AUSCERT

COMPUTER EMERGENCY RESPONSE TEAMS IN 2026: NOW AND BEYOND

A White Paper on the role of CERTs in the global fight against cyber-crime

January 2026

Contents

Executive Summary

This white paper examines the evolving role of **Computer Emergency Response Teams (CERTs)** in a rapidly transforming cyber threat landscape. It is authored by AUSCERT, drawing on over three decades of operational developments and cross-sector insights. It outlines the challenges CERTs face today and explores how their models, mandates, and coordination mechanisms must evolve to meet the demands of 2026 and beyond. It reflects our understanding of the evolving cyber coordination environment and is intended to support constructive dialogue about how CERTs can meet future challenges and respond in partnership with government, industry and academia, to these shifts, in a way that strengthens national and regional cyber resilience.

Once focused narrowly on incident response and aspects of vulnerability management, CERTs have broadened and shifted their scope, becoming an essential infrastructure for national, sectoral, and organisational cyber resilience. As digital transformation accelerates, these teams now operate in highly complex environments marked by regulatory fragmentation, supply chain interdependence, and persistent threat escalation. Yet their evolution has been uneven, with significant disparities in mandate, maturity, and strategic integration across regions and models.

CERTs now vary significantly in scope, structure, and governance. **National CERTs** serve as centralised coordination hubs. **Sectoral CERTs** focus on industry-specific risks. **Academic CERTs** contribute to technical depth and neutrality. **Member-funded models** support broad, cross-sector communities. While this diversity enables contextual responsiveness, it also contributes to a fragmented coordination landscape where goals diverge, roles overlap, reporting lines blur, and expectations differ across jurisdictions.

This paper provides a strategic analysis of the global development of CERTs, outlines the evolving expectations for CERTs in 2026, and compares their roles with related coordination bodies such as Information Sharing and Analysis Centres (**ISACs**), Organisations (**ISAOs**), and **national cyber security centres**. It also highlights AUSCERT's position as one of the longest-operating and most active CERTs in the Southern Hemisphere.

AUSCERT, as a member-funded and not-for-profit organisation, offers a distinctive model grounded in trust, independence, and technical credibility. Its continued relevance will depend not only on operational effectiveness but also on its ability to influence policy, coordinate across fragmented ecosystems, and deliver strategic value to its members and partners.

The paper concludes with practical recommendations for public and private stakeholders and outlines a strategic pathway for AUSCERT to strengthen its leadership in national, regional, and global cyber security resilience.

Reading Note

The roles and expectations placed on CERTs have expanded beyond technical response into policy influence, multi-stakeholder coordination, and cross-border risk management. Yet models for CERT governance remain highly varied, and clarity about their strategic value and operational positioning is often lacking.

This document is not a prescriptive framework, but **a strategic analysis and positioning paper**, grounded in practice and informed by the challenges faced by CERTs working independently of both government and commercial control. It is directed at multiple audiences: government policymakers, regulatory bodies, industry executives, sectoral coordination entities, international CERTs, and others involved in designing and sustaining cyber resilience frameworks.

AUSCERT recognises that no single model fits all contexts. Our intention is to offer this white paper as a resource to:

- Clarify the diversity of CERT typologies.
- Highlight coordination challenges.
- Articulate the strategic value of independent, member-driven CERTs.

It also provides insights into how AUSCERT's own structure, history, and cross-sectoral reach position the organisation to contribute to both national and regional resilience in a time of escalating cyber risk.

Acknowledgments

AUSCERT would like to acknowledge the work and contributions of all those who collaborated in preparing this white paper. In particular, a special acknowledgement goes to Edidiong James for her work in organising and structuring the significant amount of information this project started with.

1. Background: Origins and Development of CERTs

"Coming together is a beginning, staying together is progress, and working together is success"
(Henry Ford)

CERTs have been around for decades.

The concept emerged in 1988 as a direct response to the **Morris Worm**, a computer worm that exploited vulnerabilities in Unix systems and disrupted over 6,000 machines across the early internet[1]. The incident revealed a lack of formal mechanisms for vulnerability coordination and highlighted the risks posed by unregulated code propagation[2]. In response, the **United States Defense Advanced Research Projects Agency** (DARPA) funded the creation of the first CERT Coordination Center (CERT/CC[3]) at **Carnegie Mellon University**. CERT/CC became the blueprint for a new institutional model:

> *A technical team responsible for coordinating responses to cyber security incidents, issuing alerts, managing vulnerabilities, and facilitating communication among affected stakeholders.*

Following the establishment of CERT/CC, other response teams began to emerge globally. Notably, Australia played a formative role in this early expansion with the creation of AUSCERT (formally known as SERT), which was established in the early 1990s and is widely recognised as the second CERT in the world. Originating from a collaboration between three Australian universities, AUSCERT quickly developed close operational ties with CERT/CC and other early international teams, contributing to the foundational shaping of global incident response practices.[4]

As the terminology developed, the term *Computer Security Incident Response Team (CSIRT)* also gained traction, particularly outside the US. Despite recent attempts[5] to establish clear-cut boundaries between CERTs and CSIRTs' scope and functions (e.g., the former having a broader, proactive focus; the latter having a narrower, reactive one), functionally, CSIRTs and CERTs perform very similar roles. This includes handling security incidents, coordinating responses and support, and disseminating advisories. Moving forward, it can be confidently said that these functions will have even more similarities. There are also some important differences in nomenclature and branding.

The term ***CERT*** is a protected trademark of Carnegie Mellon University in several jurisdictions,

[1] https://www.sciencedirect.com/topics/computer-science/computer-emergency-response-team
[2] https://www.fbi.gov/history/famous-cases/morris-worm
[3] https://www.sei.cmu.edu/divisions/cert/
[4] https://auscert.org.au/blogs/2018-03-08-25-years-auscert/
[5] https://www.infosecurityeurope.com/en-gb/blog/guides-checklists/cybersecurity-structures-101-cert-csirt.html

including the US, and its usage requires permission. As a result, in the past, many organisations adopted the term CSIRT to describe similar teams without infringing on the trademark. In Europe, for example, the term CSIRT is more widely used, particularly in documentation by the European Union Agency for Cybersecurity (ENISA) and the Task Force CSIRT (TF-CSIRT) community[6].

