TEVORA™

Verizon Digital Media Services
2018 MPAA Content Security Review

Christina Whiting
David Grazer
Adoriel Bethishou

Delivered February 28th, 2019

Table of Contents

Executive Summary

Overview

Verizon Digital Media Services (VDMS) engaged Tevora to conduct a Motion Picture Association of America (MPAA) Content Security Review for the purpose of evaluating compliance with MPAA's best practices for securely storing, processing, and delivering protected media and content. This report is also designed to identify gaps in compliance and provide considerations for remediating those gaps, to meet the MPAA's best practices requirements.

The assessment was conducted from June 18th to October 21st of 2018 and included the following areas in scope:

- VDMS – Playa Vista
- EdgeCast CDN – Playa Vista, CA
- upLynk Lehi – Lehi, UT
- upLynk Dulles – Dulles, Virginia

Environment

VDMS is a content delivery network (CDN) based in Los Angeles, CA. VDMS offers various video content-related services which are used by customers and then delivered through the EdgeCast CDN. These content-related services are hosted within the VDMS Edge environment. This environment supports content caching and accelerated delivery service, as well as VDMS's video streaming service, upLynk. upLynk offers media content encoding and slicing services that provide customers the option to apply digital rights management schemes at the time of encoding. upLynk has established production systems within Amazon AWS. These systems are used by various upLynk Video clients to process transform video content, which are then delivered through the EdgeCast CDN.

VDMS does not handle any MPAA physical media. Content is ingested electronically and pre-encrypted with security features deemed appropriate by the upLynk video provider customer. Output of the content is controlled by the customer's configuration of content distribution through the CDN. The objective of the CDN is to distribute customer media content over the Internet. It is the customer's responsibility to apply the necessary content protections to media before it is ingested into the CDN. Customers are responsible for control and ownership of their data and media assets.

Additionally, VDMS does not handle or have access to pre-theatrical content, nor is it able to modify final content provided by MPAA-related entities. Therefore, several controls of the MPAA Content Security Review are not applicable.

Scoring

Each MPAA Content Protection control is evaluated to determine the applicability and level of compliance within the VDMS environment. The below legend explains how each control is evaluated.

M	**Meets Best Practice**	**B**	**Below Best Practice**
I	**Needs Immediate Improvements**	**N**	**Not Applicable**

Summary

The following table below summarizes results the assessment against the in-scope environments for compliance with the MPAA Content Protection standard.

Security Topic	M	B	I	N/A
Management System	**33**	**0**	**0**	**0**
Physical Security	**44**	**0**	**0**	**56**
Digital Security	**91**	**1**	**0**	**26**
Total	**168**	**1**	**0**	**82**

Further details on the evaluation methods are explained in the remaining sections.

Assessor's Opinion

It is the opinion of the assessing firm, Tevora, that VDMS meets the overall objectives and intent of the MPAA Content Protection standard. Only one control was deemed to be below best practice. It should be noted that while most controls are sufficiently implemented, Tevora recommends remediating the gap noted in this assessment to further ensure compliance with the standards laid out by the MPAA.

Site Survey Dashboard

Management System	
Executive Security	M
Risk Management	M
Security Organisation	M
Policies and Procedures	M
Incident Response	M
BC & DR	M
Change Control	M
Workflow	M
Segregation of Duties	M
Background Checks	M
Confidentiality Agreements	M
Third Party Use and Screening	M

Facility	
Entry/Exit Points	M
Visitor Entry/Exit	M
Identification	M
Perimeter Security	M
Alarms	M
Authorization	M
Electronic Access Control	M
Keys	M
Cameras	M
Logging and Monitoring	M
Searches	N

Asset Management	
Inventory Tracking	N
Inventory Counts	N
Blank Media/Raw Stock Tracking	N
Client Assets	N
Disposals	N

Transport	
Shipping	N
Receiving	N
Labelling	N
Packaging	N
Transport Vehicles	N

Infrastructure	
Firewall/WAN/ Perimeter Security	M
Internet	N
LAN/Internal Network	M
Wireless/WLAN	M
I/O Device Security	N
System Security	M
Account Management	B
Authentication	M
Logging and Monitoring	M
Mobile Security	M

Content Management	
Security Techniques	N
Content Tracking	M

Content Transfer	
Transfer Systems	M
Transfer Device Methodology	N
Client Portal	M

Remediation Summary

Subject	Control	Consideration for Improvement	Assessment Observation
DS-7.6 Account Management	DS-7.6	VDMS Administration Staff – ESRA 2018.03 VDMS IT should document and formalize an access review procedure by the server's data owner for the NAE server that is enforced, audited, and conducted regularly.	VDMS Administration Staff – ESRA 2018.03 Access review for the NAE network device configuration services are performed with reviews of the TACACS+ server, meaning they do not have an independently defined process. Evidence provided from VDMS confirms that efforts are underway to remediate this risk. The expected remediation date is *April 8, 2019*.

Overall Risks and Recommendations

Effort has been observed in remediating risks noted during assessment. Evidence and business justifications provided have closed many of the risks originally noted during assessment. The remaining gap is planned for remediation in the second quarter of 2019. VDMS should ensure this risk is remediated and that security and privacy remain at the forefront of operations throughout the organization. This will help to ensure continuing compliance with MPAA standards.

Assessment Survey Results – Detail

Management Systems

Best Practice Title	Best Practice Description	Survey Result
MS-1.0 Executive Security Awareness/Oversight	Establish an information security management system that implements a control framework for information security which is approved by the business owner(s) /senior management.	**M – Meets Best Practice**
MS-1.1 Executive Security Awareness/Oversight	Review information security management policies and processes at least annually.	**M – Meets Best Practice**
MS-1.2 Executive Security Awareness/Oversight	Train and engage executive management/owner(s) on the business' responsibilities to protect content at least annually.	**M – Meets Best Practice**
MS-1.3 Executive Security Awareness/Oversight	Create an information security management group to establish and review information security management policies.	**M – Meets Best Practice**
MS-2.0 Risk Management	Develop a formal, documented security risk assessment process focused on content workflows and sensitive assets in order to identify and prioritize risks of content theft and leakage that are relevant to the facility.	**M – Meets** Best **Practice**
MS-2.1 Risk Management	Conduct an internal risk assessment annually and upon key workflow changes, based on, at a minimum, the MPAA Best Practice Common Guidelines and the applicable Supplemental Guidelines—and document and act upon identified risks.	**M – Meets Best Practice**

