Risk Assessment Exception : 464194

First Published: 8/16/2017 1:42 PM Last Updated: 11/16/2017 4:30 PM

Extend/Update Request

Extend/Update Exception Form

Request	Author	Date of Extension/Update Request	Purpose
No Records Found			

Assessment

Risk Assessment Exception Request Form

Risk Assessment ID:	464194	**Overall Status:**	In Process
Historic Risk Assessment Name:		**Review Stage:**	Awaiting Author Submission to Manager
Division:	Information Technology	**Exception Duration:**	180 Days
Assessment Type:	RA	**Expiration Date:**	2/12/2018
Issue:	MacOS Use	**Days to Expiration:**	63
Data Classification:	Confidential	**Approved Date:**	
Subject:	To allow the aggregate risk of the current state of MacOS Device use at Delta		
Requestor:	Lewis, Robert	**Requestor Phone:**	
Requestor Submission Status:	Submitted	**Date of Request:**	8/16/2017

Business Background Information

Business Background Information:

Risk Assessment Purpose: Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta.

Risk Assessment Scope: This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development

- IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of June 2017, AirWatch reports 150 enrolled MacOSX devices (excludes iOS)

Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) –Acquisition and Outsourcing negotiations.

Known Improvement Efforts:

- Other MDM solutions are being considered such as Jamf in lieu of AirWatch.
  - As of August 2017, direction has shifted to AirWatch and Apple DEP management by Insight.
- Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.
- Delta is in negotiations (or plans to negotiate) outsourcing support of Macs.
  - ~~CDW Direct, LLC SoW for End-to-End Mac support is being drafted.~~ (See Below)
  - Insight Direct USA, Inc. SoW is being drafted for Standard Imaging, POC, and On-Site Support (August 2017, see attachment.)
  - Other companies, such as Stratix/Apple Business, are being considered.

Existing Mitigating Controls

Existing Mitigating Controls:

(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are established, but compliance with Delta's standards are partial or unknown.)

- AirWatch (Mobile Device Management)
    - Enforces pin code policy:
        - Session timeout: 15 Min. (§ 11.4.3)
        - (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2))
    - In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1)
- Symantec Endpoint Protection
    - Installed and configured to match Windows scan times.
        - (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.)
    - (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3))
- Pulse Client (VPN Access)
    - Access requested via Ishop.
    - Certificate deployed by AirWatch. (§ 11.5.3)
    - Requires SEP and AirWatch to be installed before allowing connections.
        - (NOTE: May not be compliant with "must meet baseline security standards" because none have been formally established.) (§ 11.5.3)
- Software Updates
    - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
        - (NOTE: Updates are not centrally managed. (§ 10.1.3))
    - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
    - Devices are assigned a name (X/WATLMAC0000x)
    - Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1)
    - All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1)
        - (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))

Are there recommended mitigating controls?:

Yes

Recommended Mitigating Controls:	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the MacOSX CIS Benchmarks (as is currently done for other systems). ○ Security Standard 12.1.1 required analysis must be completed early in this process. ○ As of August 2017, the Insight SoW mandates Insight collaborate with Delta to provide "as-built" documentation during initital configurations. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.

Remediation Strategy to Achieve Compliance with Information Security Policy and Standards

Remediation Strategy:

- Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section.
  - Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible.
- Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed):
  - Active Directory Integration
  - MacOS Client Directory integration
    - Kerberos
    - SSO
    - Password policies
    - Local accounts vs mobile
    - Admin accounts vs standard
  - Print queues
  - SharePoint / DFS
  - Wireless (e.g., 802.1x, Certs, WPA)
  - VPN
  - Cisco ISE
  - Cisco FastLane
  - Proxy servers
  - Airwatch enrollment
  - Build a new standard configuration / new image
  - Current build / configuration process
  - Onboarding / off-boarding process
  - Reporting
  - Airwatch access
  - Recommended settings for MacOS
  - Windows vs MacOS security gap analysis
  - Role of Airwatch in security
  - Profile build outs and discussions
  - Password policies
  - Encryption
  - Antivirus options
  - Lost Mode, Remote Wipe, Activation Lock
  - Best practices
  - Endpoint backup options

Control Standards Impacted

Category Number	Standard Path	Standard Name	Statement	Status
07	07. Management of Information Assets &nbsp07.1. Identification of Assets &nbsp07.1.1. Asset Inventory	Asset Inventory	Asset Owners create and maintain an inventory of information assets within their control that includes: • **Classification**: This specifies the sensitivity and security requirements of the asset. See section 7.3.1 for details. • **Format**: This can include, but is not limited to, paper, CD, magnetic tape, thumb drive, e-mail, electronic file or database • **Location**: This identifies where the asset is stored and retained, such as a filing cabinet, database, corporate records repository or other location where the asset can be found	Published

			• **Backup Information**: This identifies if the asset is backed up, and if so, at what location • **Retention Schedule**: This identifies the duration of time the asset is retained. The asset inventory is to be reviewed and at a minimum updated annually to maintain accuracy	
07	07. Management of Information Assets &nbsp07.2. Ownership of Assets &nbsp07.2.1. Designated Owner	Designated Owner	All Delta information assets must have a designated owner. By default, the asset creator/acquirer is the asset owner. The asset owner is responsible for assigning classification and ensuring all activities and actions required under this Standard and any other regulation or law are implemented. If there is a question of ownership, CyberSecurity Governance or Corporate Records and Information Management (CRIM) will facilitate the assignment of an owner. There may be instances where records created by one originating department become important records for another department. An example of this type of record might be a purchase order originated by the Purchasing Department which becomes part of the Accounting Department's support of payment. In such instances, each originating department will be responsible for ensuring compliance with the established retention schedule for the records created by that department. **Roles and Responsibilities** Asset Owners (Originating Department) • Identify assets • Classify assets for security, storage and retention purposes • Define and periodically review access restrictions and access control. A custodian, e.g., a System Administrator or Information Technology group, can be delegated to have the daily primary management responsibility, but the responsibility and accountability for the asset remain with the asset owner • Periodically inventory assets • Manage each asset according to the security, storage and retention requirements specified for appropriate classifications throughout its lifecycle Corporate Records Information Management (CRIM) • Delta’s official records management resource • Maintains Delta’s Records Retention Program, which includes ensuring the adoption of governing policies while establishing guidelines and practices • CRIM communicates changes and updates to the Records Retention	Published