In practice, both CERTs and CSIRTs provide **incident coordination, vulnerability handling, stakeholder communication, and technical support**. The differentiation is largely historical and legal rather than operational. Some organisations use both terms to describe different teams or functions within the same institution, while others have chosen one over the other based on regional preferences or branding strategy[7]. For the purposes of this white paper, the term CERT is used to refer to the broad category of incident response teams, acknowledging that CSIRT is an equally valid and often preferred designation in global contexts.

Throughout the 1990s and the early 2000s, the **CERT model proliferated internationally**. Many countries established **national CERTs** to support critical infrastructure protection, fulfil incident reporting obligations, and provide early warning capabilities[8]. In parallel, **sectoral CERTs** emerged in domains such as finance, health, energy, and transportation, often with mandates to address sector-specific threats and regulatory compliance needs. These CERTs were typically supported by industry associations, governments, or hybrid partnerships[9]. **Academic and research-based CERTs** also developed, often situated within universities or national research networks. These CERTs played a pivotal role in advancing technical tooling, open standards, and training.

An associated model, often under-recognised but increasingly relevant, is the **member-based CERT**. These teams operate on a subscription or pay-per-service basis, supported by a network of organisational members. Member-based CERTs are not government-funded or commercially owned. Instead, they provide cyber security services such as alerts, incident support, training, and threat intelligence to their members, who may come from public, private, or not-for-profit sectors, in exchange for a subscription fee. This model allows for **operational independence** and close alignment with **practical organisational needs**. It also creates space for **trust-based relationships** that are difficult to mandate through policy alone.

The early 2000s also saw the rise of **private** and **commercial CERTs** within multinational technology firms. Companies such as Microsoft and Cisco built internal response teams, not only to protect their own operations, but also to engage with the broader security community. These teams introduced new dynamics into the coordination landscape, particularly around information sharing and vulnerability disclosure policies, as their business models sometimes conflicted with open coordination principles.

[6] https://cisre.egr.uh.edu/wp-content/uploads/2023/09/csirt.pdf
[7] https://www.sei.cmu.edu/documents/1605/2003_002_001_14099.pdf
[8] https://www.newamerica.org/cybersecurity-initiative/policy-papers/csirt-basics-for-policy-makers/
[9] itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_3E.pdf

During this same period, several multilateral initiatives emerged to improve global coordination. The **Forum of Incident Response and Security Teams** (**FIRST**), established in 1990, became a key platform for professional development, community trust-building, and knowledge exchange.

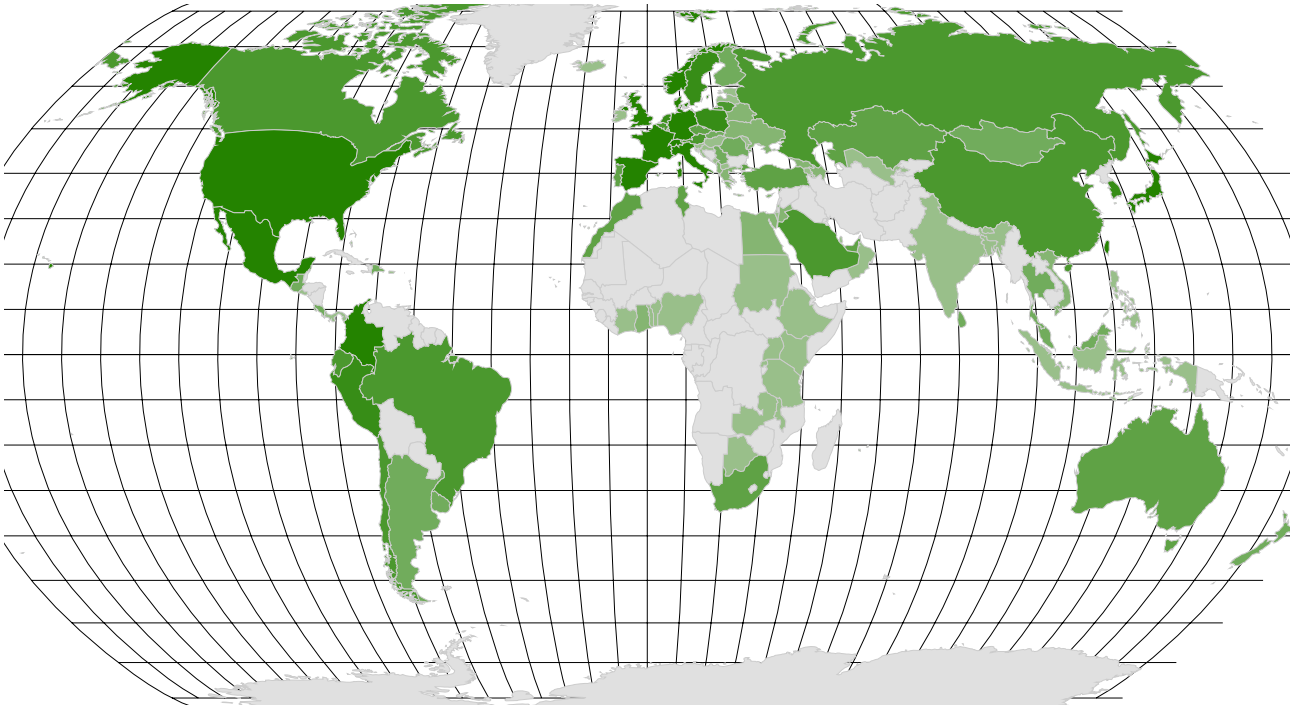

Figure 1: Countries with CERTs affiliated to FIRST (in green). Source: FIRST website.

As one of the oldest CERTs globally, AUSCERT was part of the early cohort of teams whose operational collaboration and trust-based information sharing helped shape FIRST's foundational model, contributing practical, non-US perspectives that reinforced FIRST's evolution as a genuinely international forum rather than a geographically concentrated one.