Best Practice Title	Best Practice Description	Survey Result
MS-3.0 Security Organization	Identify security key point(s) of contact and formally define roles and responsibilities for content and asset protection.	M – Meets Best Practice
MS-4.0 Policies and Procedures	Establish policies and procedures regarding asset and content security.	M – Meets Best Practice
MS-4.0.1 Policies and Procedures	Establish dedicated policies governing the use of social media by company personnel.	M – Meets Best Practice
MS-4.0.2 Policies and Procedures	Establish policies governing the using of mobile computing devices.	M – Meets Best Practice
MS-4.1 Policies and Procedures	Review and update security policies and procedures at least annually.	M – Meets Best Practice
MS-4.2 Policies and Procedures	Communicate and require sign-off from all company personnel (e.g., employees, temporary workers, interns) and third-party workers (e.g., contractors, freelancers, temp agencies) for all current policies, procedures and/or client requirements.	M – Meets Best Practice
MS-4.3 Policies and Procedures	Develop and regularly update an awareness program about security policies and procedures, and train company personnel and third-party workers upon hire, and annually thereafter on security policies and procedures.	M – Meets Best Practice
MS-5.0 Incident Response	Establish a formal incident response plan that describes actions to be taken when a security incident is detected and reported.	M – Meets Best Practice

MS-5.1 Incident Response	Identify the security incident response team who will be responsible for detecting, analyzing, and remediating security incidents.	**M – Meets Best Practice**
MS-5.2 Incident Response	Establish a security incident reporting process for individuals to report detected incidents to the security incident response team.	**M – Meets Best Practice**
MS-6.0 Business Continuity & Disaster Recovery	Establish a formal plan that describes actions to be taken to ensure business continuity.	**M – Meets Best Practice**
MS-6.1 Business Continuity & Disaster Recovery	Identify the business continuity team who will be responsible for detecting, analyzing and remediating continuity incidents.	**M – Meets Best Practice**
MS-6.2 Business Continuity & Disaster Recovery	Establish a data backup policy that addresses the following: • Systems and data • Retention and protection requirements • Backup frequency • Encryption • Recovery time objectives (RTO) • Recovery point objectives (RPO) • Restoration testing • Secure offsite storage	**M – Meets Best Practice**
MS-7.0 Change Control and Configuration Management	Establish policies and procedures to ensure new data, applications, network, and systems components have been pre-approved by business leadership.	**M – Meets Best Practice**

MS-8.0 Workflow	Document workflows tracking content and authorization checkpoints. Include the following processes for both physical and digital content.	**M – Meets Best Practice**
MS-9.0 Segregation of Duties	Segregate duties within the content workflow. Implement and document compensating controls where segregation is not practical.	**M – Meets Best Practice**
MS-10.0 Background Checks	Perform background screening checks on all company personnel and third-party workers.	**M – Meets Best Practice**
MS-11.0 Confidentiality Agreements	Require all company personnel to sign a confidentiality agreement (e.g., non-disclosure) upon hire and annually thereafter. The agreement includes requirements for handling and protecting content.	**M – Meets Best Practice**
MS-11.1 Confidentiality Agreements	Require all company personnel to return all content and client information in their possession upon termination of their employment or contract.	**M – Meets Best Practice**
MS-12.0 Third Party Use and Screening	Require all third-party workers (e.g., freelancers) who handle content to sign confidentiality agreements (e.g., non-disclosure) upon engagement.	**M – Meets Best Practice**
MS-12.1 Third Party Use and Screening	Require all third-party workers to return all content and client information in their possession upon termination of their contract.	**M – Meets Best Practice**
MS-12.2 Third Party Use and Screening	Include security requirements in third-party contracts.	**M – Meets Best Practice**
MS-12.3 Third Party Use and Screening	Implement a process to reclaim content when terminating relationships.	**M – Meets Best Practice**

MS-12.4 Third Party Use and Screening	Require third-party workers to be bonded and insured where appropriate (e.g., courier service).	**M – Meets Best Practice**
MS-12.5 Third Party Use and Screening	Restrict third-party access to content/production areas unless required for their job function.	**M – Meets Best Practice**
MS-12.5.1 Third Party Use and Screening	Control access of third-party IT service providers to the computing environment.	**M – Meets Best Practice**
MS-12.6 Third Party Use and Screening	Notify clients if subcontractors are used to handle content or if work is off-loaded to another company.	**M – Meets Best Practice**

Physical Security

Best Practice Title	Best Practice Description	Survey Result
PS-1.0 Entry/Exit Points	Secure all entry/exit points of the facility at all times, including loading dock doors and windows.	**M – Meets Best Practice**
PS-1.1 Entry/Exit Points	Control access to areas where content is handled by segregating the content area from other facility areas (e.g., administrative offices, waiting rooms, loading docks, courier pickup and drop-off areas, replication and mastering).	**M – Meets Best Practice**
PS-1.2 Entry/Exit Points	Control access in facilities where there are collocated businesses, which include but are not limited to the following: • Segregating work areas • Implementing access-controlled entrances and exits • that can be segmented per business unit • Logging and monitoring of all entrances and exits within • facility • All tenants within the facility must be reported to client • prior to engagement	**M – Meets Best Practice**
PS-2.0 Visitor Entry/Exit	Maintain a detailed visitors' log (sign in/out).	**M – Meets Best Practice**
PS-2.1 Visitor Entry/Exit	Assign an identification badge or sticker, which must always be visible , to each visitor and collect badges upon exit.	**M – Meets Best Practice**

Best Practice Title	Best Practice Description	Survey Result
PS-2.2 Visitor Entry/Exit	Do not provide visitors with key card access to content/production areas.	M – Meets Best Practice
PS-2.3 Visitor Entry/Exit	Require visitors to be escorted by authorized employees while on-site, or in content/production areas.	M – Meets Best Practice
PS-2.3.1 Visitor Entry/Exit	Visitors should be required to sign a nondisclosure agreement (NDA) and a visitor log prior to entering a facility.	M – Meets Best Practice
PS-3.0 Identification	Provide company personnel and long-term third-party workers (e.g., janitorial) with a photo identification badge that is required to be visible at all times.	M – Meets Best Practice
PS-4.0 Perimeter Security	Implement perimeter security controls that address risks the facility may be exposed to, as identified by the organization's risk assessment.	M – Meets Best Practice
PS-4.1 Perimeter Security	Place security guards at perimeter entrances and non-emergency entry/exit points.	M – Meets Best Practice
PS-4.2 Perimeter Security	Implement a daily security patrol process with a randomized schedule and document the patrol results in a log.	M – Meets Best Practice
PS-4.3 Perimeter Security	Lock perimeter gates at all times.	M – Meets Best Practice