			Program Information Technology Department (IT) • Provides technical support to the owners of electronic information assets throughout the asset lifecycle, managing , where appropriate: ○ Access control (systems, applications and data) ○ Asset operational maintenance ○ Backup and Storage Law (Delta Legal) • Ensures compliance with Delta's Records Retention Policy • Governs a legal hold and management process	
07	07. Management of Information Assets &nbsp07.3. Information Classification &nbsp07.3.1. Classification Guidelines	Classification Guidelines	Asset owners are responsible for assigning appropriate security classifications for assets they manage. If a classification is absent for an asset, it is assigned a default classification of Confidential and managed accordingly. Security classifications must be reviewed and/or revised annually and at any other appropriate time during the asset's lifecycle. The following chart is meant to assist in the classification of information at Delta Air Lines and to provide guidelines for the lifecycle of the information It is the responsibility of information asset owners to appropriately apply the guidelines for the information they manage.	Published

Classification	**Description**	**Examples**
Restricted	Assets whose loss, corruption or unauthorized disclosure would result in severe financial, reputation and legal loss. Statutorily protected and/or industry-regulated assets.	Trade secrets, Aircraft incident records, Passenger credit card data, Social Security Numbers, Strategic planning information, Critical financial data prior to public disclosure, Legal proceedings,

		Authentication passwords, and Information security incidents
Confidential	Assets whose loss, corruption or unauthorized disclosure would have an adverse impact on the company, its customers. An asset loss that may result in financial loss, reputation damage and/or legal action.	Personally Identifiable Information, Sensitive Security Information, Aircraft Situation Display to Industry Class One data (ASDI), Aircraft maintenance records, Contracts, HR information, Electronic data tapes,

		and Video surveillance media
InternalUse	Information not approved for general circulation outside Delta, where its disclosure would inconvenience the organization or management, but is unlikely to result in financial loss, liability or serious damage to Delta’s credibility or reputation.	Commonly available materials across Delta including: policies, procedures, employee directories, and organizational charts
Public	Information in the publi	Public website, Press releases, Corporate

	c domain approved for general public use and distribution.	magazines, Public statements, Investor/analyst communications, Annual reports, SEC-reported financials

07	07. Management of Information Assets &nbsp07.4. Information Handling &nbsp07.4.1. Information Handling Procedures	Information Handling Procedures	Information Handling Procedures apply to all Delta information assets regardless of whether they are hosted by a third party, e.g., cloud service deployment, or hosted internally within Delta's own environment. See the chart on the following page for prescribed handling procedures for all data classifications: *Public, Internal, Confidential* and *Restricted*	Published

	Restricted
Access	Access to the information is strict limited to the minimum number o must have access to the informat access requires two-factor authe sign on is not permitted. If information is stored in the Clou accessible in a readable format u
Labeling	Physical assets must have a labe have labels embedded in the doc
Data Cloaking	In the event that Delta's Operatio the integrity of all records (physic

	Restricted

Storage	The asset must be protected for in ensure no unauthorized alteration. Physical media will be stored and desk, cabinet, container, enclosed center. Electronic media stored on premis be stored encrypted or otherwise data is backed up as required by tl owner. Prior to storing data in the assessment must be completed ar provided of compliance with all Info Procedures. If hosted in the Cloud, Delta's data segmented and separated from th clients of the service provider.
Session Timeout	15 minutes
Transporting / Transmitting	Physical media that will be transpo Delta facility must be inventoried p transportation, shipped securely by and confirmation of receipt must b All electronic information being tra or externally, including information to and from the Cloud, must be en made unreadable if intercepted.
Logging	All systems that handle restricted includes the following: user Id of p component or resource. Cloud service providers must be a
Third Parties	Third parties must sign a confider contracted to handle data subject must provide proof of their complia of these special types is transferre
Inventory	All assets must be inventoried at
Retention	The Delta Corporate Records and process or as specified by industry https://deltaairlines.sharepoint.com
Destruction	Physical and electronic media wil possible. For paper, this is by cros wiped before disposal using metho

10	10. Communications and Operations Management &nbsp10.1. Operations Management &nbsp10.1.1. Documented Operating Procedures	Documented Operating Procedures	Each IT system is required to have documented operating procedures to ensure continuity and consistency. Documented procedures provide detailed instructions for how each job or task is performed including: • Processing and handling of information • Job scheduling • Backup and recovery • Error handling • Restart and recovery procedures • Output and media handling	Published