Other regional structures, such as the **Asia Pacific Computer Emergency Response Team (APCERT)**—of which AUSCERT is a charter member—and the **European CSIRT Network**, formalised mechanisms for regional cooperation, but varied widely in governance arrangements, scope, and operational maturity.

As of 2025, the **global CERT landscape** includes more than 800 teams affiliated with FIRST (Figure 1), and approximately 32 teams participating in the APCERT network. These statistics illustrate both the scale and fragmentation of the global CERT landscape.

Team	Official Team Name
Atlassian Detection and Response	Atlassian Detection and Response
AUSCERT	Australian Cyber Emergency Response Team

Australian Cyber Security Centre	Australian Cyber Security Centre
Deloitte-CICAU	Deloitte Australia Cyber Intelligence Centre
MON-CSIRT	Monash University Cyber Security Incident Response Team
Telstra T-CERT	Telstra Computer Emergency Response Team

Table 1: List of Australian teams affiliated with FIRST. Source: FIRST website.

Despite the growth of FIRST as a coordinating mechanism, significant **disparities** in CERTs' **capability**, **authority**, and **interoperability** remain[10] [11].

Some of them operate under formal authority with statutory mandates. Others are informal or voluntary collectives. Funding models also vary, with some CERTs fully government-funded, while others operate through member subscriptions and service agreements. The absence of a unified standard for **CERT governance**, combined with divergent expectations among stakeholders, has led to inconsistencies in strategies, modes of delivery, service quality, and public accountability[12].

Today, CERTs exist in most countries and sectors, but the absence of standard frameworks and their uneven evolution across regions have led to persistent variation in effectiveness. As cyber threats become more systemic, the limitations of fragmented coordination models are becoming more visible. Addressing these challenges requires a clearer understanding of the different CERT types, their strengths and constraints, and the conditions under which they can collaborate successfully.

2. Typologies and Governance Models

The diversity of CERTs worldwide reflects a **lack of uniformity** in how countries, industries, and institutions understand and operationalise cyber security response coordination. Although all CERTs share a core set of functions such as incident response or support, vulnerability coordination and information dissemination, their governance structures, funding mechanisms, and institutional affiliations vary considerably. These differences have practical implications for effectiveness, credibility, and stakeholder alignment. Table 2 summarises the most common typologies of CERTs. Two elements are worthwhile emphasising: first, these are the most common CERT models, but others could exist that are not included in the list; second, the models are not mutually exclusive, and several CERTs could have elements of various models.

[10] https://www.anao.gov.au/work/performance-audit/management-cyber-security-incidents
[11] https://www.sciencedirect.com/science/article/pii/S0167404823006090
[12] https://www.sciencedirect.com/science/article/pii/S0967070X23002330

CERT Type	Typical Host/Control	Funding Model	Key Services	Model features	Potential constraints	Examples
National	Government agencies or ministries	Government	National coordination, incident response, regulatory compliance	Authority, visibility, statutory mandate	Bureaucracy, neutrality, trust issues	CISA, JPCERT/CC, CERT-In
Sectoral	Industry bodies, regulators or associations	Industry	Sector-specific threat intel, training, incident coordination	Contextual knowledge, peer trust, alignment with sector risks	Narrow scope, sector silos, limited cross-sector vision	Austrian Energy CERT, Nordic Financial CERT, CERTFIN
Academic and Research-Based	Universities or national research networks	Institutional or grant-based	Technical research, institutional support, regional coordination	Technical depth, independence, research credibility	Funding, authority, strategy integration	SWITCH-CERT, DFN-CERT
Organisational	Private corps., NFPs, public sector	Internal budgets	Global response, vulnerability research, discretionary sharing	Tooling, speed, global reach, technical sophistication	Shareholder alignment, limited transparency, no coordination role	Microsoft Security Response Center, IBM X-Force Incident Response, MON-CSIRT
Member-Based	Independent entities or university-hosted bodies	Subscriptions, paid services	Threat intel, training, bulletins, incident response	Agility, neutrality, trust, cross-sector flexibility	No specific mandate, funding dependency, limited authority	AUSCERT

Table 2: Typologies of CERTs (most common)

The following section provides an overview of these models.

2.1 National CERTs

National CERTs are established and funded by **central governments**, often with formal mandates to protect national critical infrastructure, facilitate public-private coordination, and serve as a single point of contact for international incident notification. In many jurisdictions, the national CERT is integrated into the telecommunications ministry, cyber security authority, or national security apparatus. Examples include the United States Cyber Security and Infrastructure Security Agency (CISA), Japan's JPCERT/CC, and India's CERT-In.

These CERTs benefit from **statutory authority**, **stable funding**, and **high visibility**. They are

often able to compel incident reporting from regulated industries and act as intermediaries between public and private sectors. On the flipside, their functioning may rely more on bureaucratic structures than independent CERTs. This could lead to challenges in their engagement with external stakeholders, outside formal legal or policy-driven mandates. Moreover, there could be a perception that these CERTs operate as extensions of state surveillance or regulatory enforcement, which can hinder trust and cooperation with civil society and private sector. On this note, in recent years, these CERTs have invested significant resources in improving the visibility of their mandates and, overall, building trust in organisations and society in general.

2.2 Sectoral CERTs

Sectoral CERTs are specialised teams that address the cyber security needs of **specific industries** or **critical infrastructure sectors**, such as finance, energy, healthcare, transportation, and aviation. Typically established by industry regulators, associations, or over-arching bodies, these CERTs provide sector-specific threat intelligence, training, and incident coordination tailored to the operational context of their domain. An example is the Energy Sector CERT in the United States, which supports cyber security coordination across electric, oil, and natural gas providers.

A related form of sector collaboration are the **Information Sharing and Analysis Centers** (ISACs), or the **Information Sharing and Analysis Organizations** (ISAOs). Whilst **ISACs and ISAOs are not CERTs** themselves, they complement the role of sectoral CERTs by fostering real-time threat information exchange and resilience-building across industry stakeholders (see section 4).

