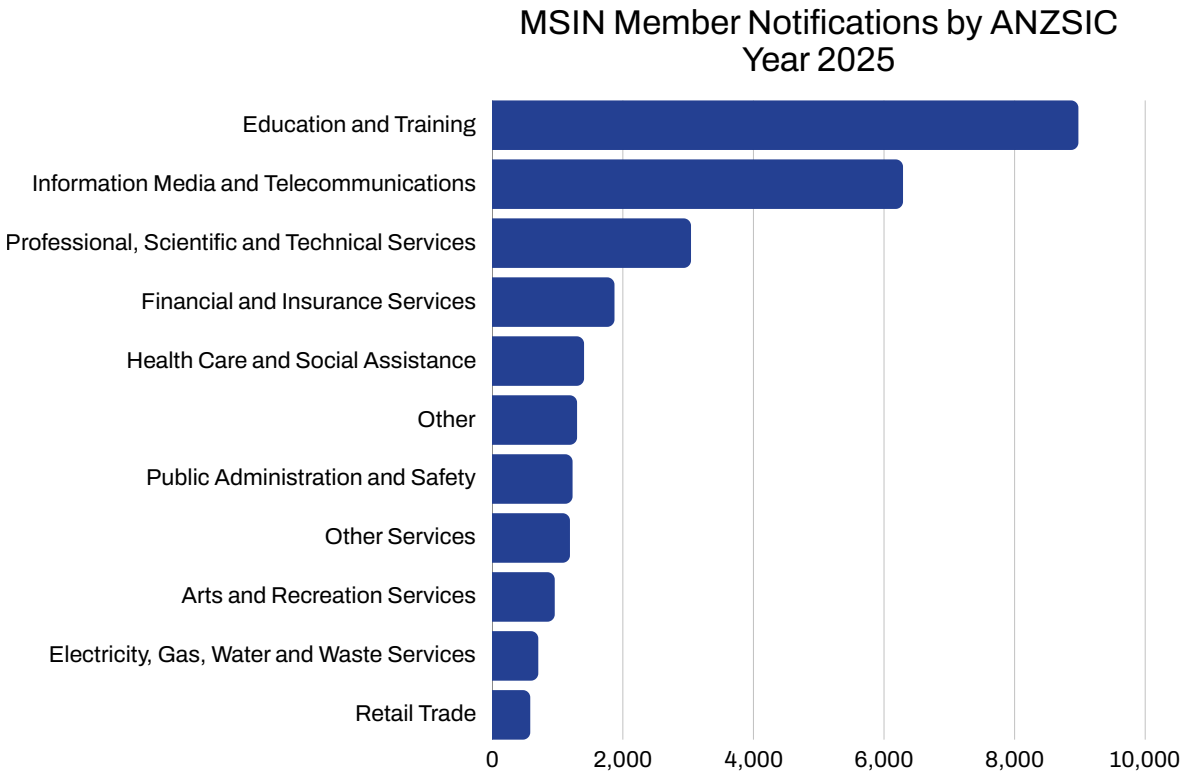


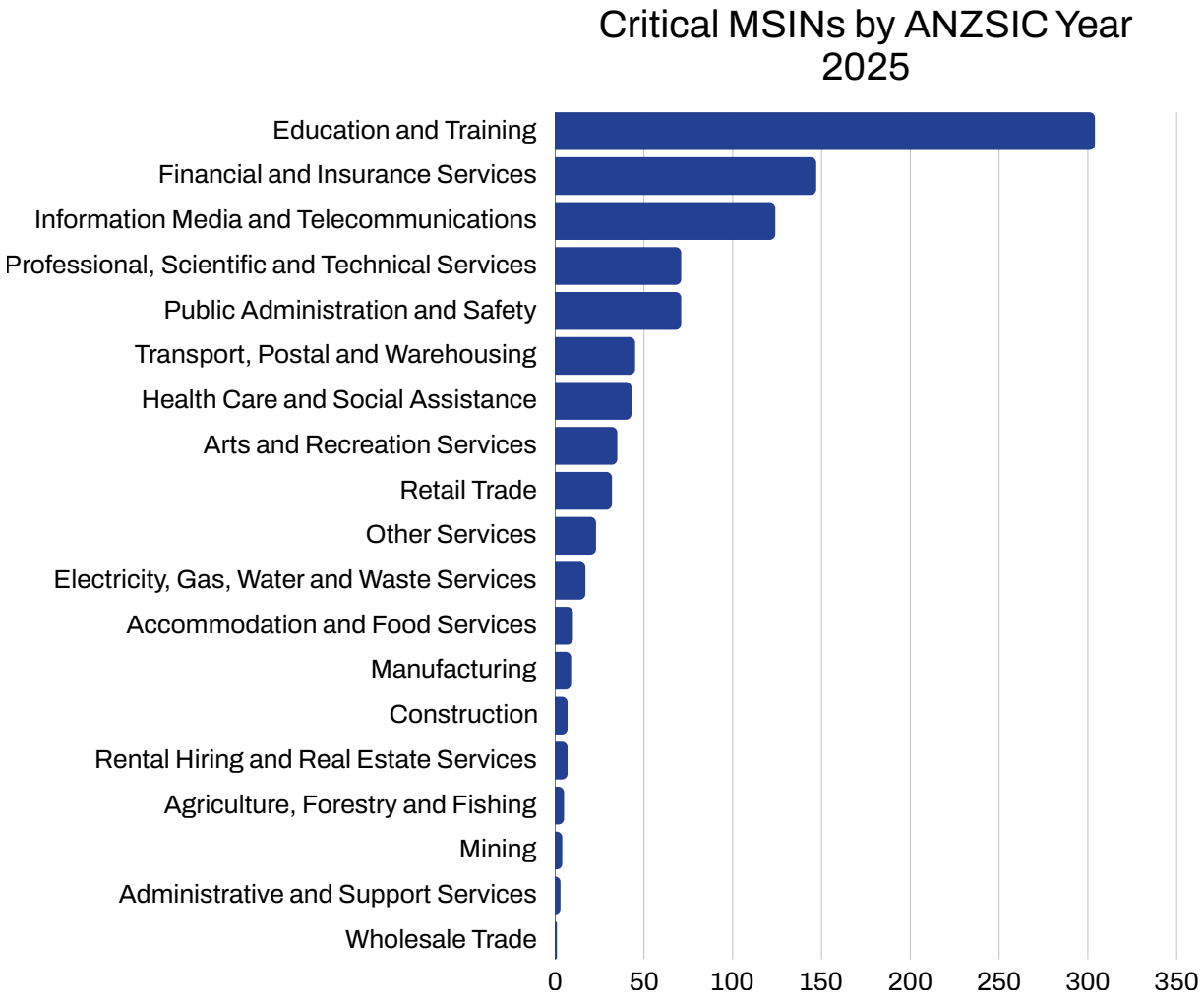