			Documentation identifies resources to be contacted when operational or technical problems occur. Documented procedures are current and accessible to all users who need them. All changes to operating procedure documents are authorized and controlled by the system owner.	
10	10. Communications and Operations Management &nbsp10.1. Operations Management &nbsp10.1.3. System Patches	System Patches	Identification System patching activities are applicable to hardware, operating systems, systems software (e.g. databases), and third party application software. In order to maintain current patches on all systems, CyberThreat Unit (CTU) performs daily checks of vulnerability announcements, reviews the security vulnerabilities and assigns risk. Once security vulnerability is obtained, it is reviewed for relevance to the Delta environment, a risk rating is assigned, and the remediation steps reviewed for impact. When a new security bulletin is released, all related information is compiled from the vendor and reviewed. A Vulnerability Note or Assessment is generated if the vulnerability is relevant to Delta. When a new security bulletin is released, all related information is compiled from the vendor and reviewed. This information includes the following: • Date of Notification of Vulnerability • Impact of Vulnerability (Both Delta and vendor) • Severity Rating (if applicable) • Affected Software • Vulnerability Details • Remediation: Work-around or Patch Update **Evaluation** Published vulnerabilities are reviewed to check for applicability to Delta systems with affected operating systems, platforms (Unix, Wintel, router, switch), services running, hardware, system exposures, and installed software versions. Reviews are performed by the appropriate component, application, or hardware owner. A component owner may challenge the risk assessment from the CyberThreat Unit (CTU) rating process, however ultimate responsibility for remediation remains with the owner. Arbitration by CyberSecurity Governance and approval of an exception may alter the following remediation requirements. A risk rating will be assigned by the vendor or by component owners. However, Information Security uses the following risk rating scale to	Published

evaluate vulnerabilities:

- **Critical**: A critical vulnerability gets immediate scrutiny by the CyberThreat Unit (CTU). Within one business day the vulnerability whose exploitation could impact Delta's critical flight operations is reviewed, evaluated and disseminated to the appropriate component/application/hardware owner for remediation action.
- **High**: A high vulnerability is reviewed, evaluated, and disseminated within two business days. It is a vulnerability whose exploitation could result in a compromise of the confidentiality, integrity, or availability of users' data, or the integrity or availability of processing resources.
- **Medium**: A medium vulnerability will be reviewed, evaluated and published within three business days. It is a vulnerability whose exploitability is mitigated to a significant degree by factors such as: default configuration, hardware filtering, auditing, or difficulty of exploitation.
- **Low**: A low vulnerability is reviewed, evaluated and published within seven business days. It is a vulnerability whose exploitation is extremely difficult, or whose impact is minimal.

It is recommended that the guidance provided by NIST Common Vulnerability Scoring System (CVSS) v. 2 or newer be used for risk assessments. (http://nvd.nist.gov/cvss.cfm?calculator&version=2).

Disagreements between assessments by component, application, or hardware owner are arbitrated by the CyberSecurity Governance and risk responsibility accepted by owner and CyberSecurity Governance. CTU team ratings remain as identified with exception as approved by CyberSecurity Governance.

Remediation

- **Critical**: 7 days
- **High**: 30 days
- **Medium**: 60 days
- **Low**: 90 days

If a patch deployment is scheduled, all lower priority patches are deployed. For example, if it is decided to push a high priority patch, any outstanding low priority items must also be pushed. Exception: Critical patches, due to their out-of-band nature, do not require pending patch deployment.

Testing

Each patch will be tested in a lab environment.

			The package is deployed and tested within the TEST and/or DEV environment to ensure there are no adverse effects before being applied to any SI or Production system, with the exception of critical rated patches which require immediate remediation to prevent exploitation. **Deployment** Whenever possible, security-related updates are deployed in groups to minimize the effect of rebooting and accessing the servers The change window schedule is documented by the platform owners This schedule contains the following: • Change window timeline from patch notification to patch implementation • Time limit of no more than thirty days whenever possible for implementation of patch Occasionally, updates require deployment through the use of a custom script file or batch file requiring administrator input. All deployments are documented with change management in case there are issues with the install. The contents of this documentation will assist in the complete removal of the update if a problem arises. Patches are installed in the following order: • Development servers are patched first, and may be patched during normal operating hours • System Integration servers are patched after the DEV servers, and may be patched during normal operating hours • Production servers are the last group to be patched and are patched during normal change windows as defined by the platform owners **Rollback** During the patching process, testing of every update is completed but sometimes not all flaws will be discovered in test. If an update that was released into the environment causes disruption to the environment, the implementation is rolled back and out of production. If the update is not able to be uninstalled, the system state must be restored from the backup.	
10	10. Communications and Operations Management &nbsp10.4. Network Management &nbsp10.4.4. Hardening Network Devices	Hardening Network Devices	Delta network devices must be configured according to approved guidelines based on industry hardening standards. Hardening standards will be reviewed and updated annually or when new vulnerabilities are identified. Delta has adopted the Center for Internet Security (CIS) baselines for hardening standards. Specific standards vary for different systems, but general guidelines include:	Published

			• Delete/disable unnecessary applications, functions and services • Only one primary function will be implemented on any device used to process and/or store customer credit card data • Do not use insecure communication protocols (e.g., Telnet, FTP) to access or transfer information containing passwords or any other content with a classification of Confidential or Restricted • Delete/deactivate unused or inactive user accounts • Change all default user and admin account passwords • Close unnecessary communication ports • Enable automatic updates for operating system and security patches • Enable activity logging and mirror logs to secured storage • Only approved products are installed on Delta owned assets (product list is owned and maintained by Delta's Enterprise Architecture group) • Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. • Configure system security parameters to prevent misuse. Information on specific system baselines is found on the CIS web site, http://www.cisecurity.org. Installation and operation procedures must follow industry best practices. Compliance with these configuration and operating standards must be regularly checked via automated tools or manual review, at least annually, or more often as prescribed by legal and regulatory requirements. Vendor specific security checklists might also be used to supplement guidelines, where they add greater protection. Procedures exist for controlling physical and logical access to diagnostic and configuration ports. Access ports that no longer support authorized connections must be disconnected and unused cables removed from network components.	
10	10. Communications and Operations Management &nbsp10.4. Network Management &nbsp10.4.5. Evaluating Network Security	Evaluating Network Security	Only resource administrators or third parties approved by CyberSecurity Governance are authorized to implement traffic and activity monitoring tools on Delta networks and information resources. Delta has implemented a multi-faceted approach to evaluate network security. This includes the following procedures:	Published