Best Practice Title	Best Practice Description	Survey Result
PS-5.0 Alarms	Install a centralized, audible alarm system that covers all entry/exit points (including emergency exits), windows, loading docks, fire escapes, and restricted areas (e.g., vault, server/machine room).	M – Meets Best Practice
PS-5.1 Alarms	Install and effectively position motion detectors in restricted areas (e.g., vault, server/machine room) and configure them to alert the appropriate security and other personnel (e.g. project managers, producer, head of editorial, incident response team, etc.).	M – Meets Best Practice
PS-5.2 Alarms	Install door prop alarms in restricted areas (e.g. vault, server, machine rooms) to notify when sensitive entry/exit points are open for longer than a pre-determined period (e.g., 60 seconds).	M – Meets Best Practice
PS-5.3 Alarms	Configure alarms to provide escalation notifications directly to the personnel in charge of security and other personnel (e.g., project managers, producer, head of editorial, incident response team, etc.).	M – Meets Best Practice
PS-5.4 Alarms	Assign unique arm and disarm codes to each person that requires access to the alarm system, and restrict access to all other personnel.	M – Meets Best Practice
PS-5.5 Alarms	Review the list of users who can arm and disarm alarm systems quarterly, or upon change of personnel.	M – Meets Best Practice
PS-5.6 Alarms	Test the alarm system quarterly.	M – Meets Best Practice

PS-5.7 Alarms	Implement fire safety measures to prevent unauthorized access in the event of a power outage, when fire doors fail to open and all other doors fail shut.	**M – Meets Best Practice**
PS-6.0 Authorization	Document and implement a process to manage facility access and keep records of any changes to access rights.	**M – Meets Best Practice**
PS-6.1 Authorization	Restrict access to production systems to authorized personnel only.	**M – Meets Best Practice**
PS-6.2 Authorization	Review access to restricted areas (e.g., vault, server/machine room) quarterly and when there are changes to the roles or employment status of company personnel and/or third-party workers.	**M – Meets Best Practice**
PS-7.0 Electronic Access Control	Implement electronic access throughout the facility to cover all entry/exit points and all areas where content is stored, transmitted, or processed.	**M – Meets Best Practice**
PS-7.1 Electronic Access Control	Restrict electronic access of system administration to appropriate personnel.	**M – Meets Best Practice**
PS-7.2 Electronic Access Control	Store card stock and electronic access devices (e.g., key cards, key fobs) in a locked cabinet and ensure electronic access devices remain disabled prior to being assigned to personnel. Store unassigned electronic access devices (e.g., key cards, key fobs) in a locked cabinet and ensure these remain disabled prior to being assigned to personnel.	**M – Meets Best Practice**
PS-7.3 Electronic Access Control	Disable lost electronic access devices (e.g., key cards, key fobs) in the system before issuing a new electronic access device.	**M – Meets Best Practice**

PS-7.4 Electronic Access Control	Issue third-party access to electronic devices with a set expiration date (e.g. 90 days) based on an approved timeframe.	**M – Meets Best Practice**
PS-8.0 Keys	Limit the distribution of the master keys and/or keys to restricted areas to authorized personnel only (e.g., owner, facilities management).	**M – Meets Best Practice**
PS-8.1 Keys	Implement a check-in/check-out process to track and monitor the distribution of master keys and/or keys to restricted areas.	**M – Meets Best Practice**
PS-8.2 Keys	Use keys that can only be copied by a specific locksmith for exterior entry/exit points.	**M – Meets Best Practice**
PS-8.3 Keys	For each quarter, create an inventory for master keys and keys to restricted areas, including facility entry/exit points.	**M – Meets Best Practice**
PS-8.4 Keys	Obtain all keys from terminated employees/third-parties, and from those who no longer need the keys for access.	**M – Meets Best Practice**
PS-8.5 Keys	Implement electronic access control or rekey the entire facility when master or sub-master keys are lost or missing.	**M – Meets Best Practice**
PS-9.0 Cameras	Install a CCTV system that records all facility entry/exit points and restricted areas (e.g. server/machine room, etc.).	**M – Meets Best Practice**

PS-9.1 Cameras	Review camera positioning and recordings to ensure adequate coverage, function, image quality and lighting conditions and frame rate of surveillance footage at least daily.	**M – Meets Best Practice**
PS-9.2 Cameras	Restrict physical and logical access to the CCTV console and to CCTV equipment (e.g., DVRs) to personnel responsible for administering/monitoring the system.	**M – Meets Best Practice**
PS-9.3 Cameras	Ensure that camera footage includes an accurate date and time-stamp, and retain CCTV surveillance footage and electronic access logs in a secure location for at least 90 days, or for the maximum time allowed by law.	**M – Meets Best Practice**
PS-9.4 Cameras	Designate an employee or group of employees to monitor surveillance footage during operating hours and immediately investigate detected security incidents.	**M – Meets Best Practice**
PS-10.0 Logging and Monitoring	Log and review electronic access to restricted areas for suspicious events, at least weekly.	**M – Meets Best Practice**
PS-10.1 Logging and Monitoring	Log and review electronic access, at least daily for the following areas: • Masters/stampers vault • Pre-mastering • Server/machine room • Scrap Room • High Security Cages	**M – Meets Best Practice**
PS-10.2 Logging and Monitoring	Investigate suspicious electronic access activities that are detected.	**M – Meets Best Practice**

PS-10.3 Logging and Monitoring	Maintain an ongoing log of all confirmed electronic access incidents and include documentation of any follow-up activities that were taken.	**M – Meets Best Practice**
PS-11.0 Searches	Establish a policy, as permitted by local laws that allows security to randomly search persons, bags, packages, and personal items for client content.	**N – Not Applicable**
PS-11.1 Searches	Implement an exit search process that is applicable to all facility personnel and visitors.	**N – Not Applicable**
PS-11.2 Searches	Prohibit personnel from entering/exiting the facility with digital recording devices (e.g., USB thumb drives, digital cameras, cell phones) and include the search of these devices as part of the exit search procedure.	**N – Not Applicable**
PS-11.3 Searches	Enforce the use of transparent plastic bags and food containers for any food brought into production areas.	**N – Not Applicable**
PS-11.4 Searches	Implement a dress code policy that prohibits the use of oversized clothing (e.g., baggy pants, oversized hooded sweatshirts).	**N – Not Applicable**
PS-11.5 Searches	Use numbered tamper-evident stickers/holograms to identify authorized devices that can be taken in and out of the facility.	**N – Not Applicable**
PS-11.6 Searches	Implement a process to test the exit search procedure.	**N – Not Applicable**
PS-11.7 Searches	Perform a random vehicle search process when exiting the parking lot.	**N – Not Applicable**

