Schrems II @ Accenture

March 2022

Schrems II @ Accenture

At Accenture, meeting the highest ethical standards is paramount.

We maintain a global data privacy program closely aligned to GDPR standards and treat privacy as a fundamental right for all individuals, and therefore take the protection of the personal data we handle for us and on behalf of our clients very seriously.

While we already have a strong program in place to address data privacy, the European Court of Justice (ECJ) July 2020 decision, known as “Schrems II,” requires organizations to take further actions around protection. Specifically, organizations are to assess and identify if, when moving personal data to most countries outside of the European Economic Area (EEA), there is a risk the information can be accessed and ultimately exposed to foreign authorities. Should an increased risk of exposure exist, specific “supplementary measures” to mitigate the risk need to be applied.

In response, Accenture has assessed our current compliance approach and standards, consulting with our external legal counsel to confirm our process addresses the Schrems II requirements. We have also strengthened our business-as-usual process, assessed relevant country laws and performed Transfer Impact Assessments where Accenture is an exporter. Our ISO 27001 and ISO27701 certified Data Privacy and Information Security programs have been reviewed to ensure they address the European Data Protection Board (EDPB) recommendations on supplementary measures.

Based on our review of the relevant laws, as well as the standard supplementary measures and controlled clauses we’ve embedded into our process, we believe we are well positioned to continue to deliver our services in a manner consistent with how we do today. Understandably, there still may be questions and concerns not addressed within this overview. We remain readily available to communicate and work closely with you, our client, to ensure everyone is aligned in driving privacy compliance.

Certified secure

Ready for Schrems II

Accenture maintain a global data privacy program closely aligned to GDPR to enable a consistent, global standard to address client and business data protection.

This has enabled us to achieve and maintain **ISO 27001 and 27701** certifications of our enterprise data privacy and client data protection programs.

Accenture's ISO-certified Enterprise and Client Data Protection programs embody our steadfast dedication to information security and are reinforced by our standings with other industry standards organizations.

Finally, all Accenture people are required to participate in award-winning programs focused on instilling smart security and data protection practices.

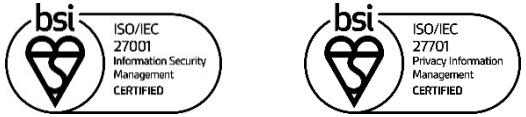
Security is in our DNA.

NIST Cyber Security Framework (CSF)

Assessed as "at" or "exceeding" in all categories against its peer and industry verticals by BSI

ISO 27001* and 27701*

Maintains certification for information security and data privacy standards



CIS Critical Security Controls Version 7.1

Maintains at or above its peers and industry verticals in all 20 categories, validated by Verizon Security Services