			• Internal threat and vulnerability assessments are performed quarterly using an automated vulnerability scanner • Internal assessments of our wireless environment are performed quarterly • Third party attack and penetration test are performed on an annual basis • Automated daily log reviews occur for network related components in sensitive processing environments Test results are used to evaluate current risks and create action plans to remediate operational security gaps discovered.	
10	10. Communications and Operations Management &nbsp10.4. Network Management &nbsp10.4.6. Controls against Malicious Code	Controls against Malicious Code	All information technology systems will employ an approved endpoint security solution to include anti- virus and firewall appropriate to those systems. The endpoint security solution must be maintained with the current available version. Filtering technology will be deployed to reduce the risk of malicious code entering Delta's computing environment through web browser vulnerabilities, web browsing user error, and other paths such as e- mail, e-mail attachments, and FTP traffic.	Published
10	10. Communications and Operations Management &nbsp10.7. Cryptographic Controls &nbsp10.7.1. Cryptographic Controls	Cryptographic Controls	Information classified as Confidential or Restricted shall be encrypted in storage and in transit. Such information must not be sent over the Internet (e.g., e-mail, FTP), via Remote Access or other external networks unless the message is using an encryption technology approved by CyberSecurity Governance. Examples of information that must be encrypted include, but are not limited to: • Credit card numbers or other cardholder information • Passwords • Research and development information • Employee social security numbers Employee healthcare related information Refer to section 7.4.1. for the Information Asset Security Classification Chart. When employing public key cryptography in a production environment, the public and private key pairs must be issued by an approved certificate authority. Certificate validity dates must be monitored and renewals made on a timely basis to keep all operational certificates current. The use of expired certificates is not allowed. Self-signed certificates are not to be used in production without a completed risk assessment performed by CyberSecurity Governance.	Published

			The Delta Air Lines PKI Policy Management Authority (PMA) provides governance of internal PKI activities and the implementation of trust relationships with external PKI entities, contact crypto@delta.com for help and information.	
10	10. Communications and Operations Management &nbsp10.8. Logging & Monitoring &nbsp10.8.2. Monitoring System Use	Monitoring System Use	All use of an information processing facility shall be monitored. The use of a system is monitored for security risks, known attack patterns, and activity thresholds. Integrity checking mechanisms are used to verify software, firmware, and information integrity. Auditing will record all actions performed by technical support (system operators, system managers, system engineers, and system administrators), including any emergency actions performed by support personnel. Areas that must be audited and monitored include: • All user login attempts • All privileged operations ○ Use of privileged accounts ○ System start-up and shut-down • Unauthorized access attempts ○ Failed or rejected user actions ○ Failed or rejected actions involving data and other resources ○ Access policy violations ○ Alerts from intrusion detection systems • System alerts or failures • Changes to, or attempts to change critical system files, directories, processes, and system security settings and controls • Attempts to initialize or remove system or application logs If any condition is identified that appears to be outside of normal operation, an alert is generated and sent to the CyberThreat Unit (CTU) for further investigation.	Published
10	10. Communications and Operations Management &nbsp10.8. Logging & Monitoring &nbsp10.8.3. Administrator and Operator Logs	Administrator and Operator Logs	System administrator and system operator activities must be logged. Logs must include: • Time at which the event occurred • Information about the event or failure • Which account and which administrator was involved • Which processes are involved System administrator logs are to be regularly reviewed by either the Managed Security Provider or the CyberThreat Unit (CTU).	Published
10	10. Communications	Fault Logging	System faults must be logged, analyzed, and	Published

	and Operations Management &nbsp10.8. Logging & Monitoring &nbsp10.8.4. Fault Logging		appropriate action taken. Faults reported by users or systems must be logged. Error logging must be enabled for all systems and applications on which it is available. Consideration shall be given to the possibility of performance degradation when configuring error logging.	
10	10. Communications and Operations Management &nbsp10.8. Logging & Monitoring &nbsp10.8.6. Log Retention	Log Retention	Audit trail history must be readily accessible for a minimum of three (3) months and retrievable for a minimum of one year, subject to local laws.	Published
11	11. Access Control &nbsp11.3. Privileged Access &nbsp11.3.1. Privileged User Access	Privileged User Access	All users that have privileged access rights must have their own personal accounts for normal business use. Shared “super-user” or privileged access accounts must never be logged into directly if their usage cannot be tracked. Administrators must not use the same password for their administrator accounts and any accounts they have for general use. Privileged access accounts must maintain a unique password for that account, different from that of any other user or admin accounts. A privileged access account may or may not be associated with an individual. If the account is not associated with an individual, it must provide an audit trail pointing back to an authorizing user. These accounts must be kept to a minimum, individually approved, documented and strictly limited to those with a business justification. Emergency privileged access may be invoked by contacting the Help Desk at 404-714-4357. Only the level of access needed to resolve the emergency will be granted and the granted access must be revoked as soon as the emergency is resolved. A log must be kept detailing the rationale for granting access, who approved it, who was granted access, what actions were taken with the access, and when the access was granted and revoked.	Published
11	11. Access Control &nbsp11.4. Account Management &nbsp11.4.2. Password Management Program	Password Management Program	**Password Strength** All passwords must be sufficiently strong to prevent guessing or hacking in accordance with the following requirements: • They must be a minimum of eight (8) characters long • They must be composed of both alpha and numeric characters • They must contain both uppercase and lowercase alpha characters, where	Published