The strength of sectoral CERTs lies in their **contextual knowledge** and close alignment with operational realities. They often enjoy high trust among member organisations due to shared risk profiles and regulatory frameworks. Their specialisation limits however their ability to gauge interdependencies across sectors, and this is by design. Multi-sector or national-scale incidents tend to be outside their remit. A reduced degree of fragmentation improves their effectiveness; hence, their impact is strongest in environments where industry self-regulation is well-developed, and compliance cultures are mature.

2.3 Academic and Research-Based CERTs

Academic CERTs play a prominent role in the creation and development of CERTs worldwide. These CERTs are hosted within universities or national research and education networks (NRENs), and are known for their technical depth, access to cutting-edge research, and institutional neutrality. They often serve both internal institutional needs and broader regional or sectoral communities. Examples include SWITCH-CERT in Switzerland and DFN-CERT in Germany.

The primary advantage of academic CERTs is their ability to act without the commercial or political constraints faced by private or government-run teams. Their credibility is often enhanced by their independence and their contributions to knowledge production and technical standards development. However, they frequently operate with **constrained budgets**, **limited formal authority**, and **varying degrees of integration** with national cyber strategies. Their long-term sustainability often

depends on the strength of their member base or the reliability of institutional support.

2.4 Private and Commercial CERTs

Large **technology firms** and **multinational corporations** can maintain internal CERTs that operate at a high level of technical sophistication. These teams often handle incident response across global infrastructure, engage in vulnerability research, and can participate in community-wide coordination efforts. Notable examples include Microsoft's Security Incident Response team (formerly DART/CRSP) and IBM X-Force Incident Response.

While private CERTs often lead in **speed**, **capabilities**, and **tooling**, their alignment with shareholder interests may limit transparency and trust. Their outputs may prioritise client services or brand protection, and their engagement in public coordination is usually discretionary. These CERTs contribute significant technical knowledge to the global ecosystem but are not structured to assume broader coordination responsibilities.

2.5 Member-Based and Subscription-Funded CERTs

Member-based CERTs operate independently of direct government control and are typically **funded through subscription models**, **voluntary participation**, or **industry partnerships**. These CERTs deliver a broad range of services, pre- and post-event (e.g., threat intelligence, vulnerability management, incident response or support, training). Their legitimacy often stems from **longstanding community trust**, **independence**, **technical reliability**, and their **ability to respond** directly to the needs of their members.

The strengths of the member-based CERT model include agility, institutional neutrality, and the ability to adapt quickly to emerging cyber security challenges. Unlike government-operated teams, these CERTs can often engage more flexibly across sectors and jurisdictions, particularly in contexts that may be diplomatically sensitive or bound by national regulations.

While they do not hold formal authority to compel action, their impact is grounded in their ability to influence through trust, expertise, and service excellence. Their potential to be exposed to significant budgetary pressures, associated with the need to maintain funding through service delivery, and growing competition, has made these CERTs a fertile ground for expansion of service delivery beyond incident response or support. As a result, several CERTs that adopt this model now encompass the broadest range of services: threat intelligence, vulnerability management, training and consulting-like engagements are examples of services these CERTs can deliver.

2.6 Hybrid Models and Emerging Variants

Many CERTs **combine features from multiple typologies**. For example, some national CERTs also provide services to private sector entities or maintain research partnerships with academic institutions. Others operate as consortia or federations, pooling resources from multiple stakeholders. Emerging variants include regional CERTs that coordinate multiple countries or sub-national CERTs created to manage risks at the regional, state or municipal level. The proliferation of

models reflects the adaptive nature of the CERT concept but also contributes to challenges in coordination and standardisation.

Recognising this diversity is essential for designing collaboration mechanisms that work across boundaries. The following section explores how the expectations placed on CERTs are evolving in 2026 and what this means for their strategic roles in cyber security ecosystems.

3. The Role and Expectations of CERTs in 2026

As mentioned, the **scope of responsibilities assigned to CERTs has expanded significantly over the past decade**. No longer confined to reactive incident response (which is becoming less of a focus for many), CERTs are now expected to serve as strategic enablers of national and sectoral cyber resilience. The role of a CERT in 2026 reflects a new reality: one in which cyber threats are persistent, sophisticated, and deeply embedded in the operations of government, industry, and civil society. Regulations are also becoming more stringent in the cyber security domain, which further exerts pressure on demand-side organisations and, therefore, CERTs. Similarly, **competitive pressures** are coming from traditional vendors and cyber security providers, such as Managed Security Services Providers (**MSSPs**): CERTs started operating at the dawn on the cyber security industry, as the only teams capable of responding to cyber-crises. Nowadays the landscape has profoundly changed, and **hundreds of players operate** in the same space as CERTs.

With this shift, CERTs face rising expectations in terms of responsiveness, transparency, leadership, and influence.

Modern expectations most CERTs must meet include:

- **Multi-stakeholder coordination:** CERTs are now expected to coordinate not just among technical peers, but across government agencies, industry partners, regulators, and the public. They must navigate institutional silos, legal constraints, and differing risk appetites while maintaining trust and neutrality.

- **Proactive threat intelligence:** Leveraging their innate capacity to act upon data breaches in a timely fashion, many CERTs are nowadays tasked with identifying emerging threats before they occur, conducting threat hunting, and disseminating forward-looking intelligence. This requires access to data, analytical capacity, and trusted information-sharing relationships.

- **Support for cyber policy implementation:** In many jurisdictions, CERTs are expected to assist with implementing cyber security strategies, regulatory compliance, and national critical infrastructure protection frameworks. This includes advising on sector-specific regulations, incident reporting thresholds, and response protocols.

- **Public communication and trust-building:** CERTs must now communicate, directly or indirectly, during crises, at times issue media statements, and engage with non-technical

audiences. Their credibility depends not only on technical competence but also on communication, transparency, responsiveness, and reputational integrity.

- **Interoperability and international engagement:** With cyber threats crossing borders, CERTs must be interoperable with global partners. This requires shared standards, compatible tools, and participation in transnational forums.