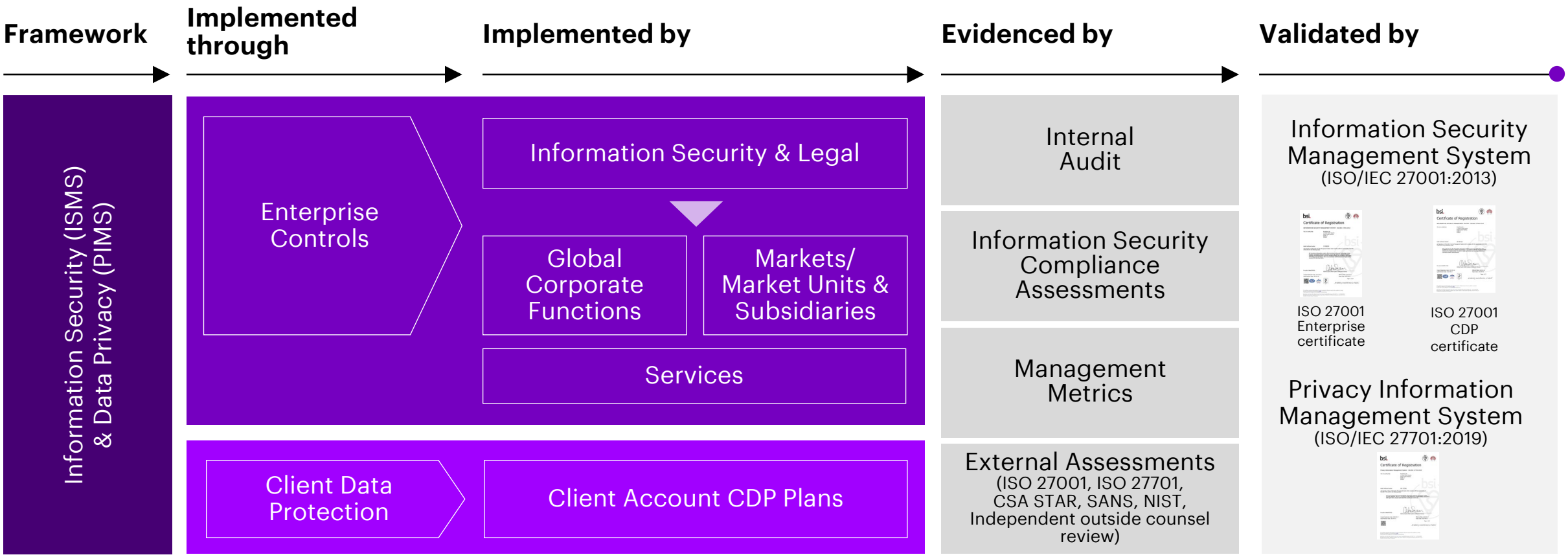
CSA Security, Trust & Assurance Registry (STAR)

Awarded, and maintains, the highest Gold-level certification for Accenture-managed cloud infrastructure and certification of CIO cloud services (to be extended across all cloud services)

*The ISO/IEC 27000 family of standards helps organizations keep information assets secure.
https://www.iso.org/isoiec-27001-information-security.html

Accenture IS and DP management systems

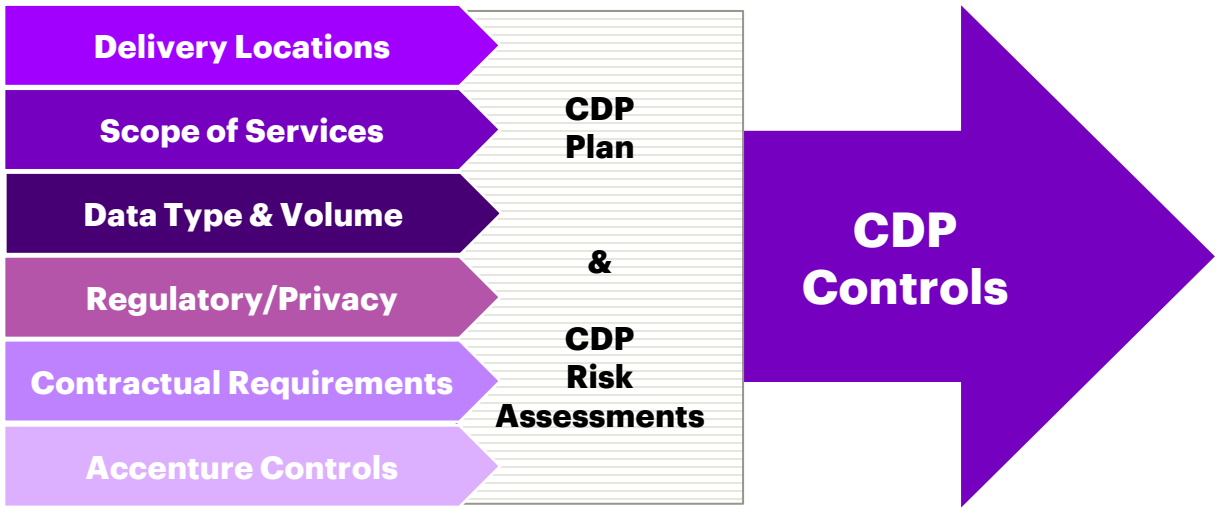
Representing a standardized, information-centric framework implemented across the entire Accenture environment covering information security (IS) and data privacy (DP). Information Security and Privacy Information Management Systems share complementary security and data privacy controls. The Client Data Protection (CDP) program supports the IS and DP ISO certification programs.



