



Information Management

Infosys Cybersecurity integrates a robust strategy with a comprehensive framework - SEED and a strong governance program to ensure optimal protection. The strategy is designed to minimize Cybersecurity risks and align to our business goals. It focuses on proactive enablement of business, besides ensuring continual improvement in the compliance posture through effective monitoring and management of cyber events. We believe that an effective security culture would complement our cybersecurity objectives by reducing enterprise risks. Infosys Cybersecurity program ensures that required controls and processes are implemented, monitored, measured, and improved continuously to mitigate cyber risks across domains.

Positioned as a leader in ISG
Provider Lens™

Infosys is committed to

- Protecting the confidentiality, availability, and integrity of information assets from internal and external threats
- Ensuring and maintaining stakeholders trust and confidence about Cybersecurity

The executive Cybersecurity governing body is in place to direct and steer:

- Alignment of Cybersecurity Strategy and policy with business and IT strategy.
- Value delivery to stakeholders.
- Assurance that cyber risks are being adequately addressed.

Approach

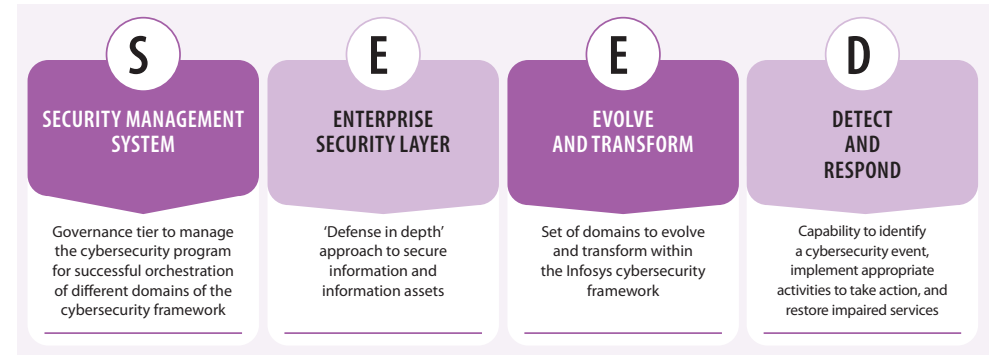
WHAT	SECURE BY DESIGN	SECURE BY SCALE	SECURE THE FUTURE
WHY	<ul style="list-style-type: none"> • Maximize visibility • Minimize risk • Early engagement 	<ul style="list-style-type: none"> • Optimize cost • Amplify reach • Rapid development 	<ul style="list-style-type: none"> • Innovate faster • Deliver value • Thought leadership
HOW	<ul style="list-style-type: none"> • Awareness and culture • Security architecture • DevSecOps • Intuitive dashboards • Compliance 	<ul style="list-style-type: none"> • Platforms and accelerators • Integrated and optimized • Automation • Managed security service • Academic collaboration 	<ul style="list-style-type: none"> • Competency building • Research and innovation • Co-created partner solution • Emerging technologies

Cybersecurity Strategy and Governance

The high-level objectives of the Cybersecurity program at Infosys are:

1. A Proactive business security and employee experience
2. Continuously improve security posture and compliance
3. Effective management of cyber events and,
4. Building a security culture

Infosys' Cybersecurity framework is built basis leading global security standards and frameworks such as the National Institute of Standards Technology (NIST) Cybersecurity framework and ISO 27001 which is structured around the below four key areas:



The framework also entails a comprehensive Cybersecurity maturity model which helps to ascertain the Cybersecurity maturity as well as benchmark against industry peers on an ongoing basis. This helps in continued oversight and commitment from the Board and Senior Management on an ongoing basis through

the Information Security Council (ISC) and the Cybersecurity sub-committee.

In keeping with the 'defense in depth' philosophy, we have deployed several layers of controls to ensure that we keep ours, as well as our clients' data, secure and thereby always uphold stakeholders' trust.



Cybersecurity Management and Reporting

The cybersecurity practices at Infosys have evolved to look beyond compliance. The comprehensive cybersecurity metrics program has been contributing to the continuous improvement of the existing security practices and integration of cybersecurity within the business processes.

Information management, being an essential part of good IT governance, is a cornerstone at Infosys and has helped provide the organization with a robust foundation. Care is taken to ensure that standardized policies or guidelines apply to and are practical for the organization's culture, business, and operational practices. Cybersecurity requires participation from all spheres of the organization. Senior management, information security practitioners, IT professionals, and users have a pivotal role to play in securing the assets of an organization. The success of cybersecurity can only be achieved by full cooperation at all levels of an organization, both inside and outside and this is what defines the level of commitment here at Infosys.

As a final level of defense, we undergo many internal audits as well as external attestations and audits in a year at an organization level (e.g. SSAE-18 SOC 1 & SOC 2 Type II, ISO 27001). We also undergo client account audits to assess our security posture and compliance against our obligations on an ongoing basis.

There was no material cybersecurity incident reported in fiscal 2025.