Undeniably, these expanded expectations have introduced **tensions**. CERTs are being asked to act faster, operate more transparently, and address more complex risks, often without commensurate increases in authority, resources, or legal clarity. The diversity of CERT structures compounds this challenge. For example, a member-based CERT may have the agility and trust to act quickly across sectors but may not have statutory access to sensitive data. Conversely, a national CERT may have legal authority but lack the operational trust of private stakeholders.

Despite these challenges, evolving expectations also create opportunities (Figure 2). CERTs can position themselves as **key convenors within cyber security ecosystems**, bridging public and private sectors, translating technical risks for policy audiences, and grounding **high-level strategies in operational realities**. To do this effectively, CERTs must continue to invest in technical capacity, stakeholder engagement, and governance models that align with their specific contexts.

Global alignment around a shared understanding of CERT roles is also becoming more essential. This includes clarifying what different types of CERTs can realistically deliver, identifying complementary roles, and ensuring that gaps in coverage do not become vulnerabilities. Standardisation efforts, regional frameworks, and capacity-building initiatives can support this

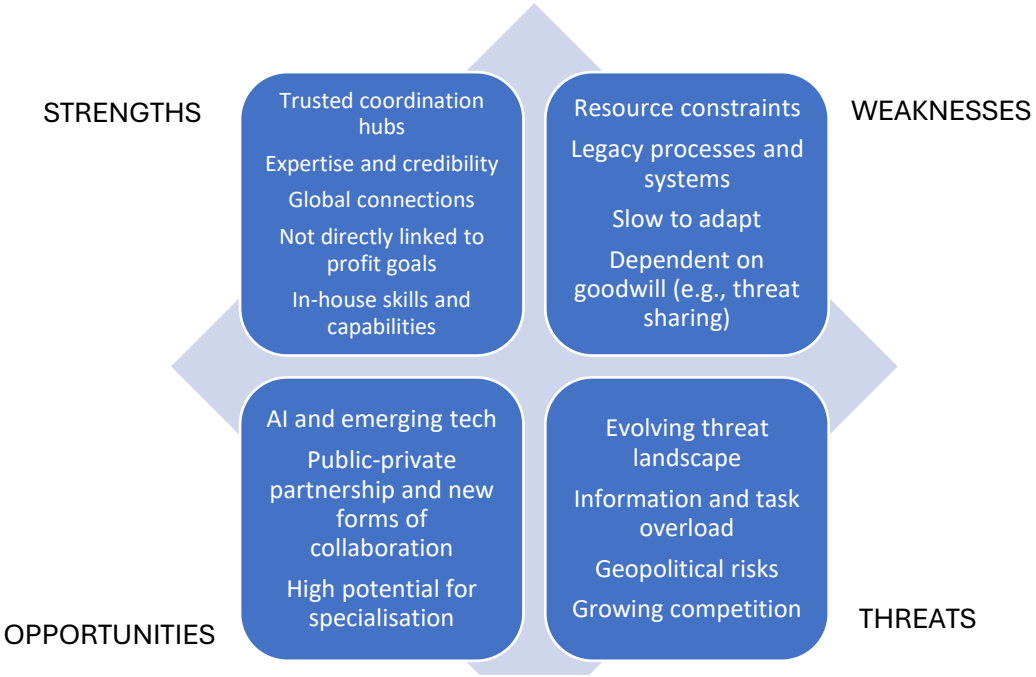

Figure 2: SWOT Analysis of CERTs in 2026

alignment, but must be flexible enough to accommodate the diverse forms CERTs take.

4. CERTs and Other Coordination Bodies

As the cyber security landscape has matured, a range of coordination bodies has emerged to support information sharing, incident response, and resilience planning across sectors. Among the most prominent are **Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs),** and **national or supranational cyber security coordination centers**. While these entities often work alongside CERTs, they are not synonymous with them. Understanding their distinct roles and institutional designs is critical for ensuring interoperability, avoiding redundancy, and supporting more coherent cyber response frameworks.

ISACs are sector-specific entities that facilitate information sharing among peer organisations within a defined industry. The financial sector, for example, has a well-established ISAC structure that enables banks, payment processors, and regulators to share intelligence related to fraud, phishing, distributed denial-of-service (DDoS) attacks, and other threats (Financial Services ISAC – FS ISAC). ISACs are not typically responsible for incident response. Their primary function is to build trusted communities of practice where information can be exchanged without fear of regulatory or reputational consequences. They often operate under safe harbor arrangements, which encourage disclosure and learning.

ISAOs represent a **broader and more flexible model**, intended to support information sharing across sectors, geographic regions, or stakeholder types. Unlike ISACs, which are generally aligned to critical infrastructure sectors, ISAOs may serve professional associations, small and medium-sized enterprises, or communities of interest such as healthcare professionals or manufacturing supply chains. The purpose of ISAOs is to lower the barrier to entry for collaborative cyber security, particularly for organisations that may lack access to national CERTs or sector-specific ISACs.

Cyber security Coordination Centers, by contrast, are typically institutionalised within national governments or supranational entities. Examples include the Australian Cyber Security Centre (ACSC), United Kingdom's National Cyber Security Centre (NCSC), the European Union Agency for Cyber security (ENISA), and Singapore's Cyber Security Agency. These centers often serve strategic functions beyond incident coordination. They may oversee national threat assessments, coordinate interagency exercises, develop policy guidance, and act as focal points for international cooperation. Whilst national CERTs often operate within these centers, the center itself is a broader institutional construct, designed to integrate technical, regulatory, and policy capabilities.

Each of these bodies fills a different niche in the cyber security ecosystem. CERTs bring technical credibility, rapid response capability, and coordination expertise. ISACs contribute sector-specific intelligence, deep contextual awareness, and trusted peer networks. ISAOs extend access to organisations that would otherwise be excluded from information sharing initiatives. Coordination centres have the broadest mandate and bring scale, authority, and political alignment.