Client data protection

Our Client Data Protection [**CDP**] program provides project teams with a standardized approach to managing risk through a set of processes, controls, and metrics. This **ISO 27001/27701 certified** program focuses on safeguarding client data.

> **Protecting client data is essential to maintaining client trust, and that trust is the cornerstone of every one of our client relationships.**



Real time visibility to 1.1 million controls covering over 45K client contracts

- Access Logging
- Accountability
- Administrator Access
- Approved Devices and Tools
- Change Management
- Cloud
- Content Moderation
- Data Disposal
- Delivery Locations
- Disaster Recovery
- Encryption and Storage of Data
- Environment and Config Mgmt
- Environmental
- Firefighter ID
- Firewall, Antivirus & IDS/IPS
- Foxtrot
- General Infrastructure / Hosting
- Least Privileged Access
- Legal/Contractual
- Logging & Monitoring
- Managed Security Service
- Movement of People Between Engagements (Roll-on/Roll-off)
- Password Management
- Physical Security
- Reuse of Work Products
- Secure Application Development
- Security Incident Reporting
- Subcontractors
- Training
- Transmission of Data
- User Access Management
- Vulnerability Management

Information security technical architecture

ENDPOINT

- Hard Disk Encryption
- Endpoint Protection
- Endpoint Malware Response
- Email Client Security
- Application Blacklisting
- Patch Management
- Endpoint Web Filtering
- Mobile Device Management Solution
- Workstation Rights Control
- Workstation Compliance
- Host IPs
- Endpoint Tolling

NETWORK, INFRASTRUCTURE, CLOUD

- Network Perimeter
- Remote Access
- Vulnerability Management and Configuration Compliance
- DDoS Protection
- Native Cloud Protections for AWZ, Azure and Google
- Container Security and Scanning
- Security Configuration Management of Network Devices and Cloud Platforms
- Web Filtering
- Network Access Control
- Security Information and Event Management

DATA

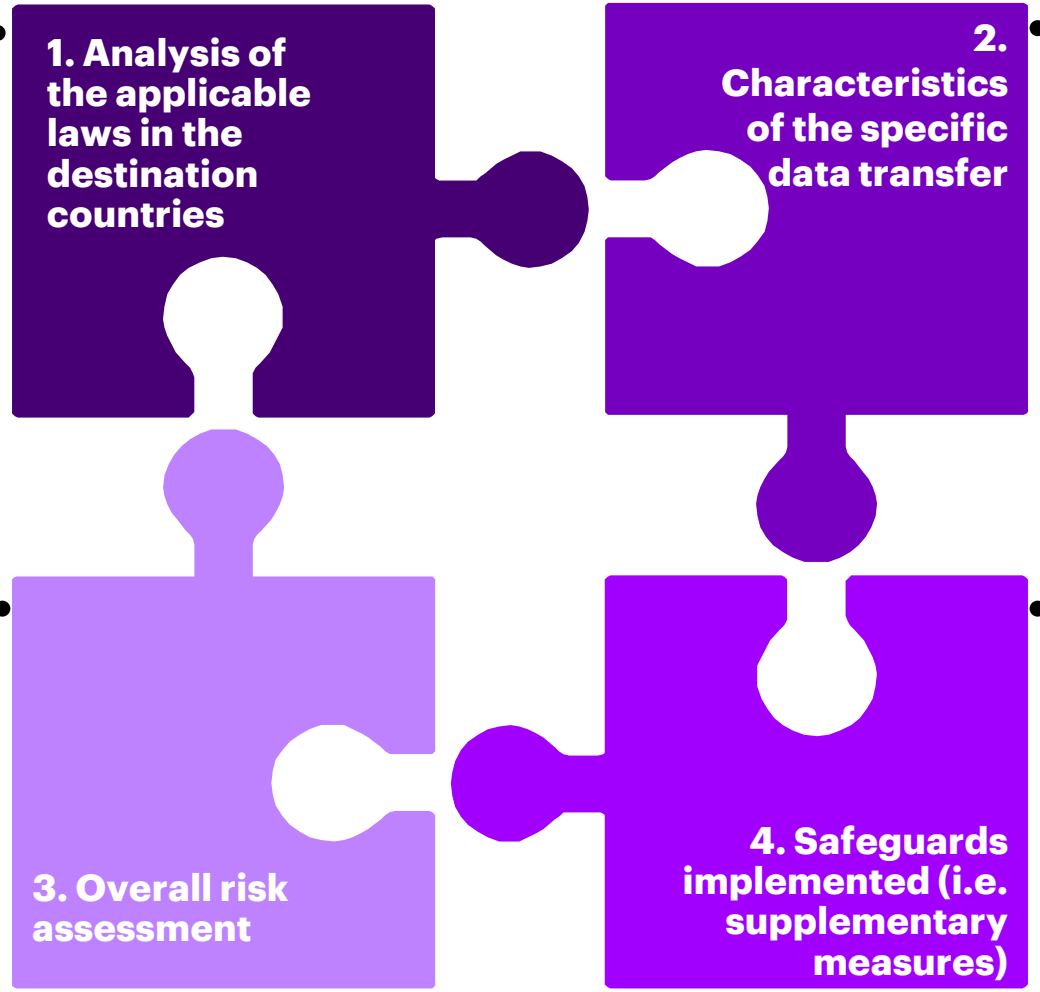
- SecureErase
- Information Rights Mgmt. & Classification
- Email and Endpoint DLP
- Cloud Application Security
- Web Application Firewall
- O365 Security: Email, SharePoint, OneDrive, MS Teams
- Secure Analytics and Threat Intelligence
- Web and Mobile Application Scanning
- Governance, Risk and Compliance Tools (GRC)