PS-11.8 Searches	Segregate replication lines that process highly sensitive content and perform searches upon exiting segregated areas.	**N – Not Applicable**
PS-11.9 Searches	Implement additional controls to monitor security guards' activity.	**N – Not Applicable**
PS-12.0 Inventory Tracking	Implement a content asset management system to provide detailed tracking of physical assets (i.e., received from client created at the facility).	**N – Not Applicable**
PS-12.1 Inventory Tracking	Barcode or assign unique tracking identifier(s) to client assets and created media (e.g., tapes, hard drives) upon receipt and store assets in the vault when not in use.	**N – Not Applicable**
PS-12.1.1 Inventory Tracking	Develop a data classification scheme to categorize physical assets of differing security requirements.	**N – Not Applicable**
PS-12.2 Inventory Tracking	Retain asset movement transaction logs for at least one year.	**N – Not Applicable**
PS-12.3 Inventory Tracking	Review logs from content asset management system at least weekly and investigate anomalies.	**N – Not Applicable**
PS-12.4 Inventory Tracking	Use studio film title aliases when applicable on physical assets and in asset tracking systems.	**N – Not Applicable**
PS-12.5 Inventory Tracking	Implement and review a daily aging report to identify highly sensitive assets that are checked out from the vault and not checked back in.	**N – Not Applicable**
PS-12.6 Inventory Tracking	Lock up and log assets that are delayed or returned if shipments could	**N – Not Applicable**

	not be delivered on time.	
PS-13.0 Inventory Counts	Perform a quarterly inventory count of each client's asset(s), reconcile against asset management records, and immediately communicate variances to clients.	**N – Not Applicable**
PS-13.1 Inventory Counts	Segregate duties between the vault staff and individuals who are responsible for performing inventory count.	**N – Not Applicable**
PS-14.0 Blank Media/Raw Stock Tracking	Tag (e.g., barcode, assign unique identifier) blank stock/raw stock per unit when received.	**N – Not Applicable**
PS-14.1 Blank Media/Raw Stock Tracking	Establish a process to track consumption of raw materials (e.g., polycarbonate) monthly.	**N – Not Applicable**
PS-14.2 Blank Media/Raw Stock Tracking	Store blank media/raw stock in a secured location.	**N – Not Applicable**
PS-15.0 Client Assets	Restrict access to finished client assets to personnel responsible for tracking and managing assets.	**N – Not Applicable**
PS-15.1 Client Assets	Store client assets in a restricted and secure area (e.g., vault, safe, or other secure storage location).	**N – Not Applicable**
PS-15.2 Client Assets	Require two company personnel with separate access cards to unlock highly sensitive areas (e.g., safe, high-security cage) after-hours.	**N – Not Applicable**

PS-15.3 Client Assets	Use a locked fireproof safe to store undelivered packages that are kept at the facility overnight.	**N – Not Applicable**
PS-15.4 Client Assets	Implement a dedicated, secure area (e.g., security cage, secure room) for the storage of undelivered screeners that are locked, access-controlled, and monitored with surveillance cameras and/or security guards.	**N – Not Applicable**
PS-16.0 Disposals	Require that rejected, damaged, and obsolete stock containing client assets are erased, degaussed, shredded, or physically destroyed before disposal.	**N – Not Applicable**
PS-16.0.1 Disposals	Finished elements (e.g. check discs, test prints, mock-ups, ADR scripts) should be destroyed immediately after use, unless otherwise specified by content owners. Require paper materials containing client assets (scripts, artwork, storyboards, etc.) to be physically destroyed before disposal.	**N – Not Applicable**
PS-16.1 Disposals	Store elements targeted for recycling/destruction in a secure location/container to prevent the copying and reuse of assets prior to disposal.	**N – Not Applicable**
PS-16.2 Disposals	Maintain a log of asset disposal for at least 12 months.	**N – Not Applicable**
PS-16.3 Disposals	Destruction must be performed on site. On site destruction must be supervised and signed off by two company personnel. If a third-party destruction company is engaged, destruction must be supervised and signed off by two company personnel and certificates of destruction must be retained.	**N – Not Applicable**
PS-16.4 Disposals	Use automation to transfer rejected discs from replication machines directly into scrap bins (no machine operator handling).	**N – Not Applicable**

PS-17.0 Shipping	Require the facility to generate a valid work/shipping order to authorize client asset shipments out of the facility.	**N – Not Applicable**
PS-17.1 Shipping	Track and log client asset shipping details.	**N – Not Applicable**
PS-17.2 Shipping	Secure client assets that are waiting to be picked up.	**N – Not Applicable**
PS-17.3 Shipping	Validate client assets leaving the facility against a valid work/shipping order.	**N – Not Applicable**
PS-17.4 Shipping	Prohibit couriers and delivery personnel from entering content/production areas of the facility.	**N – Not Applicable**
PS-17.5 Shipping	Document and retain a separate log for truck driver information.	**N – Not Applicable**
PS-17.6 Shipping	Observe and monitor the on-site packing and sealing of trailers prior to shipping.	**N – Not Applicable**
PS-17.7 Shipping	Record, monitor and review travel times, routes, and delivery times for shipments between facilities.	**N – Not Applicable**
PS-17.8 Shipping	Prohibit the transfer of film elements other than for client studio approved purposes.	**N – Not Applicable**
PS-17.9 Shipping	Ship prints for pre-theatrical screenings in segments (e.g., odd versus even reels).	**N – Not Applicable**