Where these models are well integrated, they reinforce one another. CERTs can receive threat indicators from ISACs, validate them, and distribute advisories to a wider audience. ISAOs can amplify CERT communications within hard-to-reach communities and serve as a feedback channel for

emergent threats. National coordination centers can align all actors to a common strategic posture, ensuring that sectoral response does not crumble during crisis events.

However, overlaps could occur. In some countries, unclear delineation of responsibilities between these bodies could lead to confusion among stakeholders. Organisations may receive conflicting guidance or experience delays in incident triage due to duplicated reporting channels. These challenges underscore the need for clear definitions, documented protocols, and ongoing dialogue among coordination bodies.

5. The Australian Computer Emergency Response Team (AUSCERT)

Australia's entry into the computer emergency response ecosystem began in **1993** with the formation of the **Security Emergency Response Team (SERT),** a joint initiative between The University of Queensland, Queensland University of Technology, and Griffith University, in Brisbane (Queensland). This followed a widely publicised hacking incident involving a university student who, from Australia, gained unauthorised access to NASA systems, prompting the urgent need for formalised incident coordination in Australia[13]. The initiative responded to Australia's growing profile in international threat intelligence reports, both as a target of attacks and as the potential source of incidents affecting overseas systems.

Operational capacity in the early days was minimal, with incidents recorded manually in logbooks. Nevertheless, SERT established valuable relationships with global counterparts including CERT/CC in the United States and *Deutsches ForschungsNetz* Computer Emergency Response Team (DFN-CERT) in Germany. **On 1 April 1994, SERT formally became AUSCERT**, supported by Australia's Academic and Research Network (AARNet), which had recently begun providing national research network infrastructure. In the late 1990s, AUSCERT transitioned to a member-funded model mainly operating through organisational subscriptions (Figure 3).

Today, AUSCERT is based at, and supported by, The University of Queensland, and is one of the longest-operating CERTs globally and one of the oldest cyber security organisations in Australia. While it operates at a global level, AUSCERT is not a government CERT. Instead, it is a university-hosted, not-for-profit, member-funded organisation that maintains independence from both government control and commercial influence.

[13] https://auscert.org.au/about-us/

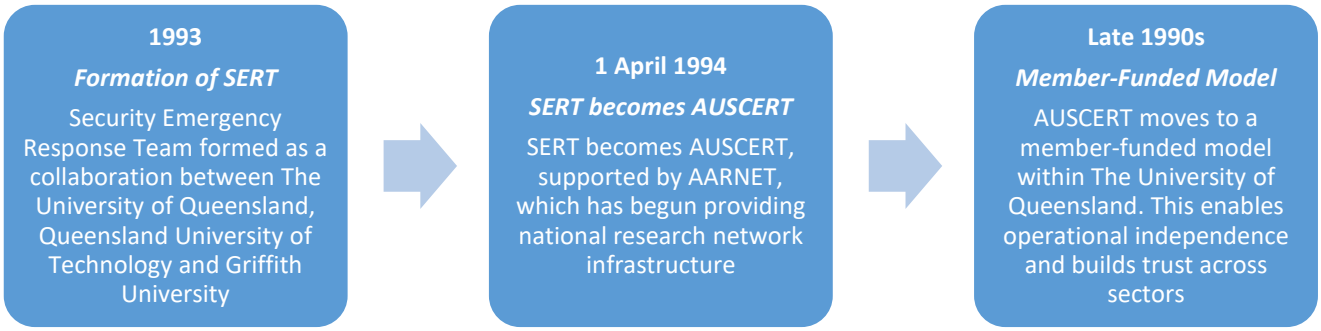

Figure 3: Evolution of AUSCERT

AUSCERT's member-based model forms the foundation of its service delivery, providing tailored threat intelligence, incident support, vulnerability management, Governance, Risk and Compliance (GRC) services, and training to a broad membership base, spanning 19 industries (ANZ Standard Industrial Classification). These include **critical infrastructure**, **higher education**, **healthcare**, **finance**, **government**, etc. AUSCERT's strength lies in timely engagement delivered by an experienced team with long-standing sectoral relationships and deep technical knowledge.

AUSCERT's operating model offers several comparative advantages. First, AUSCERT is **structurally autonomous**. It is not subject to political directives, national intelligence priorities, or commercial revenue incentives. This enables it to operate with neutrality, making it a trusted partner for sectors and jurisdictions that may be hesitant to engage directly with government CERTs or proprietary security firms. Its institutional setting within a public university reinforces this perception of impartiality and long-term credibility.

Second, AUSCERT maintains **strong relationships** with national and regional coordination bodies while preserving its operational independence. It collaborates with federal government bodies such as the **Australian Cyber Security Centre** or the **Australian Department of Foreign Affairs and Trade (DFAT)**, State-based entities (e.g. **Queensland Government**), as well as with other national CERTs and sectoral ISACs. AUSCERT also contributes to international information sharing communities such as FIRST and APCERT. Its position allows it to act as a connector between national strategy and sectoral implementation, translating broad cyber policies into operational advice for frontline entities. It is also capable of supporting CERT capacity-building internationally, particularly in economies where institutional development is still emerging. Recent examples include AUSCERT's support in the constitution of the Ethiopian CERT (Ethio-CERT) and its collaboration with institutions based in the Asia-Pacific area (e.g., Papua New Guinea and Fiji).

Third, AUSCERT is well-positioned to serve as a **resilience multiplier across multiple sectors**. Its member base includes several Small and Medium Businesses (SMEs), many of which lack dedicated cyber security teams. AUSCERT's services enable these organisations to access professional-grade support, benefit from shared threat intelligence, and obtain incident support without needing to invest in large internal security teams. This distributive function supports baseline

cyber security maturity.

However, AUSCERT's model is not without **limitations**. As a subscription-funded entity, it must continually demonstrate value to retain and grow its member base, an endeavor not traditionally associated with CERT mandates. This creates pressure to prioritise service quality, responsiveness, and tangible outputs. It also constrains its ability to scale quickly or absorb new mandates without corresponding financial support. While this discipline ensures a strong focus on performance, it may reduce strategic flexibility, particularly in responding to major national or regional crises that fall outside the direct service remit.