IDENTITY

- Device Aware Authentication
- Multi Factor Authentication
- Single Sign - On & Federated Identity Management
- Privileged Access Management
- PKI & Certificate Management

Transfer Impact Assessments (TIA)

- A review of relevant laws and practices of a destination country to assess if they are clear, proportionate, have effective remedies and independent oversight.
- Review if relevant requests for disclosure were received from public authorities.



Includes the:

- Types of data
- Entities involved and their industry sectors
- Purposes of transfer/processing
- Any onward transfers
- Storage vs access
- Circumstances of the transfer
- Regularity
- Physical transfer or access only

Considering the characteristics of the data transfer and the laws of the Third Country, understand the risk profile of the proposed transfer.

Where needed, technical, organisational or legal measures to ensure that the protection for people whose personal data is transferred to a destination country where protection for individuals is essential.

Overview of Accenture's Supplementary Measures

TECHNICAL MEASURES

- **Proper Encryption Algorithm and Key Management Strategy**

- **Privileged Access Management**
- **Data Leakage Prevention**

- **Data Classification**

- **Logging & Monitoring**

ORGANIZATIONAL MEASURES

- **Internal Policies –** set allocation of responsibilities

- **Minimization Measures –** assess to identify personal data strictly necessary for the transfer

- **Transparency Measures** – documentation of requests to data importers available

- **Standards and Best Practices –** e.g. data security and privacy policies; ISO Norms; ENISA

LEGAL MEASURES

- **Certification re**: lack of back doors/similar programming easing the access to personal data

- **Implementation of procedures for changes in law notification and swift suspension of the data transfer**
- Agreement **on notifications to clients** where permitted

> Click here for a full set of Technical and Organization Measures, including all our standard Supplementary Measures

Award-winning employee security training

All Employees – Global IS Advocate Training Program

Driving global awareness and adoption of secure behaviors with interactive, gamified learning.

- Top 10 critical 'security hygiene' behaviors addressed through continuous learning through tiered, quarterly releases
- Customized content driven by KPIs and industry trends
- Data-driven program is continually measured and adjusted based on internal metrics and external benchmarks

High Priority Groups – Targeted IS Training Tracks

Targeting key topics for high-risk groups such as new hires, technology delivery roles, Leadership, HR, and others.

- Focused on role-specific information security content
- Priority to instill a secure mindset and accountability for security
- Seamless integration with IS Advocate global curriculum

Client Account Roles - Client Data Protection (CDP) Training

Improving effectiveness and compliance of CDP through role-specific security training for critical roles.

