INFORMATION SECURITY

MASTERING THE SPECTRUM OF RISK
INFORMATION SECURITY AT ACCENTURE

Protecting data of Accenture, its clients, and employees is a 24/7 job that requires dedicated people, strategies, processes and technologies. Accenture’s Information Security organization does this and more, keeping a constant eye on today’s changing security and risk landscapes, evolving technologies, as well as expanding regulatory environments across every business location.

Our Organization

Client Data Protection
A global Client Data Protection (CDP) team helps to ensure the safety of the client information and systems entrusted to Accenture. The CDP processes require all client teams to implement a control regime derived from ISO 27001, with continuous monitoring and oversight by the CDP team.

Incident Response
The Cyber Incident Response Team (CIRT) manages data-related incidents, from proactively assessing Accenture’s digital enterprise to leveraging world-class forensic technologies to remediate issues. The team also uses industry-leading threat intelligence to detect and defend against malicious cyber activity.

Technology Infrastructure
The technology team identifies, deploys and runs security technologies that strengthen defenses to protect client and Accenture data. Over half a million end-points are monitored and fortified, along with numerous data centers and cloud environments.

Governance, Risk & Compliance
Accenture’s cyber governance, risk and compliance team continually measures and improves its effectiveness with a focus on regulatory and business risk, as well as threat intelligence—ensuring a risk-resilient enterprise.

Learning and Communications
The behavior change team embeds an understanding of information security into Accenture’s culture with interactive, immersive training programs using video dramatization and gamification, so workers act to keep client, employee and Accenture information secure.
Accenture’s Information Security organization is a global team of over 750 security professionals charged with protecting company, client, and employee data. The team’s expertise spans technical architecture and security operations, governance and risk management, threat intelligence, compliance, and incident management. The team also provides strong leadership in support of Accenture’s security technology investments, business processes, communications and behavioral change programs, aimed at incident prevention and the establishment of an overall culture of working smart to stay safe.

The Information Security team manages formal governance relationships with Accenture’s Legal, Data Privacy and Business Continuity functions. The group also maintains strong relationships with law enforcement agencies, third-party security advisors, and the information security organizations of clients and suppliers.

Certifications & Endorsements

ISO 27001:2013* is the security standard awarded by the British Standards Institution (BSI) that serves as international certification for companies that adhere to the highest and strictest postures.

Accenture’s ISO 27001 certification, current to date, validates that its processes and security controls provide an effective framework for protecting client and company information. Accenture also holds BSI’s ISO 27701 certification established to uphold global data privacy regulations and personally identifiable information (PII) across its enterprise and client service businesses. Accenture is one of the first organizations—and the largest global organization—to achieve this expanded certification. The BSI standards cover Accenture’s entire global operations delivering services to clients in over 120 countries.

In addition to receiving the largest single certification ever awarded by BSI, Accenture’s approach to information security has been validated by other entities:

• Global Data Protection Regulation (GDPR) readiness endorsement from Morrison & Foerster
• Cyber Essentials Plus endorsement from BSI, required for suppliers to the UK government
• Outperformed peer group in top-tier, third party security benchmarking
• Rated as highest “Role Model” in all 23 categories of the NIST Cybersecurity Framework (CSF) by BSI
• Rated “Fully Implemented,” the highest possible level, for all 20 control categories in the Center for Internet Security (CIS) Critical Security Controls by Verizon Security Services

*The ISO/IEC 27000 family of standards helps organizations keep information assets secure. https://www.iso.org/isoiec-27001-information-security.html
The Information Security group keeps Accenture risk-resilient with a strategy that ensures Accenture maintains a fortified security posture, addressing today’s challenges while also preparing for new issues tomorrow might bring.

The team works to close the gap between a security compromise and the time it takes to respond. Security is embedded into the core of Accenture through policy, process, and education, supported by leadership and a workforce that puts security first. A common information security language is used across all parts of the business with a shared culture of stewardship focused on protecting information. Technology investments are made to further enable real-time detection and response, as well as to anticipate future disruptive technologies.
CLIENT DATA PROTECTION
& INCIDENT RESPONSE

Client Data Protection
Safeguarding client data is one of the most fundamental and critical responsibilities at Accenture.

The Information Security team has developed, and continually evolves, a global Client Data Protection (CDP) program that ensures client teams understand and comply with data privacy and security obligations relevant to each client engagement. The program arms the teams with tools and processes that enable them to identify and mitigate security risks over the lifecycle of a client project. CDP provides client teams with a standardized approach to protect client data that includes:

- Clear accountability for information security within each client engagement
- Controls that protect client data when it is being accessed, handled, transmitted, hosted or stored, as well as service-specific controls tied to risks inherent in specific types of work
- Technology to protect client data including hard drive encryption, workstation configuration scanning, and data loss prevention protection
- Client team-specific training that incorporates unique client requirements and addresses project-specific risk factors
- Subject matter expertise that shares leading practices and regularly reviews the effectiveness of client team security processes and controls

Key CDP metrics are included in the global management metrics that are reviewed each month by Accenture’s senior leadership including the CEO and COO.