			supported • They must be changed at least every 90 days • A user may not have a new password that is the same as any of the previous four (4) passwords • User IDs must be disabled after a maximum of six (6) consecutive failed login attempts. • Users must contact the Help Desk or an Identity Access Management (IAM) Administrator to unlock a disabled account. **Failed Login Message** Message displayed after failed login attempt provides information necessary for corrective action without revealing information about a user's credentials that could be exploited to gain access to Delta's information assets, e.g., 'Either the User ID or Password Entered is Not Valid'. **Password Storage** Passwords must be stored using one way encryption or hashing, where a password cannot be decrypted into clear text. Passwords must never be written down or stored on information systems in an unprotected form. **Temporary Passwords** If the use of a temporary password is required to establish a user's initial access or to facilitate a password reset, the temporary password will meet the following conditions: • Temporary passwords are set to a unique value • Temporary passwords must be changed immediately upon logging on to the initial session • Temporary passwords must comply with the same password standards as permanent passwords **Password Resets** Password resets may be issued only after validating a user's identity via photo ID or challenge/response questions and will only be communicated in a secure manner by one of the following: • Face-to-face • E-mail to company mailbox • Phone contact • Company interoffice mailer containing a sealed envelope to the user's intra-company mail drop • US Postal mail to the user's home	
11	11. Access Control &nbsp11.4. Account Management	Session Time-out	Systems must automatically lock the application if a session has been idle (no keystroke, mouse or touch screen activity) that exceeds time limit	Published

	&nbsp11.4.3. Session Time-out		based on classification of data as determined in the Information Handling Guidelines, Section 7.4.1. The user must re-enter the password to re-activate the application.	
11	11. Access Control &nbsp11.4. Account Management &nbsp11.4.5. User Access Review	User Access Review	System access rights must be reviewed at periodic intervals to ensure that the access rights remain valid. Access reviews are done on systems containing Confidential or Restricted information every 90 days. It is the responsibility of the employee’s manager to ensure that access rights to business systems are modified or revoked when an employee moves to a new position or group.	Published
11	11. Access Control &nbsp11.5. Network Access &nbsp11.5.1. Authorized Access	Authorized Access	Logical controls (identification, authentication, authorization) are in place to ensure only authorized users access Delta network services and information assets. Accounts provide access only to those network systems and applications for which they have an authorized business use. Only Delta-owned devices are allowed to connect directly to the Delta network. For the purpose of this Standard, Delta considers two factor authentication to be a type of multi-factor authentication. Furthermore, Delta uses the definition of the terms "Multi-factor" and "Token" as specified in the National Institute of Standards and Technology (NIST) Special Publication 800-63, Electronic Authentication Guideline. Authentication using a user ID and password would be an example of single factor authentication. Authentication using a user ID and a password and a Verisign hardware token would be an example of two factor authentication. Authentication using a user ID and password and a cookie that identifies the user’s device as a trusted device would be an example of multi-token authentication.	Published
11	11. Access Control &nbsp11.5. Network Access &nbsp11.5.3. Remote Access Process	Remote Access Process	Remote users to Delta's corporate network must authenticate using two factor authentication. Devices used to access Delta’s corporate network must meet baseline security standards including current levels of malware protection and critical software patches. When accessing Delta's corporate network remotely, it is prohibited to copy, move, or store Confidential or Restricted data onto local hard drives or removable electronic media devices that are not provided and managed by Delta for this purpose. Technologies such as Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access Control System (TACACS) with	Published

			multi-factor tokens or VPN with individual certificates must be used. When accessing Delta's corporate network remotely, the session must be disconnected after 15 minutes of inactivity. Remote access that is setup for vendors or business partners is monitored when in use. Vendor remote access is activated only when needed and is immediately deactivated after its use.	
12	12. System Acquisition, Development & Maintenance &nbsp12.1. System Security Requirements &nbsp12.1.1. Security Requirements	Security Requirements	During the business requirements and analysis phase of systems development, the definition of security requirements must be completed. Security requirements include: • Data classification • Business data owner • User and roles definition • User and roles access requirements • Network access requirements • System availability and disaster recovery requirements • Data integrity and confidentiality requirements • FAA, HIPAA, PCI, SOX,TSA or any other government or regulatory requirements • System attack surface analysis • Security control requirements • Data backup requirements • Security control requirements • Outage windows for hardware, OS, systems software and application software maintenance and patches.	Published
12	12. System Acquisition, Development & Maintenance &nbsp12.2. Application Development Security &nbsp12.2.2. Access Control to Program Source Code	Access Control to Program Source Code	System source code control and versioning is implemented to ensure the ability to recover different releases of the system and allow roll-back and roll-forward capabilities. Access to system source code is limited to authorized individuals whose current job responsibilities require it. Requirements for access to source code shall be reviewed at least annually, and will be terminated for any user without a current valid business need or operations responsibility requiring access. Access to source code must be monitored and logged.	Published
12	12. System Acquisition, Development & Maintenance &nbsp12.3. System Management Security &nbsp12.3.2. System Documentation	System Documentation	System Owner maintains accurate and complete documentation covering production hardware and software. System documentation is stored securely but easily accessible by authorized parties and includes: operator manuals, user guides, configuration specifications, security baselines and recovery plans.	Published