- Actionable guidance on key CDP processes and controls
- Custom content based on client-relevant scenarios
- Agile support on critical IS issues and emerging threats

By the numbers:

20+ Awards

Hacker Land web series viewed 3.2M times

98% of Accenture employees are IS Advocates

Addressing DP/IS risk in supplier contracts

Accenture's approach to supplier contracting includes a thorough due diligence process in order to identify DP/IS risks to be addressed contractually and monitored operationally through the life of the contract.

The 5-step approach to supplier security management

1

Conduct Data Privacy, Transfer Impact Assessments and Information Security Risk Profiling Evaluation

2

Determine level of supplier IS risk – 1 of 3 ratings - Low, Above Normal and High

3

Conduct a Supplier Security Assessment (SSA) for suppliers with heightened levels of IS risk

4

Agree to security controls, operational processes and – where required- supplementary measures in the supplier contract

5

Monitor supplier performance through the life of the contract. Correct non-compliance

Monitoring supplier security performance

Through the life of the contract, an Accenture business contract owner is accountable for managing supplier related information security risks, monitoring the agreed-upon supplier information security contract controls and supplementary measures, and closing non-compliance remediation activities resulting from supplier assessments.

FAQ

What has Accenture done to address geographical regulatory requirements?

GDPR started several waves of country-specific data privacy regulatory movements. As we implemented GDPR as a global baseline. Our Information Security and Data Privacy organizations work together under the direction of our Chief Compliance Officer, Chief Operating and Chief Information Security Officers to design and implement programs that address data privacy and information security requirements across our global enterprise, including our client services business and which supplement as necessary with country specific requirements.

Processing client personal data
Accenture is mindful of, and fully understands, our clients' duties to comply with the requirements of applicable data privacy legislation particularly where services may be performed outside of the countries where the data subjects reside.

To confirm **compliance with international data transfer requirements**. Accenture is willing to enter into specific additional agreements to enable clients to comply with international data transfer regulations.

Accountability
Senior-level responsibility for data protection and mandatory program adoption.

Privacy by Design and Default
Embed Privacy by Design and Default into the design and architecture of solutions.

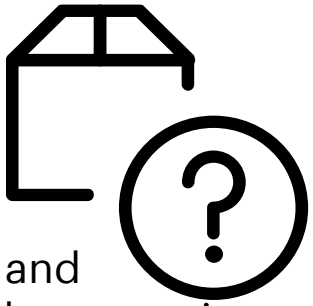
Purpose of limitation regarding the use of data
Limiting the collection and use of personal data to only those purposes for which Accenture was specifically contracted.

Notice
Confirming that appropriate privacy notices have been provided and following client instructions when providing such notices on clients' behalf.

Individual rights
Implementing processes into solution or application design based on our clients' instructions gives individuals the ability to access, view, correct, and/or delete collected personal data.

Data transfers
Establishing data transfer agreements with clients as appropriate when data originating from certain countries (the European Union and European Economic Area), is being transferred to another country. Generally, Accenture serves as a data processor when providing services to clients, we use privacy-related controls to manage the use of personal data as agreed with clients and monitor those.

How does Accenture prepare for potential government requests for client data?



To the extent Accenture is able to share such information, Accenture has not been subject to a broad and indiscriminatory request for personal information from national security or intelligence authorities in the countries we operate within the past 36 months.*

To prepare for future eventualities, Accenture has expanded its proven and tested incident management approach and procedures to also cover government requests for personal information. Should we receive any such request defined broad and indiscriminate government request for personal information, the request is tracked through a central intake process and managed centrally by Accenture´s specialized legal and forensics teams and under the supervision of the Director of Cybersecurity and Data Integrity.

As a matter of principle, Accenture will not hand over personal data without a valid government order or warrant and it will take reasonable steps to challenge a government order or a warrant if Accenture´s specialized internal teams and external advisors identify legal deficiencies with such order or warrant.

If a government request relates to client data for which Accenture is the processor, Accenture will notify the client of the request and align potential further steps with the client unless applicable law prohibits a disclosure or immediate action is required. If Accenture is prohibited to inform the client, it will request that the government or authority will inform the client directly.