2025 CVSS Score Severity Ratings

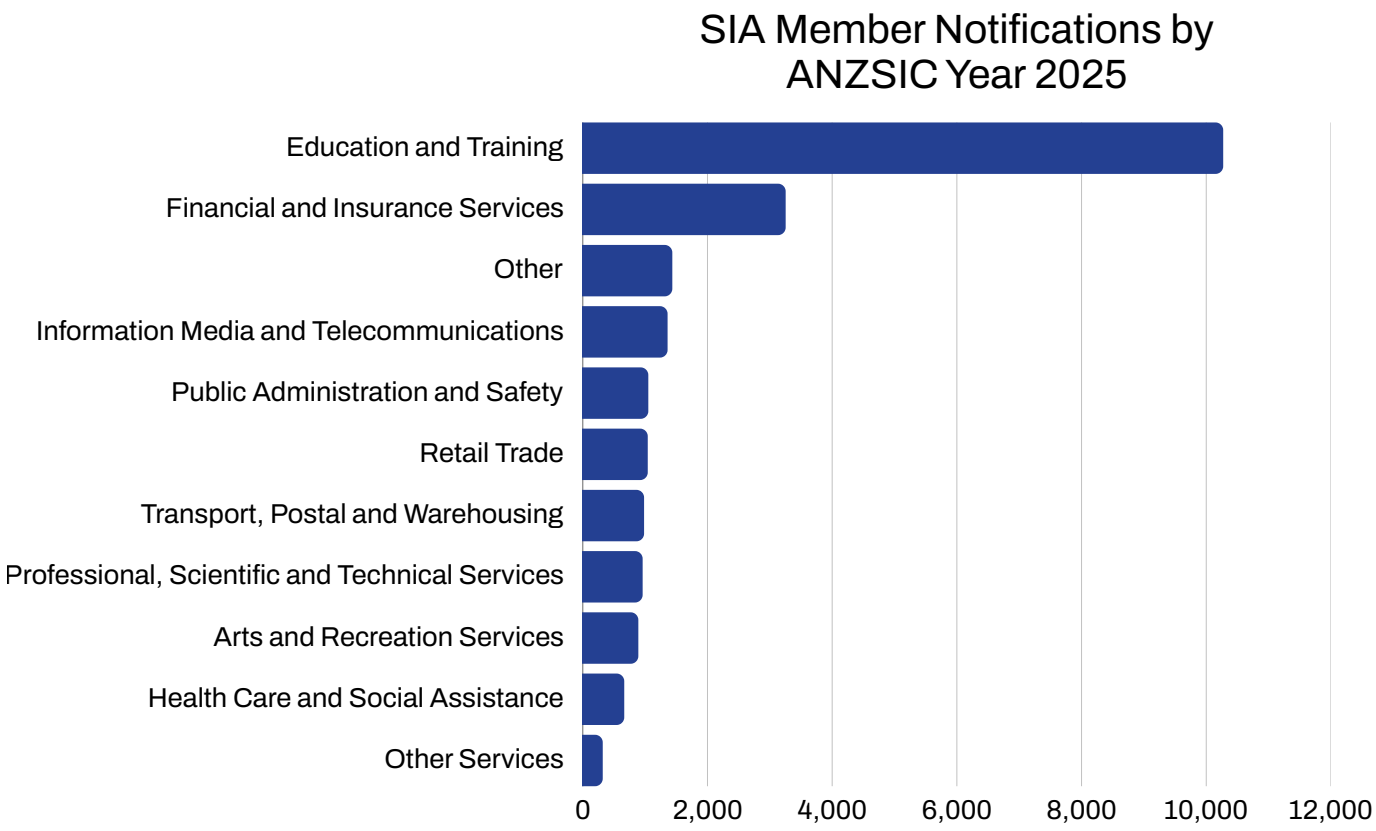
0.01 - 3.9: Low
4.0 - 6.9: Medium
7.0 - 8.9: High
9.0 - 10.0: Critical