			Timely documentation updates are made for all system and component changes.	
14	14. IT Business Continuity and Disaster Recovery &nbsp14.1. IT Business Continuity and Disaster Recovery Programs &nbsp14.1.1. IT Business Impact Analysis	IT Business Impact Analysis	A business impact analysis must be done to define Delta’s core business functions and the IT resources that support them. Based on the criticality of the functions that IT systems are determined to support, business owners must classify all IT systems and assign each a Recovery Priority and a Severity Level • Recovery Priority (RP) is assigned to identify the priority given a system’s operations and its position in the sequence of restoration, defining when it must be recovered in the event of a disaster (See Table 14-1 below) • Severity Level (SL) is assigned to signify the severity of the impact on core business operations in the event the system becomes unavailable The severity level helps to determine the escalation and response process to system problems during normal operations (See Table 14-2 below) If the Recovery Priority and/or Severity Level of a system requires changing, business owners must engage their IT Management contact to facilitate the change. All information technology (IT) systems used to support Delta’s business must have an Operational (Ops) Plan. The plan is maintained throughout the lifetime of the system to ensure the accuracy of system contacts, architectural design, and other system attributes. The attributes identified through a Business Impact Analysis (RP, SL, operating- and system dependencies) will be incorporated into the Operational Plan. Systems are defined as technology elements: • That are supported by Delta IT • That are supported by other companies (e.g., Travelport, IBM, Affiliated Computer Services, Unisys) where Delta IT is responsible for the relationship • That when grouped together deliver one or more related business functions • That share a common architecture (e.g. server, database, middleware, applications)	Published
14	14. IT Business Continuity and Disaster Recovery &nbsp14.2. IT Business Continuity and Disaster Recovery Planning &nbsp14.2.1. IT	IT Business Continuity Operational Plans	An Operational Plan must include, at a minimum: 1. System Profile 2. Data Flow Diagram 3. Operations Support and Organizational Communication Plan 4. Operations Troubleshooting	Published

	Business Continuity Operational Plans		Procedures 5. Recovery Procedures	
15	15. Compliance &nbsp15.1. Compliance &nbsp15.1.1. Identification of Applicable Legislation	Identification of Applicable Legislation	Asset owners or their designee must ensure that all security procedures and controls within their areas of responsibility are carried out correctly to achieve compliance with legal and regulatory requirements as well as privacy and security policy and standards. Asset owners or their designees must regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements. If any non-compliance is found as a result of the review, the asset owners or their designees will: • Determine the cause of non-compliance • Evaluate the need for actions to ensure the non-compliance does not recur • Determine and implement appropriate corrective action • Review the corrective action taken Results of the reviews and corrective actions carried out by asset owners or their designees must be recorded and these records must be maintained. The asset owners report the results to the person carrying out the independent reviews when the independent review takes place in their area of responsibility.	Published
15	15. Compliance &nbsp15.1. Compliance &nbsp15.1.3. Automated Audit Tools	Automated Audit Tools	Automated audit tools are classified as Restricted. Possession, distribution or use of network diagnostic, monitoring and scanning tools is limited to designated and authorized personnel in accordance with their job responsibilities. This includes anything which can replicate the functions of such tools. Authorization for use of such tools can only be granted by asset owner. Unauthorized possession, use or distribution of such tool is prohibited and may be grounds for immediate termination.	Published

Regulatory Constraints

Regulatory Constraints ⍰ Source:		**Regulatory Contstraints Comments:**	Because present/authorized assets (data in use/data at rest) on Mac devices are not thoroughly identified, applicability of regulatory contraints is not known.
Regulatory Constraints ⍰ Topic:			
Regulatory Constraints ⍰ Section:			
Regulatory Constraints ⍰ Sub Section:			

Risk Rating Worksheet

Risk Rating Worksheet (To be filled out by CyberSecurity Governance)

Risks are related to *the things that could happen as a result of being out of compliance*, like inadvertent data exposure or unauthorized access to confidential information. The more likely an event will happen, and the greater the business impact, the higher the risk.

Accessing Risk

Risk Rating Scale

The Potential Impact field measures how an event could impact cost, technical performance, and/or reputation. Values available for selection are given below with corresponding definitions.

- High (Severe damage, 3 points)
- Medium (Minor damage, 2 points)
- Low (Little to no damage, 1 point)

The Probability field measures the likelihood of an event occurring. Values available for selection are given below with corresponding definitions.

- High (Likely to occur, 3 points)
- Medium (Somewhat likely, 2 points)
- Low (Not likely, 1 point)

The Business Impact field is automatically calculated by multiplying the point values of the Potential Impact and Probability fields.

- High (9 total points)
- Medium (4-8 points)
- Low (1-3 points)

Level of Control Rating Scale

1 - Appropriate security measures; Security procedures consistently followed; Documented security policy/ procedures; Continuous auditing
2 - Mitigating controls in place; No consistent enforcement
3 - Security procedures not consistently followed; Weak mitigating controls; No enforcement
4 - Security policy and procedures exist but are not documented; Security procedures are done on an ad-hoc ; No mitigating controls; No enforcement; Third party employees involved
5 - Nothing is being done to address the security risk; No security processes/policies/procedures are in place; No mitigating controls in place

Risk Score

The Risk Score before/after implementing mitigating controls is automatically calculated by multiplying the Business Impact by the Level of Control. The possible risk score values are given below with corresponding point ranges.