Accenture will maintain a log of governments requests and will provide regular reports to Accenture Leadership.

*as of March 2022

What has Accenture done to comply with the new transfer requirements?

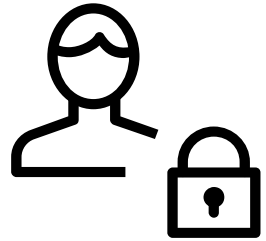
Country Assessments:
Accenture regularly carries out assessments of law and practices of the more than 30 not adequate countries Accenture transfers personal data to, and we share a summary of those with our clients upon request. Working with external and local Accenture legal professionals, Accenture has made risk determinations for each country. These assessments serve as one source of insights when we perform Transfer Impact Assessments.

Transfer Impact Assessments:
Accenture has completed and will continue to complete Transfer Impact Assessments as required. Our Transfer Impact Assessments look among others at the type and volume of personal data involved in the transfer, the services that will be executed, and countries those services will be delivered from.

We use the result of those inputs to validate that our measures are appropriate for each transfer. We recognize that in some cases, additional measures may be needed, and guidance is provided to support the team engaged in performing the Transfer Impact Assessment to understand what other potential measures would help secure the transfer.

Updating EU Standard Contractual Clauses (SCCs)
We are working with our vendors and clients to update EU Standard Contractual clauses (SCCs) within the transition period. We are working closely with our providers in ensuring they are also taking appropriate actions to enable compliance with the ruling.

How does Accenture protect against someone inadvertently or intentionally moving data to where it shouldn't go?



As part of everyday business operations, Accenture uses **Data Loss Prevention** (DLP) technologies across workstations that in turn drive DLP processes for Accenture workers (unless prohibited by locally**).

Activities scanned by DLP technologies include uploading to cloud storage sites, copying or sharing data through websites, USB sticks and printing. DLP also scans all outbound Accenture e-mail sent via Microsoft Outlook, Outlook Web Access (OWA) and Outlook Mobile Access (OMA).

In addition to DLP, Accenture uses a tool which enables URL blocking and prevent Accenture workers from connecting to untrusted sites.

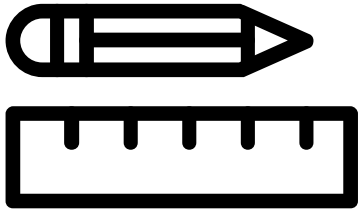
USB ports on workstations are either prevented from writing to removable media or restricted to only writing to media encrypted by ***Bitlocker to Go***, depending on the employee's role. (Certain employees that work in creative agency roles have open use of USB as their client collaboration needs demand it.)

Finally, within our **Client Data Protection** (CDP) program, we work closely with our clients to look for additional ways to protect against the movement of - or our exposure to - data. The controls can result in the following outcomes:

- Masked or de-identified data
- Additional more restrictive DLP policies that trigger on client specific keywords
- Requirements that all data is always stored on client-controlled systems
- If Citrix or VDI environment is provided by the client, confirmation that those systems are set to block offloading of data

***Accenture uses DLP for information security and data protection purposes in accordance with applicable laws and internal policies.*

How does Accenture monitor and measure the effectiveness of its information security management program?



Management metrics

The Accenture Information Security organization regularly shares and reviews key information security metrics on processes, technology and behavior with key business leaders to understand performance and agree on any corrective actions. Common performance metrics include security incidents, Client Data Protection (CDP) performance, acquisition integration as well as network, infrastructure and application vulnerabilities.

Information security compliance assessments

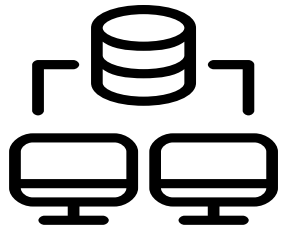
Accenture uses a multi-step model to ensure ongoing compliance to the tenants of our programs:

1. Key metrics exists within the CDP program along with defined reviews to ensure ongoing compliance on a daily, weekly and monthly basis
2. The CDP program utilizes the assessment team within Information Security to validate the effectiveness of the control implementation
3. The Accenture Internal Audit group performs additional reviews as a neutral party to help validate the strength of the management of the CDP Program and the overall effectiveness of the control model
4. External assessments are performed by BSI on a quarterly basis to validate current practices which enable continuous certification to ISO27001 and ISO27701.
5. External assessments are performed by our Clients to validate current practices and alignment to contractual terms. These assessments help corroborate that Accenture's practices are well aligned to industry requirements.