Another structural limitation is the lack of formal authority. Unlike national CERTs, AUSCERT cannot compel reporting, mandate participation in exercises, or enforce vulnerability disclosure timelines. **Its influence depends on trust, reputation, and voluntary cooperation**. In many cases, this has proven sufficient, but as regulatory frameworks evolve and cyber policy becomes more formalised, there may be greater demand for CERTs with defined legal mandates and enforcement powers.

Despite these limitations, a member-based model offers a compelling alternative to traditional CERT configurations. It demonstrates that independence, credibility, and agility can coexist with operational effectiveness. AUSCERT's recent focus on continuous improvement, consistent member engagement, and role in regional knowledge exchange validate the relevance of its approach. The key question is not whether AUSCERT can continue to deliver tactical services, but whether it can evolve into a more strategic actor capable of influencing cyber security outcomes across Australia and the broader Asia-Pacific region.

AUSCERT's contribution originates in the **operational/tactical** cyber security environments. Born with technical cyber security teams as main "clients", AUSCERT has in recent years expanded its scope to serve more **strategic and leadership** audiences (e.g., Senior Cyber security Managers, CISOs, boards, etc.), as well as non-technical ones, in particular through its GRC and training services. AUSCERT's services provide benefits across national-level contributions, strategic partnerships with executives and organisational leaders, and member-level operational support, directly and indirectly (Figure 4).

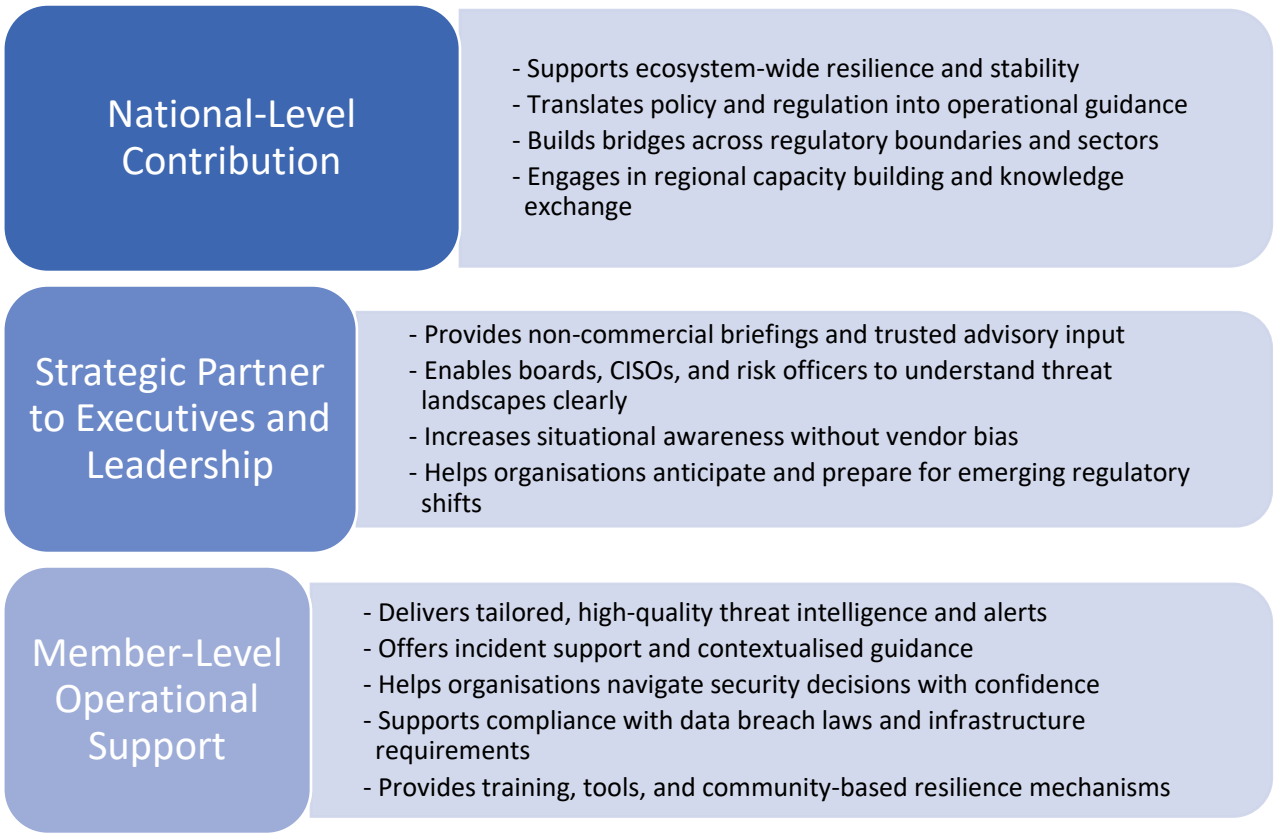

Figure 4: AUSCERT's impact at different levels

AUSCERT's future will be defined by how well its strategic partnerships and member relationships evolve. If its stakeholders recognise and support its unique role, it will continue to deliver high operational value while growing its strategic influence. If they treat it solely as a service provider, its ability to contribute to broader resilience objectives may be constrained. The choice is not AUSCERT's alone. It is a collective decision, with implications for national coordination, sectoral strength, and organisational security outcomes.

6. Conclusion

The CERT model was born from technical necessity but has since become a strategic fixture in global cyber security ecosystems. Over three decades, CERTs have evolved from ad hoc response teams into institutions with **critical roles in incident coordination**, **intelligence sharing**, **capacity building**, and **policy influence**. Yet, as the threat landscape continues to evolve, the CERT community faces renewed questions about its relevance, structure, and ability to scale.

The current ecosystem is complex and often fragmented. CERTs operate under different mandates, funding models, and governance frameworks, potentially leading to inconsistent coordination, overlapping responsibilities, and strategic blind spots. While this diversity allows CERTs to adapt to local needs, it also creates ambiguity for policymakers, members, and international partners. It is no longer sufficient to focus only on technical excellence. The CERTs of 2026 must

demonstrate strategic maturity, institutional trustworthiness, and the ability to navigate multi-stakeholder environments. The future of coordination requires more than incident triage and technical bulletins. It requires institutions that can engage with government without being controlled by it, serve members without being captured by them, and speak across jurisdictions without being limited by them.