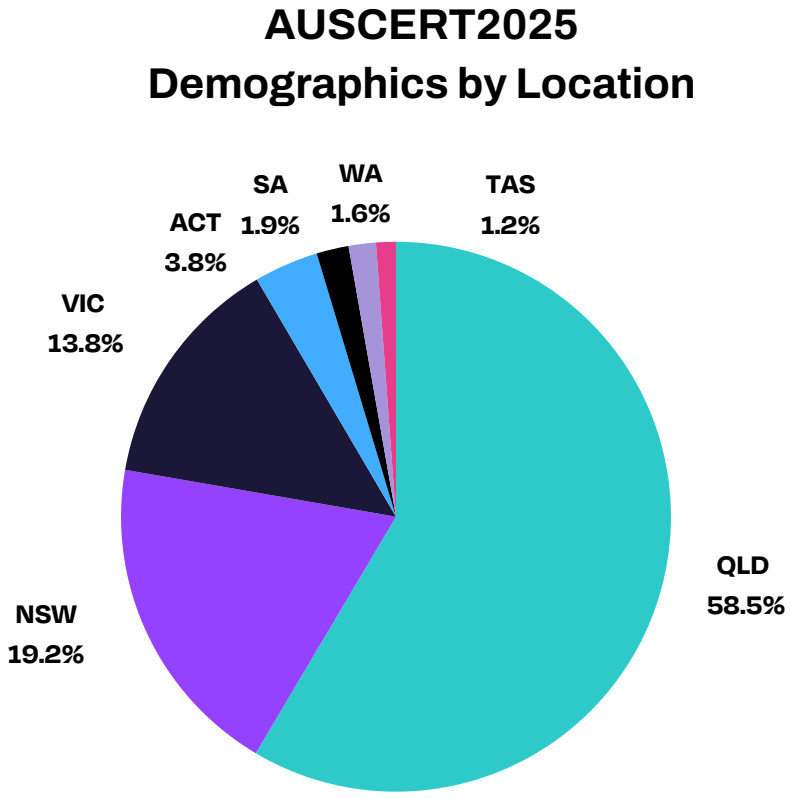
Appendix


MSIN Member Notifications by ANZSIC Year 2025
Education and Training
Information Media and Telecommunications
Professional, Scientific and Technical Services
Financial and Insurance Services
Health Care and Social Assistance
Other
Public Administration and Safety
Other Services
Arts and Recreation Services
Electricity, Gas, Water and Waste Services
Retail Trade
0
2,000
4,000
6,000
8,000
10,000


Critical MSINs by ANZSIC Year 2025
Education and Training
Financial and Insurance Services
Information Media and Telecommunications
Professional, Scientific and Technical Services
Public Administration and Safety
Transport, Postal and Warehousing
Health Care and Social Assistance
Arts and Recreation Services
Retail Trade
Other Services
Electricity, Gas, Water and Waste Services
Accommodation and Food Services
Manufacturing
Construction
Rental Hiring and Real Estate Services
Agriculture, Forestry and Fishing
Mining
Administrative and Support Services
Wholesale Trade
0
50
100
150
200
250
300
350

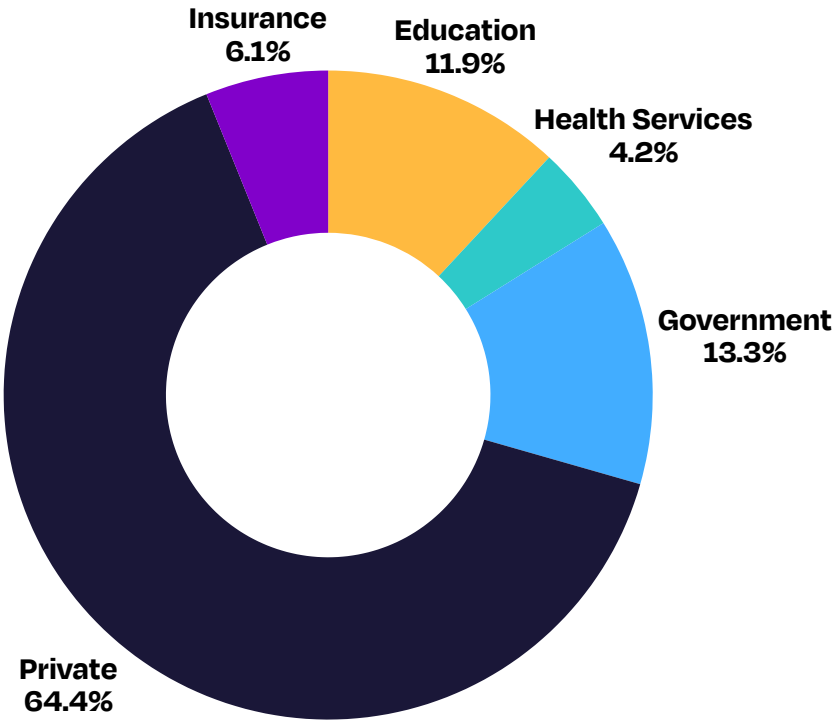
Appendix


SIA Member Notifications by ANZSIC Year 2025
Education and Training
Financial and Insurance Services
Other
Information Media and Telecommunications
Public Administration and Safety
Retail Trade
Transport, Postal and Warehousing
Professional, Scientific and Technical Services
Arts and Recreation Services
Health Care and Social Assistance
Other Services
0
2,000
4,000
6,000
8,000
10,000
12,000


AUSCERT2025
Demographics by Location
SA 1.9%
WA 1.6%
TAS 1.2%
ACT 3.8%
VIC 13.8%
NSW 19.2%
QLD 58.5%

Appendix

Demographics by Industry



Demographics by Position