How does Accenture protect data when it's being transmitted?

As part of everyday business operations, Accenture tools use modern encryption protocols for secure transmission of information. Scans are conducted to look for insecure protocols like so remediation can take place. The key areas of encryption are:

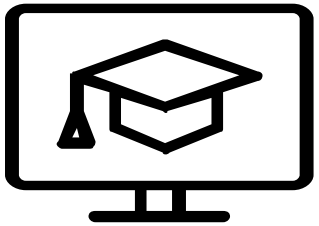
- Non-VPN traffic uses HTTPS and TLS 1.2 standards for data in transit encryption between workstations and services (e.g., *Office 365*)
- Accenture VPN traffic uses TLS 1.2 for data in transit
- Accenture provides the capability to set up secure connectivity to client sites using site-to-site / client-to-site VPN tunnels with appropriate encryption.
- Accenture's email solution (*Microsoft Exchange*) uses digital certificates for email encryption using SHA2-RSA 2048-bit keys.
- Additionally, email can be digitally signed for non-repudiation. It has a "permissions" functionality feature that can encrypt the content with AES 128-bit encryption.
- Accenture supports both enforced and opportunistic Transport Layer Security (TLS) encryption for emails between the client and Accenture domains.
- Data transmission on the network must be protected with a minimum of 128-bit encryption.
- Applications use TLS v1.2 and above as the encryption mechanism with 2048-bit key strength.



What training does Accenture provide its people about adopting secure behaviors?

Accenture Information Security has a long-established behavior change and learning program that leverages award-winning, custom-built activities to engage every employee in knowing the importance of their role in keeping data secure.

- Quarterly launched training experiences include both required and voluntary online activities.
  - Required training sees a **98% completion rate**
  - supplemental, voluntary activities are completed by **~70% of all employees**.
- Custom-produced live action video series, Hacker Land, continually garners the highest viewership rates of all videos; incorporates current headline themes into plot lines that are relatable to employees
- All employees are tested quarterly on their ability to identify phishing and social engineering emails; those that do not pass with ease (in some cases) are enrolled in a remedial program.
- Active participation in Cyber Security Awareness month, Data Privacy Day and other promotional security activities which award 'flair'



What happens if a laptop / desktop that has access to client information is lost or stolen?

Unfortunately, theft is an occurrence in life regardless of current crises, but Accenture is steadfast in its ability to secure information should a device fall into unauthorized hands.

Accenture has several measures in place to secure its computers, so they are protected against this type of threat, and to prevent the compromise of the data:

- All hard drives are encrypted
- An 8-digit PIN is required to enable the computer to boot
- A unique username and password required to log into the system
- After 6 failed login attempts, the user is locked out
- We can remotely deploy a “kill package” that will keep the workstation from booting

Accenture workers are required to immediately report lost devices to Accenture's Security Operations Center (ASOC).

What steps is Accenture taking to address physical security risks?

Accenture understands that in a WFH model, physical security controls change. While there is no way to replicate physical controls that would exist within a Delivery Center, Accenture's overall security model provides a level of assurance on how data is protected. Those key controls include:

Data offloading protection is enabled on our workstations with DLP, web filtering and USB/media blocks. Additionally, if data is accessed via a Citrix or VDI environment that is provided by the client, confirmation that those systems are set to block offloading of data must be in place.

Multifactor Authentication is enabled on almost every Accenture application, including VPN. This approach helps mitigate the impact of a lost or compromised user ID and password.

Encryption is required at multiple points within the Accenture environment: Accenture workstations, use of Office 365 for data at rest, data written to USBs (if allowed) and transmission of data.