Our industry contributions and thought leadership

In this era of rapid technology disruptions and digital transformations, Infosys enables the businesses to embrace innovations and adapt to new technologies. We focus on strengthening cyber resiliency through platform led convergence and consolidation of security capabilities and deliver AI-first service offerings.

We promote cybersecurity through various social media channels such as LinkedIn, Twitter, and YouTube; sharing our point of views, whitepapers, service offerings, articles written by our leaders, their interviews stating various perspectives, and podcasts through our corporate handles providing the cybersecurity thought leadership. The topics include impact of evolving technologies such as GenAI on cybersecurity, cloud security, data privacy and protection, and compliance, etc. In addition to this, we work with analysts such as PAC

Group and industry bodies such as Data Security Council of India (DSCI), Information Security Forum (ISF), etc. to create joint thought leadership that is relevant to the industry practitioners. In our efforts to strengthen cyber awareness across social communities, we also participate in cybersecurity awareness initiatives led by non-profit organizations such as NASSCOM. Further, we publish a technology centric report that provides insights into emerging technology trends and how they can be applied to businesses. It essentially acts as a guide for enterprises looking to navigate the evolving digital landscape and make informed technology decisions based on current trends. We also host various global chapters of Infosys regularly that aim to be a catalyst for innovation and transformation in the cybersecurity domain. The distinguished members of the council collaborate to discuss, strategize, and prepare roadmaps to address the current security challenges of member organizations and help decipher the evolving industry trends. We, therefore, through various channels, drive awareness of and appreciation for cybersecurity.

Vulnerability Management

The vulnerability management program at Infosys follows best-in-class industry practices coupled with top-notch processes that have been evolving over the years. Rich experience of deftly managing the end-to-end vulnerability life cycle of Infosys Network and the constant hunger to stay abreast of the latest tools, technologies and related market intelligence have acted as a catalyst in fortifying the overall vulnerability management program.

A robust enterprise vulnerability management program builds the foundation for healthy security hygiene of an organization. The following practices have been put in place at Infosys for,

1. Real time asset discovery followed by instantaneous identification of vulnerabilities, misconfigurations, and timely remediation
2. Automation of vulnerability management, configuration compliance, security assessments and review for assets, applications, network devices, data, and other entities in real time
3. Close coupling of detection and remediation processes; auto prioritization to reduce the turnaround time for closure of detected vulnerabilities
4. Continuous monitoring of all public facing Infosys sites and assets for immediate detection of vulnerabilities, ports, or services
5. Regular penetration testing assessments and production application testing for detection and remediation of vulnerabilities on a real time basis



The vulnerability remediation strategy of Infosys focuses on threat-based prioritization, vulnerability ageing analysis and continuous tracking for timely closure. We have successfully eliminated the ticketing system for vulnerability tracking by establishing a continuous detection and remediation cycle, where the IT teams are enabled and onboarded onto the vulnerability management platform. A Cybersecurity awareness culture is nurtured, and teams are encouraged to proactively remediate the vulnerabilities reported on their assets or applications.

Supply Chain Cyber Risk Management

A comprehensive supplier security risk management program at Infosys ensures effective management of potential security risks across the various stages of supplier engagement. The process comprises:

- Categorization of the suppliers based on the nature of the services provided and the sensitivity of the data involved.
- Defining standardized set of information security controls as applicable to each category of supplier
- Defining, maintaining, and amending relevant security clauses in the supplier contracts as applicable to each category of supplier
- Due diligence, security risk assessment for effective management of the information security risks associated with suppliers

Defining and monitoring of key security metrics for suppliers (e.g., background check, security awareness training completion, timely interventions with regard to information security incidents etc.) threat intel tracking and governance further strengthen the Infosys supplier security risk management program.

Cybersecurity Competency Development

With the increasing demand for cybersecurity jobs and a skilled workforce, Infosys has taken several measures to counter the cybersecurity talent shortage as well as in skilling, retaining, and diversifying its security workforce in areas such as application security / secure development lifecycle.

Cybersecurity team members undergo technical as well as behavioral training on an ongoing basis. Infosys leverages internal training programs, as well as external bodies / agencies with cybersecurity subject matter expertise, with a strong focus on learning through the classroom as well as on-the-job training.

- Over 2400 professionals were trained & 1900 certified across various cybersecurity domains. These training programs consist of advanced partner programs from OEM, external agencies and internal Cybersecurity training facilities.
- Over 1400 professionals have been trained in AI and other new age technologies.
- Launch of Cyber Aspire Program, as part of which various professionals are trained in niche Cybersecurity domains. Along with this, structured curriculum for freshers and various bridge programs have been launched for upskilling and cross-skilling of cyber professionals.
- Infosys continues its partnership with NIIT to have its professionals undergo a Cybersecurity Master's Program.