PS-18.0 Receiving	Inspect delivered client assets upon receipt and compare to shipping documents (e.g., packing slip, manifest log).	**N – Not Applicable**
PS-18.1 Receiving	Maintain a receiving log to be filled out by designated personnel upon receipt of deliveries.	**N – Not Applicable**
PS-18.2 Receiving	Perform the following actions immediately: • Tag (e.g., barcode, assign unique identifier) received assets, • Input the asset into the asset management system • Move the asset to the restricted area (e.g., vault, safe)	**N – Not Applicable**
PS-18.3 Receiving	Implement a secure method for receiving overnight deliveries.	**N – Not Applicable**
PS-19.0 Labelling	Prohibit the use of title information, including AKAs ("aliases"), on the outside of packages unless instructed otherwise by client.	**N – Not Applicable**
PS-20.0 Packaging	Ship all client assets in closed/sealed containers, and use locked containers depending on asset value, or if instructed by the client.	**N – Not Applicable**
PS-20.1 Packaging	Implement at least one of the following controls: • Tamper-evident tape • Tamper-evident packaging • Tamper-evident seals in the form of holograms • Secure containers (e.g., Pelican case with a combination lock)	**N – Not Applicable**

PS-20.2 Packaging	Apply shrink wrapping to all shipments, and inspect packaging before final shipment to ensure that it is adequately wrapped.	**N – Not Applicable**
PS-21.0 Transport Vehicles	Lock automobiles and trucks at all times, and do not place packages in clear view.	**N – Not Applicable**
PS-21.1 Transport Vehicles	Include the following security features in transportation vehicles • Segregation from driver cabin • Ability to lock and seal cargo doors • GPS for high-security shipments	**N – Not Applicable**
PS-21.2 Transport Vehicles	Apply numbered seals on cargo doors for shipments of highly sensitive titles.	**N – Not Applicable**
PS-21.3 Transport Vehicles	Require security escorts to be used when delivering highly sensitive content to high-risk areas.	**N – Not Applicable**

Digital Security

Best Practice Title	Best Practice Description	Survey Result
DS-1.0 Firewall/WAN/ Perimeter Security	Separate external network(s)/WAN(s) from the internal network(s) by using inspection firewall(s) with Access Control Lists that prevent unauthorized access to any internal network and with the ability to keep up with upload and download traffic.	**M – Meets Best Practice**
DS-1.1 Firewall/WAN/ Perimeter Security	Implement a process to review firewall Access Control Lists (ACLs) to confirm configuration settings are appropriate and required by the business every six months.	**M – Meets Best Practice**
DS-1.2 Firewall/WAN/ Perimeter Security	Deny all protocols by default and enable only specific permitted secure protocols to access the WAN and firewall.	**M – Meets Best Practice**
DS-1.3 Firewall/WAN/ Perimeter Security	Place externally accessible servers (e.g., web servers) within the de-militarized zone (DMZ)	**M – Meets Best Practice**
DS-1.4 Firewall/WAN/ Perimeter Security	Implement a process to patch network infrastructure devices (e.g., firewalls, routers, switches, etc.), SAN/NAS (Storage Area Networks and Network Attached Storage), and servers.	**M – Meets Best Practice**
DS-1.5 Firewall/WAN/ Perimeter Security	Harden network infrastructure devices, SAN/NAS, and servers based on security configuration standards. Disable SNMP (Simple Network Management Protocol) if it is not in use, or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	**M – Meets Best Practice**
DS-1.6 Firewall/WAN/ Perimeter Security	Do not allow remote management of the firewall from any external interface(s)	**M – Meets Best Practice**
DS-1.7 Firewall/WAN/ Perimeter Security	Secure backups of network infrastructure/SAN/NAS devices and servers to a centrally secured server on the internal network.	**M – Meets Best Practice**

Best Practice Title	Best Practice Description	Survey Result
DS-1.8 Firewall/WAN/ Perimeter Security	Perform quarterly vulnerability scans on at least all external IP ranges and hosts, and remediate issues.	**M – Meets Best Practice**
DS-1.9 Firewall/WAN/ Perimeter Security	Perform annual penetration testing of all external IP ranges and hosts at least and remediate issues.	**M – Meets Best Practice**
DS-1.10 Firewall/WAN/ Perimeter Security	Secure any point to point connections by using dedicated, private connections and by using encryption.	**M – Meets Best Practice**
DS-1.11 Firewall/WAN/ Perimeter Security	Implement a synchronized time service protocol (e.g., Network Time Protocol) to ensure all systems have a common time reference.	**M – Meets Best Practice**
DS-1.12 Firewall/WAN/ Perimeter Security	Establish, document and implement baseline security requirements for WAN network infrastructure devices and services.	**M – Meets Best Practice**
DS-2.0 Internet	Prohibit production network and all systems that process or store digital content from directly accessing the internet, including email. If a business case requires internet access from the production network or from systems that process or store digital content, only approved methods are allowed via use of a remote hosted application / desktop session.	**N – Not Applicable**
DS-2.1 Internet	Implement email filtering software or appliances that block the following	**N – Not Applicable**

Best Practice Title	Best Practice Description	Survey Result
	from non-production networks: • Potential phishing emails • Prohibited file attachments (e.g., Visual Basic scripts, executables, etc.) • File size restrictions limited to 10 MB • Known domains that are sources of malware or viruses	
DS-2.2 Internet	Implement web filtering software or appliances that restrict access to websites known for peer-to-peer file trading, viruses, hacking or other malicious sites.	**N – Not Applicable**
DS-3.0 LAN/Internal Network	Isolate the content/production network from non-production networks (e.g., office network, DMZ, the internet etc.) by means of physical or logical network segmentation.	**M – Meets Best Practice**
DS-3.1 LAN/Internal Network	Restrict access to the content/production systems to authorized personnel.	**M – Meets Best Practice**
DS-3.2 LAN/Internal Network	Restrict remote access to the content/production network to only approved personnel who require access to perform their job responsibilities.	**M – Meets Best Practice**
DS-3.3 LAN/Internal Network	Use switches/layer 3 devices to manage the network traffic, and disable all unused switch ports on the content/production network to prevent packet sniffing by unauthorized devices.	**M – Meets Best Practice**
DS-3.4 LAN/Internal Network	Restrict the use of non-switched devices such as hubs and repeaters on	**M – Meets Best Practice**

Best Practice Title	Best Practice Description	Survey Result
	the content/production network.	
DS-3.5 LAN/Internal Network	Prohibit dual-homed networking (physical networked bridging) on computer systems within the content/production network.	M – Meets Best Practice
DS-3.6 LAN/Internal Network	Implement a network-based intrusion detection /prevention system (IDS/IPS) on the content/production network.	M – Meets Best Practice
DS-3.7 LAN/Internal Network	Disable SNMP (Simple Network Management Protocol) if it is not in use, or use only SNMPv3 or higher and select SNMP community strings that are strong passwords.	M – Meets Best Practice
DS-3.8 LAN/Internal Network	Harden systems prior to placing them in the LAN / Internal Network.	M – Meets Best Practice
DS-3.9 LAN/Internal Network	Conduct internal network vulnerability scans and remediate any issues, at least annually.	M – Meets Best Practice
DS-3.10 LAN/Internal Network	Secure backups of local area network SAN/NAS, devices, servers and workstations to a centrally secured server on the internal network.	M – Meets Best Practice
DS-3.11 LAN/Internal Network	DNS servers used in the production network should not allow connections to and from the internet.	M – Meets Best Practice
DS-4.0 Wireless/WLAN	Prohibit wireless networking and the use of wireless devices on the content/production network.	M – Meets Best Practice