Lost devices have multiple protection points including Accenture's ability to deploy a "kill package" to Accenture workstations, and the ability to remotely wipe mobile devices registered in the Mobile Device Management (MDM) system.

Least privilege access is enforced within the Accenture environment and actively managed with clients to enable access to their systems and applications, and to ensure those systems and applications are aligned to the minimum data exposure needed to perform services.

Ongoing awareness programs continue to communicate and enhance messages around how to work securely from home.

How does Accenture protect data in the cloud?

Capabilities	Products	Security benefits
Cloud Protections for AWS, Azure and Google Provided by cloud vendors using native services and custom developed to provide automated prevention controls	• Customer security prevents using Azure Policy, AWS config Lamda functions, custom code • AWS Guard Duty • Azure Defenders • Azure and AWS WAF	• Automated control in order to prevent insecure configuration • Native cloud services to simplify adaption of malicious traffic detection
Vulnerability management and configuration compliance Enables vulnerability scanning and configuration compliance of our global infrastructure, network, servers, cloud. This capabilities is enabled by multiple tools, which also include compliance for firewall rules and cloud native controls	• QualysGuard and Qualys Agent • Nessus • Palo Alto Prisma Cloud • Http header scanner custom scrip • MFNA + Custom Scripting • Firemon •	• Vulnerability Management – External: daily scans using Nessus, Qualys and custom scripts – Internal: mostly bi-monthly scans and ongoing using Qualys agent, which provide scan data every 4 hours • Compliance validation to ensure that actual configurations are matching to the security standards for servers, network devices and cloud native controls (via Prisma) • Firemon is used to measure firewall rules compliance for network edge firewalls • MFNA provides both vuln scanning and compliance scanning for network devices
Security information and event management and threat hunting Collects logs from network, servers, cloud, and applications which are sent to SIEM for analysis. Logs are correlated using predefined use cases and archived, while alerts are used by our security operations and CIRT teams to detect suspicious activity and conduct investigations. This capability also includes automated response use of Tanium to conduct threat hunting and supplement SIEM	• Splunk • Phantom • Tanium • Cloud Security Analytics	• Devices in scope: Servers; Firewalls, IDS/IPS, VPN, NAC, Web Filtering; DNS/DHCP servers; Security consoles (IAM systems, MS cloud application security, MS Defender for Endpoint and Identity). DLP is handled outside of SIEM by a separate console • Logs from Cloud Providers (Advanced Threat Protection for PaaS, cloud Security Groups, Guard Duty, etc) • Threat hunting enabled via Tanium and MS Defender for Endpoint • Process automation enrichment of incident data, auto remediation of infected workstations, ticket management and expedite incident analysis and handling
Information Security Dashboard and Security Inventory Collects security inventory from CMDBs, spreadsheet or manually in order to know the units of reporting and assign accountability Centralize all vulnerability and compliance reporting from different tools in order to assign accountability and ensure remediation	• Custom tool • Tanium Discover • Palo Prisma Cloud • Palo Expanse	• Find all unknown systems to be measured • Maintain a list of accountable contact and known assets • Display vulnerabilities and ensure remediation via accountability • Single Pain of Glass for vulnerability and security compliance data

Does Accenture leverage external security reputation vendors?

Accenture tracks the monthly Accenture assessment ratings produced by four major cyber security risk rating organisations.

Organisation	Primary focus	Accenture treatment	Score range
BitSight https://www.bitsight.com	Compromised Systems	Proactively scan all IPs on a weekly basis for new vulnerabilities	**780-810***
RiskRecon https://www.riskrecon.com	Infrastructure compliance and Insecure HTTP	Proactively scan all IPs/URLs on a weekly basis for new vulnerabilities	**8.2-9.3****
Security Scorecard https://securityscorecard.com	Infrastructure compliance	Proactively scan all IPs on a weekly basis for new vulnerabilities	**85-99 (A)***
UpGuard https://www.upguard.com/	Open Ports, Man-in-the-Middle vulnerabilities, and Insecure HTTP	Proactively scan all URLs for new vulnerabilities on a weekly basis	**921-927***

* last 12 months; data shown as of 2022
** as of March 2022