Nurturing, and Upholding, a Robust and Sustainable Cybersecurity Culture

At Infosys, driving a positive and sustainable cybersecurity culture is one of the key constituents of our robust cybersecurity strategy. We embrace top-notch tools and technology to strengthen our cybersecurity stance and have an equally razor-sharp focus to bolster people's security and keep fostering a security-first mindset among Infosians. Various measures are in place to nurture a confident and empowered cybersecurity culture. At Infosys, we embrace the Secure by Design (SbD) principles at an organizational level with a focused SbD campaign running org-wide, and multiple trainings offered to drive awareness on SecureSDLC. There are various other diverse and proactive communication campaigns driven across the organization via different awareness means / tools, including – posters, cyber comics, employee handbook, caselets, cybersecurity scorecard, newsletter, advisories, emailers, push messages, annual mandatory awareness quiz, gamification, SME Cyber Talks, information security courses on the internal training platform, sessions, videos, podcasts, fireside chats, blogs, panel discussions, focused social engineering awareness, thought leadership messages, annual flagship event -celebrating the cybersecurity week etc. There is also a video-based, animated, and interactive e-Learning certification program that helps drive positive security behavior

amongst the Infosians.

Innovations for our clients

Infosys innovation-led offerings and capabilities:

Infosys Cyber AI, powered by Infosys Topaz, helps customers amplify their defender potential, build effective cyber defenses and enable accurate decision making by leveraging platform-centric GenAI capabilities. We help enterprises Renew, Re-Architect and Re-imagine their entire cyber strategy through AI with a focus on risk resilience. This helps us become a trusted cybersecurity partner for enterprise customers.

Cyber Next platform powered services help customers stay ahead of threat actors and proactively protect them from security risks. Our pre-engineered packaged and AI powered managed security services help monitor, detect and respond by getting extensive visibility and actionable insight through threat intelligence and threat hunting. Our offerings ensure risk-based vulnerability management by providing a comprehensive single pane of glass posture view. Recent development in our Cyber Next platform is the integration of AI powered capabilities that enhances service delivery. We have merged some of the modules within Cyber Next platform and have also introduced some new modules to offer cybersecurity solutions relevant in the era of AI. Service modules include - Cyber Watch, Cyber Scan, Cyber Compass, Cyber Protect, Cyber AI that ensure



comprehensive Managed Protection Detection and Response (MPDR) for our global customers.

Zero Trust Security architecture and solutions to navigate our customers to embrace zero trust security. Key innovations and offerings include Secure Access Service Edge (SASE) delivered as-a service. With SASE as-a Service, we ensure strengthened overall security through cloud delivered security controls and capabilities. Infosys innovation in policy standardization enforce controls at access level, accelerating rollout of service thereby reducing or eliminating legacy tools allowing our customers to reduce overall costs while enhancing end-user experience.

Secure Cloud transformation with Cobalt assets drives accelerated cloud adoption. With Secure Cloud reference architecture and Secure by Design principle we ensure security is embedded as part of cloud strategy, design, implementation, operations and automation.

Industry Recognition

Analyst recognition

- Positioned as a Leader in the **ISG Provider Lens™** Cybersecurity Services and Solutions (2021, 2022, 2023, 2024)
- Positioned as a Leader in the **Nelson Hall** Cyber Resiliency Services NEAT Assessment 2023
- Positioned as a Leader in **Everest PEAK Matrix®** Assessment Identity and Access Management (IAM) Services 2023
- Received the **ISG Provider Lens Award 2024** for our domain expertise and presence in the Americas, UK and Germany markets

Analyst testimonials

- “Infosys’ CyberSecurity Capabilities are a Testament to their Relentless Pursuit of Excellence,” says Gautam Sampath, Principal Security Analyst at Information Services Group (ISG)
- “Infosys’ CyberSecurity Portfolio is a Strong Choice,” says Gautam Sampath, Principal Security Analyst at Information Services Group (ISG)

Client testimonials

- Strengthening Cybersecurity: BECU leaders’ insights on the impact of Infosys Collaboration
- Cummins and Infosys: Securing Identities Together
- Infosys provides Managed Protection, Detection and Response to bpost (Belgian Post Group)
- Infosys secures MS Amlin’s digital transformation journey
- Infosys and Ferroglobe: Journey towards a robust and secure cyber landscape
- Ferroglobe partners with Infosys to secure their OT Security Environment

Partner awards

- Received the **Saviynt APJ Regional Delivery Partner of the Year 2024** for our innovation and excellence in leveraging Saviynt’s Identity Cloud to solve complex identity security challenges.
- Received the **Zscaler GSI Growth Partner of the Year 2024** award for our unwavering commitment to delivering exceptional business outcomes and enhancing Zero Trust implementation
- Acknowledged as the **Microsoft Security Solutions Partner** across all 4 domains demonstrating our cutting-edge expertise in deploying Microsoft Security solutions
- Acknowledged as the **AWS Competency Partner** across seven domains exhibiting our in-depth technical expertise in AWS security and delivering tailored, security-focused solutions for specific workloads and use cases