Best Practice Title	Best Practice Description	Survey Result
DS-4.1 Wireless/WLAN	Configure non-production wireless networks (e.g., administrative and guest) with the following security controls: • Disable WEP / WPA • Only Enable AES128 encryption (WPA2), or higher • Segregate "guest" networks from the company's other networks • Change default administrator logon credentials • Change default network name (SSID)	**M – Meets Best Practice**
DS-4.2 Wireless/WLAN	Implement a process to scan for rogue wireless access points and remediate any validated issues.	**M – Meets Best Practice**
DS-5.0 I/O Device Security	Designate specific systems to be used for content input/output (I/O)	**N – Not Applicable**
DS-5.0.1 I/O Device Security	Implement a multi-layered network architecture for ingesting content from external networks (Internet) into the production network, and moving content from the production network to external networks.	**N – Not Applicable**
DS-5.1 I/O Device Security	Block input/output (I/O), mass storage, external storage, and mobile storage devices (e.g., USB, FireWire, Thunderbolt, SATA, SCSI, etc.) and optical media burners (e.g., DVD, Blu-Ray, CD, etc.) on all systems that handle or store content, except for systems used for content I/O.	**N – Not Applicable**
DS-6.0 System Security	Install anti-virus and anti-malware software on all workstations, servers, and SAN/NAS systems	**M – Meets Best Practice**

DS-6.1 System Security	Update all anti-virus and anti-malware definitions daily, or more frequently.	**M – Meets Best Practice**
DS-6.2 System Security	Scan all content for viruses and malware prior to ingest onto the content/production network.	**M – Meets Best Practice**
DS-6.2.1 System Security	Local firewalls should be implemented on workstations to restrict unauthorized access to the workstation.	**M – Meets Best Practice**
DS-6.3 System Security	Perform scans as follows: • Enable regular full system virus and malware scanning on all workstations • Enable full system virus and malware scans for servers and for systems connecting to a SAN/NAS.	**M – Meets Best Practice**
DS-6.4 System Security	Implement a process to regularly update systems (e.g., file transfer systems, operating systems, databases, applications, network devices) with patches/updates that remediate security vulnerabilities.	**M – Meets Best Practice**
DS-6.5 System Security	Prohibit users from being Administrators on their own workstations, unless required for software (e.g., ProTools, Clipster and authoring software such as Blu-Print, Scenarist and Toshiba). Documentation from the software provider must explicitly state that administrative rights are required.	**M – Meets Best Practice**
DS-6.6 System Security	Use cable locks on portable computing devices that handle content (e.g., laptops, tablets, towers) when they are left unattended.	**M – Meets Best Practice**

DS-6.6.1 System Security	Apply seals or tamper evident stickers on cases used for all workstations and servers that receive, send, manipulate, or store content in the production network	**M – Meets Best Practice**
DS-6.7 System Security	Implement additional security controls for laptops and portable computing storage devices that contain content or sensitive information relating to client projects. Encrypt all laptops. Use hardware-encrypted portable computing storage devices. Install remote-kill software on all laptops/mobile devices that handle content to allow remote wiping of hard drives and other storage devices.	**M – Meets Best Practice**
DS-6.8 System Security	Restrict software installation privileges to IT management.	**M – Meets Best Practice**
DS-6.9 System Security	Implement security baselines and standards to configure systems (e.g., laptops, workstations, servers, SAN/NAS) that are set up internally.	**M – Meets Best Practice**
DS-6.10 System Security	Unnecessary services and applications should be uninstalled from content transfer servers.	**M – Meets Best Practice**
DS-6.11 System Security	Maintain an inventory of systems and system components.	**M – Meets Best Practice**
DS-6.12 System Security	Document the network topology and update the diagram annually or when significant changes are made to the infrastructure.	**M – Meets Best Practice**

DS-7.0 Account Management	Establish and implement an account management process for administrator, user, and service accounts for all information systems and applications that handle content	**M – Meets Best Practice**
DS-7.1 Account Management	Maintain traceable evidence of the account management activities (e.g., approval emails, change request forms).	**M – Meets Best Practice**
DS-7.2 Account Management	Assign unique credentials on a need-to-know basis using the principles of least privilege	**M – Meets Best Practice**
DS-7.3 Account Management	Rename the default administrator accounts and other default accounts and limit the use of these accounts to special situations that require these credentials (e.g., operating system updates, patch installations, software updates).	**M – Meets Best Practice**
DS-7.4 Account Management	Segregate duties to ensure that individuals responsible for assigning access to information systems are not themselves end users of those systems (i.e., personnel should not be able to assign access to themselves).	**M – Meets Best Practice**
DS-7.5 Account Management	Monitor and audit administrator and service account activities.	**M – Meets Best Practice**
DS-7.6 Account Management	Implement a process to review user access for all information systems that handle content and remove any user accounts that no longer require access quarterly.	**B – Below Best Practice**
DS-7.7 Account Management	Restrict user access to content on a per-project basis.	**M – Meets Best Practice**

DS-7.8 Account Management	Disable or remove local accounts on systems that handle content where technically feasible.	**M – Meets Best Practice**
DS-8.0 Authentication	Enforce the use of unique usernames and passwords to access information systems.	**M – Meets Best Practice**
DS-8.1 Authentication	Enforce a strong password policy for gaining access to information systems	**M – Meets Best Practice**
DS-8.2 Authentication	Implement two-factor authentication (e.g., username/password and hard token) for remote access (e.g., VPN) to the networks.	**M – Meets Best Practice**
DS-8.2.1 Authentication	Implement two-factor authentication (e.g., username / password and hard token / verification code text message) for access to web-based e-mail (Google, Microsoft, etc.) on desktops or mobile computing devices.	**M – Meets Best Practice**
DS-8.3 Authentication	Implement password-protected screensavers or screen-lock software for servers and workstations.	**M – Meets Best Practice**
DS-8.4 Authentication	Consider implementing additional authentication mechanisms to provide a layered authentication strategy for WAN and LAN / Internal Network access.	**M – Meets Best Practice**