This evolution will not happen by default. It will require deliberate action from multiple stakeholders. The next phase of cyber coordination in Australia and the Asia-Pacific region will be shaped by how governments, regulators, and industry partners choose to collaborate for the overall cyber security uplift.

Learn More About AUSCERT

Founded in 1993 and based at The University of Queensland, AUSCERT provides threat intelligence, vulnerability management, incident support, training, and GRC services to hundreds of organisations across the Asia-Pacific region and beyond.

As a not-for-profit organisation, AUSCERT operates independently of government or commercial ownership. This enables us to build trusted relationships across sectors, respond flexibly to emerging threats, and contribute meaningfully to national and regional cyber resilience.

AUSCERT's services are trusted by critical infrastructure operators, universities, hospitals, financial institutions, and small-to-medium enterprises. We are an active participant in global coordination networks such as FIRST, APCERT, and the Australian Cyber Security Centre (ACSC) ecosystem, and regularly contribute to international knowledge-sharing efforts.

AUSCERT continues to work with members, partners, and stakeholders to strengthen cyber security coordination across sectors. We welcome enquiries, feedback, and strategic dialogue.

To learn more about AUSCERT or to enquire about collaboration, membership, or partnership opportunities, please contact us or follow our updates:

Website: www.auscert.org.au
Email: auscert@auscert.org.au
LinkedIn: linkedin.com/company/auscert
Twitter (X): @AUSCERT
Phone: +61 7 3365 4417
Postal Address: AUSCERT, The University of Queensland, St Lucia QLD 4072, Australia

Appendix: Coordination entities in cyber security ecosystems

Entity Type	Definition	Core Functions	Strategic Role in Ecosystem
CERT (Computer Emergency Response Team)	Broad-constituency team, often national or sectoral; coordinates cyber incident response and readiness	Alerts, coordination, public-private engagement, awareness, vulnerability advisories	Serves as a backbone for large-scale coordination, trusted contact point, and policy-technical bridge
CSIRT (Computer Security Incident Response Team)	Organization-level team for incident response, detection, and internal readiness	Incident triage, containment, vulnerability management, post-incident learning	Core to enterprise defense; links internal risk response with national or sectoral bodies
SOC (Security Operations Centre)	Monitoring-focused operational unit for real-time threat detection	Network/system surveillance, alert triage, escalation, tool management	First-line detection and containment; feeds into CSIRT and CERT coordination workflows
ISAC (Information Sharing and Analysis Centre)	Sector-specific threat intelligence hub, usually non-profit and member-based	Threat sharing, sector reports, secure portals, cross-member learning	Sector-wide situational awareness, supports trusted sharing among peers and with government
ISAO (Information Sharing and Analysis Organization)	Flexible, community-based intelligence exchange collective	Inclusive threat sharing, best practice dissemination, lightweight coordination	Expands access to cyber intelligence for non-traditional stakeholders; complements ISACs and CERTs
TIP (Threat Intelligence Platform)	Software platform for aggregating, correlating, and operationalizing threat intelligence	Data enrichment, automation, real-time alerting, integration with SOCs/CSIRTs	Enables scale and consistency in intelligence workflows; technical bridge between threat feeds and operations
Fusion Centre	Multi-agency hub	Intelligence fusion, joint	Enhances cross-domain

	integrating cyber, physical, and criminal threat intelligence	coordination, predictive analysis	threat detection and response; useful in large-scale or blended threat contexts
Coordination Forum	Community or network for collaboration, standards, and trust-building (e.g. FIRST, APCERT)	Best practice frameworks, incident classification, mentoring, advocacy	Strengthens community trust and interoperability; supports collective capacity-building and crisis alignment

Further readings

DCAF – Geneva Centre for Security Sector Governance (2023)
Introduction to Computer Security Incident Response Teams (CSIRTs): Structures and Functions of Cybersecurity's First Responders ISBN: 978-92-9222-695-4
https://www.dcaf.ch/sites/default/files/publications/documents/Guidebook_for_new_CSIRT_employees_EN_09032023.pdf

Dykstra, J., Gordon, L. A., Loeb, M. P., & Zhou, L. (2023).
Maximizing the benefits from sharing cyber threat intelligence by government agencies and departments. *Journal of Cybersecurity*, 9(1), tyad003 https://doi.org/10.1093/cybsec/tyad003

ENISA – European Union Agency for Cybersecurity
CSIRTs by Country – Interactive Map
https://tools.enisa.europa.eu/topics/incident-response/csirt-inventory/certs-by-country-interactive-map

Exabeam
CSIRT vs. CERT: Similarities, Differences, and 8 Examples of CERTs
https://www.exabeam.com/explainers/information-security/csirt-vs-cert-similarities-differences-and-8-examples-of-certs/

Forum of Incident Response and Security Teams (FIRST)
Incident Management Team Types: CSIRTs, ISACs, PSIRTs, SOCs – Services Framework
https://www.first.org/standards/frameworks/csirts/FIRST-services-framework-team-types-v071.pdf

Liska, A. (2014)
Building an Intelligence-Led Security Program – Chapter 8: CERTs, ISACs, and Intelligence-Sharing Communities ISBN: 9780128021453
https://www.oreilly.com/library/view/building-an-intelligence-led/9780128021453/B9780128021453000089/B9780128021453000089.xhtml

Smith, F., & Ingram, G. (2017)
Organising cyber security in Australia and beyond. *Australian Journal of International Affairs*, *71*(6), 642-660.
https://www.tandfonline.com/doi/abs/10.1080/10357718.2017.1320972

Tanczer, L. M., Brass, I., & Carr, M. (2020).
CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy.
Global Policy, 11(3), 336–345.
https://onlinelibrary.wiley.com/doi/epdf/10.1111/1758-5899.12625