- Critical (45 points)
- High (25-44 points)
- Medium (12-24 points)
- Low (1-11 points)

Risk Score Before Implementing Mitigating Controls

Potential Impact W/O:	High	**Risk Condition W/O:**	Current use is assumed to be limited to specific non-critical functions. Despite this, no documentation exists and security controls are minimal, ad-hoc, or totally absent in some areas. While availability and integrity may not be at much risk, use of Mac devices with these weak controls as an attack vector is a major concern. Business impact will increase as more Macs are onboarded for use at Delta.
Probability W/O :	Low		
Business Impact W/O:	3		
Level of Control W/O:	5		
Range W/O:	15	**Risk Score before implementing mitigating contols:**	● Medium
		Risk Approval Level Needed:	Director

Risk Score After Implementating Mitigating Controls

Potential Impact :	High	**Risk Condition:**	Mitigation may be skipped entirely as current controls are unofficial, undocumented, and minimal. Current efforts are looking to outsource all support, including security, to a vendor. This will essentially be a complete overhaul rather than a mitigation. However, full support may also bring widespread adoption and reliance increasing business impact. Level of control will be assumed at 2 instead of 1 until the vendor relationship and operations mature and all previous instances of Mac use is brought into compliance. Business impact may increase as more Macs are onboarded for use at Delta.
Probability:	Low		
Business Impact :	3		
Level of Control:	2		
Range:	6	**Risk Score after implementing mitigating controls:**	● Low

Review and Approval

CyberSecurity Governance Team Author

Author:	Edwards, Alex	**Date Submitted to Peer Review:**	8/25/2017
Author Status:	Submitted to Manager	**Date Submitted to Manager:**	8/28/2017

CyberSecurity Governance Team Review

Peer Reviewer:	Brooks, Tarika		
Peer Review Status:	Submitted to Author	**Peer Review Date:**	8/28/2017
Peer Review Comments:	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.		
Manager:	Lewis, Robert		
Manager Review Status:	Approved	**Manager Review Date:**	8/28/2017
Manager Comments:	Approved		
Governor:	Brooks, Tarika		
Governor Review Status:	Sent to Approver	**Governor Review Date:**	8/28/2017

Approvers

Please check one of the three choices below.

I understand both the mitigated and unmitigated risk ratings associated with the assessment described in this document.

Vice President Approver:	Blanchard, Daniel	**Vice President Review Date:**	
Managing Director Approver:	Blanchard, Daniel	**Managing Director Review Date**	
Director Approver:	Moss, Wayne	**Director Review Date:**	
General Manager Approver:	Smith, Jimmy	**General Manager Review Date:**	
Approval:			

The mitigation activity is expected to be completed by:

Review Attachments

Name	Size	Type	Upload Date	Downloads
Apple Support SOW_CDW_5.18.2017 Rev 4.doc	98304	.doc	8/25/2017 5:23 PM	0
DRAFT#2_2017_MacOS Devices_RA.doc	263680	.doc	8/25/2017 5:20 PM	0
MacOS_Standard_Imaging_POC_and_On-Site_Support_JF4.docx	126585	.docx	9/27/2017 2:46 PM	0

History Log

Date	User	Field Name	Original Value	New Value
12/10/2017 8:55 PM	Calculation Agent, Archer	Days to Expiration	66	63
12/8/2017 10:50 AM	Calculation Agent, Archer	Days to Expiration	67	66
12/7/2017 10:46 AM	Calculation Agent, Archer	Days to Expiration	68	67
12/5/2017 11:01 PM	Calculation Agent, Archer	Days to Expiration	70	68
12/4/2017 3:17 AM	Calculation Agent, Archer	Days to Expiration	71	70
12/3/2017 12:29 PM	Calculation Agent, Archer	Days to Expiration	72	71
12/2/2017 2:59 PM	Calculation Agent, Archer	Days to Expiration	78	72
11/26/2017 5:26 PM	Calculation Agent, Archer	Days to Expiration	85	78
11/19/2017 12:10 AM	Calculation Agent, Archer	Days to Expiration	88	85
11/16/2017 4:30 PM	Brooks, Tarika	Subject	Aggregate Risk of the Current State of MacOS Device Use at Delta	To allow the aggregate risk of the current state of MacOS Device use at Delta
		Days to Expiration	93	88
11/10/2017 10:42 PM	Calculation Agent, Archer	Days to Expiration	96	93
11/8/2017 3:21 AM	Calculation Agent, Archer	Days to Expiration	97	96
11/7/2017 2:11 PM	Calculation Agent, Archer	Days to Expiration	98	97
11/5/2017 10:53 PM	Calculation Agent, Archer	Days to Expiration	99	98
11/5/2017 5:05 PM	Calculation Agent, Archer	Days to Expiration	102	99
11/2/2017 12:53 PM	Calculation Agent, Archer	Days to Expiration	104	102
10/31/2017 10:46 AM	Calculation Agent, Archer	Days to Expiration	105	104
10/30/2017 4:54 PM	Calculation Agent, Archer	Days to Expiration	106	105
10/29/2017 11:28 AM	Calculation Agent, Archer	Days to Expiration	107	106
10/28/2017 9:36 AM	Calculation Agent, Archer	Days to Expiration	108	107
10/27/2017 8:32 AM	Calculation Agent, Archer	Days to Expiration	109	108
10/26/2017 9:41 AM	Calculation Agent, Archer	Days to Expiration	110	109
10/25/2017 11:07 AM	Calculation Agent, Archer	Days to Expiration	111	110