DS-9.0 Logging and Monitoring	Implement real-time logging and reporting systems to record and report security events; gather the following information at a minimum: • When (time stamp) • Where (source) • Who (user name) • What (content).	**M – Meets Best Practice**
DS-9.1 Logging and Monitoring	Implement a server to manage the logs in a central repository (e.g., syslog/log management server, Security Information and Event Management (SIEM) tool)	**M – Meets Best Practice**
DS-9.2 Logging and Monitoring	Configure logging systems to send automatic notifications when security events are detected in order to facilitate active response to incidents.	**M – Meets Best Practice**
DS-9.3 Logging and Monitoring	Investigate any unusual activity reported by the logging and reporting systems.	**M – Meets Best Practice**
DS-9.4 Logging and Monitoring	Review all logs weekly, and review all critical and high daily.	**M – Meets Best Practice**
DS-9.5 Logging and Monitoring	Enable logging of internal and external content movement and transfers and include the following information at a minimum: • Username · Timestamp • File name • Source IP address • Destination IP address • Event (e.g., download, view)	**M – Meets Best Practice**
DS-9.6 Logging and Monitoring	Retain logs for at least 1 year.	**M – Meets Best Practice**

DS-9.7 Logging and Monitoring	Restrict log access to the appropriate personnel.	**M – Meets Best Practice**
DS-9.8 Logging and Monitoring	Implement logging mechanisms on all systems used for the following: • Key generation • Key management • Vendor certificate management	**M – Meets Best Practice**
DS-10.0 Mobile Security	Develop a Bring Your Own Device (BYOD) policy for mobile devices accessing or storing content.	**M – Meets Best Practice**
DS-10.1 Mobile Security	Develop a list of approved applications, application stores, and application plugins/extensions for mobile devices accessing or storing content.	**M – Meets Best Practice**
DS-10.2 Mobile Security	Maintain an inventory of all mobile devices that access or store content.	**N – Not Applicable**
DS-10.3 Mobile Security	Require encryption either for the entire device or for areas of the device where content will be handled or stored.	**N – Not Applicable**
DS-10.4 Mobile Security	Prevent the circumvention of security controls.	**M – Meets Best Practice**

DS-10.5 Mobile Security	Implement a system to perform a remote wipe of a mobile device, should it be lost / stolen / compromised or otherwise necessary.	**M – Meets Best Practice**
DS-10.6 Mobile Security	Implement automatic locking of the device after 10 minutes of non-use.	**M – Meets Best Practice**
DS-10.7 Mobile Security	Manage all mobile device operating system patches and application updates.	**N – Not Applicable**
DS-10.8 Mobile Security	Enforce password policies.	**N – Not Applicable**
DS-10.9 Mobile Security	Implement a system to perform backup and restoration of mobile devices.	**N – Not Applicable**
DS-11.0 Security Techniques	Ensure that security techniques (e.g., spoiling, invisible/visible watermarking) are available for use and are applied when instructed.	**N – Not Applicable**
DS-11.1 Security Techniques	Encrypt content on hard drives or encrypt entire hard drives using a minimum of AES 128-bit, or higher, encryption by either: • File-based encryption: (i.e., encrypting the content itself) • Drive-based encryption: (i.e., encrypting the hard drive).	**N – Not Applicable**
DS-11.2 Security Techniques	Send decryption keys or passwords using an out-of-band communication protocol (i.e., not on the same storage media as the content itself).	**N – Not Applicable**

DS-11.3 Security Techniques	Implement and document key management policies and procedures.	**N – Not Applicable**
DS-11.4 Security Techniques	Encrypt content at rest and in motion, including across virtual server instances, using a minimum of AES 128-bit, or higher encryption.	**N – Not Applicable**
DS-11.5 Security Techniques	Store secret and private keys (not public keys) used to encrypt data/content in one or more of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data- encrypting key • Within a secure cryptographic device (e.g., Host Security Module (HSM) or a Pin Transaction Security (PTS) point-of-interaction device) • Has at least two full-length key components or key shares, in accordance with a security industry accepted method	**N – Not Applicable**
DS-11.6 Security Techniques	Confirm that devices on the Trusted Devices List (TDL) are appropriate based on rights owners' approval.	**N – Not Applicable**
DS-11.6.1 Security Techniques	Access to KDMs must be restricted to the KDM creator and exhibitor only.	**N – Not Applicable**
DS-11.6.2 Security Techniques	KDM creation and handling must be physically and digitally segregated from DCP handling and replication where feasible.	**N – Not Applicable**
DS-11.7 Security Techniques	Confirm the validity of content keys and ensure that expiration dates conform to client instructions.	**N – Not Applicable**

DS-12.0 Content Tracking	Implement a digital content management system to provide detailed tracking of digital content.	**M – Meets Best Practice**
DS-12.1 Content Tracking	Retain digital content movement transaction logs for one year.	**M – Meets Best Practice**
DS-12.2 Content Tracking	Review logs from digital content management system periodically and investigate anomalies.	**M – Meets Best Practice**
DS-12.3 Content Tracking	Use client AKAs ("aliases") when applicable in digital asset tracking systems.	**M – Meets Best Practice**
DS-12.4 Content Tracking	Use enterprise (not personal) versions of online or web-based collaboration services (e.g., Google Docs, etc.) for tracking content, managing inventory, or workflow management. Use multi-factor authentication and centrally managed user accounts and access to data.	**M – Meets Best Practice**
DS-13.0 Transfer Systems	Use only client-approved transfer systems that use access controls, have a minimum of AES 128-bit or higher encryption for content at rest and for content in motion, and use strong authentication for content transfer sessions.	**M – Meets Best Practice**
DS-13.1 Transfer Systems	Implement an exception process, where client prior approval must be obtained in writing, to address situations where encrypted transfer tools are not used.	**M – Meets Best Practice**
DS-14.0 Transfer Device Methodology	Implement and use dedicated systems for content transfers.	**N – Not Applicable**