Incident Response
Accenture’s Cyber Incident Response Team (CIRT) monitors and manages a broad security landscape. Highly trained professionals provide 24/7 coverage and can deploy on site anywhere in the world, in most cases within a matter of hours. Incident response plans are rehearsed monthly, and two of these drills are managed by security specialist third parties. Simulations may cover both internal and external scenarios. A specialized group within this team continually tests Accenture defenses by simulating attacks against the company’s digital infrastructure.

Confidently Responding to Global ‘WFH’ Requirements
Prior to COVID-19, almost 200,000 Accenture workers delivered services on a daily basis working remotely. Now, the vast majority of our half million employees are set up to securely work from home (WFH) in all countries where Accenture operates. We were able to quickly reinforce behavior and training programs with updated, customized communications that addressed COVID-19-specific threats and issues. Already using established ISO* controls and processes, we were able to quickly validate our client project teams were addressing WFH risk appropriately and consistently.

*The ISO/IEC 27000 family of standards helps organizations keep information assets secure. https://www.iso.org/isoiec-27001-information-security.html
Technology Infrastructure
Accenture generates billions of data interactions daily, transmitting information through various networks, platforms and systems. Keeping technical infrastructure and data secure while allowing employees the appropriate flexibility to be successful is a continual challenge, especially among Accenture’s globally dispersed workforce, which as of March 2020 has almost entirely been working from their homes.

Accenture’s central infrastructure has over 350 data centers and hosting locations, housing approximately 50,000 servers and 6000 network devices. Accenture’s Security Operations Center (SOC) uses some of the most advanced security technologies to monitor and hunt threats across the enterprise, that in turn help implement solutions at speed and scale. This steadfast approach to fortification has earned Accenture a positive reputation among third party risk assessors; specifically, Accenture ranks top amongst its peers in maintaining a strong defense against threats, as rated by the leading cyber security benchmarking vendors in each risk category.

Governance, Risk & Compliance
The risk of malicious and accidental acts inside Accenture’s environments cannot be fully eliminated. However, the team maintains a broad yet highly focused framework of risk management controls, policies, processes and metrics that are implemented across the enterprise in order to set expectations, measure outcomes and drive change to:

- Establish top-down accountability for owning, prioritizing and protecting critical assets
- Maintain line of sight to all people and security-related processes and technology
- Ensure that our best practices are deployed everywhere consistently
Accenture’s behavior change program consists of a comprehensive, mandatory employee training program supplemented by voluntary and incentive-based training that is delivered through global and local channels. Information Security and Data Privacy training are provided at the time of hire and continue for the duration of employment.

The Information Security Advocate program goes well beyond standard corporate compliance training. It consists of several voluntary and engaging learning activities that increase employee adoption of information security best practices to protect Accenture, employee and client data. Typically, over 90% of Accenture employees consistently complete this program, achieving Information Security Advocate status and embracing stronger security behaviors.

The team conducts bi-annual, anonymous surveys of employees from all parts of the organization to understand workers’ adoption rates of information security practices and protocols; the behavior survey is supplemented with quarterly social engineering tests of our entire organization.

Industry Recognition

Accenture’s information security behavior change programs have garnered industry recognition for their use of innovative approaches and their impressive results.

Chief Learning Officer Magazine Learning Elite
• 2019 Learning Elite Gold and Winner’s Circle awards for IS Advocate Program

CSO50
• Named a 2019 CSO50 Winner for Social Engineering Awareness Program

Association for Talent Development:
• 2019 ATD Excellence in Practice award for IS Advocate Program

Cannes: Corporate Media & TV Awards
• 2018 Silver Awards for “Hacker Land” video series

Brandon Hall Group
• 2018 Silver Excellence Award in Learning for IS Advocate Program
• 2016 Gold Excellence Award in Learning for overall security learning program
About Accenture
Accenture is a leading
global professional services
company, providing a broad
range of services in strategy
and consulting, interactive,
technology and operations, with
digital capabilities across all
of these services. We combine
unmatched experience and
specialized capabilities across
more than 40 industries —
powered by the world’s largest
network of Advanced Technology
and Intelligent Operations
centers. With 513,000 people
serving clients in more than 120
countries, Accenture brings
continuous innovation to help
clients improve their performance
and create lasting value across
their enterprises.