DS-14.1 Transfer Device Methodology	Separate content transfer systems from administrative and production networks.	**N – Not Applicable**
DS-14.2 Transfer Device Methodology	Place content transfer systems in a Demilitarized Zone (DMZ) and not in the content/production network.	**N – Not Applicable**
DS-14.3 Transfer Device Methodology	Remove content from content transfer devices/systems immediately after successful transmission/receipt.	**N – Not Applicable**
DS-14.4 Transfer Device Methodology	Send automatic notifications to the production coordinator(s) upon outbound content transmission.	**N – Not Applicable**
DS-15.0 Client Portal	Restrict access to web portals which are used for transferring content, streaming content and key distribution to authorized users.	**M – Meets Best Practice**
DS-15.1 Client Portal	Assign unique credentials (e.g., username and password) to portal users and distribute credentials to clients securely.	**M – Meets Best Practice**
DS-15.2 Client Portal	Ensure users only have access to their own digital assets (i.e., client A must not have access to client B's content).	**M – Meets Best Practice**
DS-15.3 Client Portal	Place the web portal on a dedicated server in the DMZ and limit access to/from specific IPs and protocols.	**M – Meets Best Practice**

DS-15.4 Client Portal	Prohibit the use of third-party production software/systems/services that are hosted on an internet web server unless approved by client in advance.	**M – Meets Best Practice**
DS-15.5 Client Portal	Use HTTPS and enforce use of a strong cipher suite (e.g., TLS v1) for the internal/external web portal.	**M – Meets Best Practice**
DS-15.6 Client Portal	Do not use persistent cookies or cookies that store credentials in plaintext.	**M – Meets Best Practice**
DS-15.7 Client Portal	Set access to content on internal or external portals to expire automatically at predefined intervals, where configurable.	**M – Meets Best Practice**
DS-15.8 Client Portal	Test for web application vulnerabilities quarterly and remediate any validated issues.	**M – Meets Best Practice**
DS-15.9 Client Portal	Perform annual penetration testing of web applications and remediate any validated issues.	**M – Meets Best Practice**
DS-15.10 Client Portal	Allow only authorized personnel to request the establishment of a connection with the telecom service provider.	**M – Meets Best Practice**
DS-15.11 Client Portal	Prohibit transmission of content using email (including webmail).	**M – Meets Best Practice**
DS-15.12 Client Portal	Review access to the client web portal at least quarterly.	**M – Meets Best Practice**

Document Version Control

Version	Date	Changes Made	Author
1.0	11/6/2018	Initial Draft	Adoriel Bethishou
1.1	11/7/2018	Draft Review Round 1	Michael Ballantyne
1.2	11/9/2018	Draft Review Round 2	David Grazer
1.3	2/7/2019	Revisions per Client Request	Adoriel Bethishou
1.4	2/25/2019	Revisions per Evidence Obtained	Adoriel Bethishou
1.5	3/8/2019	Revisions per Evidence Obtained	Adoriel Bethishou

TEVORA™

Assessor Profiles

Christina Whiting, Managing Director of Enterprise Risk and Governance

Primary Role

As Tevora's Managing Director of Privacy, Enterprise Risk and Compliance, Christina's primary role is to assist our clients in aligning their security strategies with their business goals. With over 20 years of experience in the security and risk space, she helps organizations design, establish, and mature their privacy and security programs and capitalize on efficiency. Christina also mentors' junior consultants, manages client relationships, assists with pre-sales and post sales activities, and oversees all projects from inception to the closeout presentation to ensure that every project exceeds our client expectations.

Notable Accomplishments

With a diverse background in Education, Finance, Healthcare, Entertainment, Manufacturing, and Hospitality, Christina brings vast knowledge in both business and security to our clients. Her experience in security assessments, security strategy, risk management, privacy, compliance, governance, data loss prevention and vendor management adds value to both our practice and to our client's engagements.

Christina holds a bachelor's degree in Electronic Engineering and Information Technology, a Master's degree in Management Information Systems and is a PhD candidate in Information Security and Assurance, graduating all magna cum laude. She has been inducted into all notable security and computer science honor societies including Alpha Beta Kappa National Honor Fraternity, Alpha Chi National Honor Fraternity, and Upsilon Pi Epsilon National Honor Fraternity. Christina has presented on security and risk topics at regional conferences on the east and west coast. Also, an Information Security Instructor at University of California Irvine. Currently an Executive MBA student at MIT.

Certification and Training

Christina holds the following certifications: PCI QSA, PA-DSS QSA, Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), ISO 27001 Lead Auditor, Cobit, HITRUST Security Assessor (HSA), and a certification from the National Security Agency (NSA) Committee on National Security Systems (CNASS) in Information Security

Management (ISO 17799).

Tenure	Christina has been with Tevora since 2012.

TEVORA™

David Grazer, Senior Information Security and Privacy Consultant

Primary Role

David is a consultant responsible for leading projects within the Privacy, Enterprise Risk Management and Compliance practice areas. He works in direct support of the managing director ensuring that projects are delivered on time and within scope. He is the main day to day contact for all client engagements.

Notable Accomplishments

With a diverse background within both enterprise and consumer technology companies, David brings a unique vantage point to his engagements. Taking a holistic approach to assessing how security affects not only the technological infrastructure, but also business objectives. He marries those views when advising on potential remediation or solutions.

David possesses a bachelor's degree in business and communications from Chapman University, a graduate certificate in Global Finance from Thunderbird School of Global Management and has completed various Information Systems Security courses at UCLA Extension.

Certification and Training

David is a CIPP/US credential holder and is in the process of obtaining his CIPM and CRISC credentials.

Tenure

David has been with Tevora since November 2016.

TEVORA™

Adoriel Bethishou, Information Security Associate

Primary Role

Adoriel is an information security associate with experience in assessing information technology environments for business organizations across multiple industries. He acts as the technical resource for assessment projects, primarily responsible for research, artifact review, conducting interviews, analyzing control gaps and producing project deliverables.

Notable Accomplishments

Brought into Tevora through the Consultant Development program, Adoriel has proven to be a great fit at Tevora. Due to his technical knowledge and analytical approach to projects, he has been able to excel at learning a variety of practice areas. Adoriel is currently a member of the Privacy team, where he primarily assists with GDPR compliance and vendor management.

As an associate at Tevora, Adoriel has assisted with Data Privacy, Vendor Management, and PCI DSS projects. He continues to work closely with senior consultants to develop and strengthen his security and compliance knowledge.

Certification and Training

Adoriel has a Bachelor of Science Degree in Informatics from the University of California, Irvine, with a specialty in Organizations and Information Technology and is currently working towards obtaining his Certified Information Systems Auditor (CISA) certification.

Tenure

Adoriel has been with Tevora since June 2018.

Go forward. We've got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management