10/24/2017 10:36 AM	Calculation Agent, Archer	Days to Expiration	112	111
10/23/2017 11:49 AM	Calculation Agent, Archer	Days to Expiration	113	112
10/22/2017 11:08 AM	Calculation Agent, Archer	Days to Expiration	114	113
10/21/2017 10:22 AM	Calculation Agent, Archer	Days to Expiration	115	114
10/20/2017 9:32 AM	Calculation Agent, Archer	Days to Expiration	116	115
10/19/2017 9:57 AM	Calculation Agent, Archer	Days to Expiration	117	116
10/18/2017 9:24 AM	Calculation Agent, Archer	Days to Expiration	118	117
10/17/2017 8:40 AM	Calculation Agent, Archer	Days to Expiration	119	118
10/16/2017 10:16 AM	Calculation Agent, Archer	Days to Expiration	120	119
10/15/2017 9:48 AM	Calculation Agent, Archer	Days to Expiration	121	120
10/14/2017 10:01 AM	Calculation Agent, Archer	Days to Expiration	122	121
10/13/2017 10:04 AM	Calculation Agent, Archer	Days to Expiration	123	122
10/12/2017 1:54 PM	Calculation Agent, Archer	Days to Expiration	124	123
10/11/2017 8:47 AM	Calculation Agent, Archer	Days to Expiration	125	124
10/10/2017 3:29 PM	Calculation Agent, Archer	Days to Expiration	126	125
10/9/2017 10:56 AM	Calculation Agent, Archer	Days to Expiration	127	126
10/8/2017 10:34 AM	Calculation Agent, Archer	Days to Expiration	128	127
10/7/2017 8:25 AM	Calculation Agent, Archer	Days to Expiration	129	128
10/6/2017 9:41 AM	Calculation Agent, Archer	Days to Expiration	130	129
10/5/2017 9:43 AM	Calculation Agent, Archer	Days to Expiration	131	130
10/4/2017 8:53 AM	Calculation Agent, Archer	Days to Expiration	132	131
10/3/2017 12:14 PM	Calculation Agent, Archer	Days to Expiration	133	132
10/2/2017 11:13 AM	Calculation Agent, Archer	Days to Expiration	134	133
10/1/2017 10:16 AM	Calculation Agent, Archer	Days to Expiration	135	134
9/30/2017	Calculation Agent,	Days to Expiration	136	135

8:25 AM	Archer			
9/29/2017 4:20 AM	Calculation Agent, Archer	Days to Expiration	137	136
9/28/2017 8:13 AM	Calculation Agent, Archer	Days to Expiration	138	137
9/27/2017 3:02 PM	Edwards, Alex	Business Background Information	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture. **System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **System Scope:** • Known departments where Macs are used:	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture. **System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **System Scope:** • Known departments where Macs are used:

	◦ Marketing ◦ Delta.com / Ecommerce ◦ Delta.com Development ◦ IT engineering ◦ Social Media ◦ Video Services ◦ ATL Worldport ◦ FlightOps training ◦ TechOps ◦ Cargo ◦ Res training ◦ GA Tech ◦ Innovation ◦ IFS Program Support ◦ (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1,	◦ Marketing ◦ Delta.com / Ecommerce ◦ Delta.com Development ◦ IT engineering ◦ Social Media ◦ Video Services ◦ ATL Worldport ◦ FlightOps training ◦ TechOps ◦ Cargo ◦ Res training ◦ GA Tech ◦ Innovation ◦ IFS Program Support ◦ (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1,

	unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering)	unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering)

	– Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. ○ As of August 2017, direction has shifted to AirWatch and Apple DEP management by Insight. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ ~~CDW Direct, LLC SoW for End-to-End Mac support is being drafted.~~ (See Below) ○ Insight Direct USA, Inc. SoW 21864595 is being drafted for Standard Imaging, POC, and On-Site Support (August 2017, see attachment.) ○ Other companies, such as Stratix/Apple Business,	– Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. ○ As of August 2017, direction has shifted to AirWatch and Apple DEP management by Insight. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ ~~CDW Direct, LLC SoW for End-to-End Mac support is being drafted.~~ (See Below) ○ Insight Direct USA, Inc. SoW is being drafted for Standard Imaging, POC, and On-Site Support (August 2017, see attachment.) ○ Other companies, such as Stratix/Apple Business, are being

	are being considered.	considered.
Recommended Mitigating Controls	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on

	Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to disc	Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to disc

uss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems).

- Security Standard 12.1.1 required analysis must be completed early in this process.

2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.)
    - Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.

uss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems).

- Security Standard 12.1.1 required analysis must be completed early in this process.
- As of August 2017, the Insight SoW mandates Insight collaborate with Delta to provide "as-built" documentation during initital configurations.

2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.)
    - Based on the requirements established from Standard 12.1.1

				analysis, develop and implement controls keeping in mind Standard 12.1.2.
9/27/2017 2:54 PM	Edwards, Alex	Business Background Information	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to "sun rise" official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta's Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture. **System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **System Scope:** • Known departments	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to "sun rise" official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta's Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture. **System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **System Scope:** • Known departments

	where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment.	where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment.

However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam

However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam

Veng (Client & Mobile Engineering) – Management via AirWatch.	Veng (Client & Mobile Engineering) – Management via AirWatch.
• Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.	• Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.
Known Improvement Efforts:	**Known Improvement Efforts:**
• Other MDM solutions are being considered such as Jamf in lieu of AirWatch.	• Other MDM solutions are being considered such as Jamf in lieu of AirWatch. ○ As of August 2017, direction has shifted to AirWatch and Apple DEP management by Insight.
• Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.	• Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.
• Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	• Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ ~~CDW Direct, LLC SoW for End-to-End Mac support is being drafted.~~ (See Below) ○ Insight Direct USA, Inc. SoW 21864595 is being drafted for Standard Imaging, POC, and On-Site Support (August 2017, see attachment.) ○ Other companies, such as

				Stratix/Apple Business, are being considered.
		Peer Review Comments	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.
9/27/2017 2:47 PM	Edwards, Alex	Review Attachments	Apple Support SOW_CDW_5.18.2017 Rev 4.doc|DRAFT#2_2017_MacOS Devices_RA.doc	Apple Support SOW_CDW_5.18.2017 Rev 4.doc|DRAFT#2_2017_MacOS Devices_RA.doc|MacOS_Standard_Imaging_POC_and_On-Site_Support_JF4.docx
9/27/2017 2:22 PM	Calculation Agent, Archer	Days to Expiration	139	138
9/25/2017 9:22 PM	Classen, Tony	Business Background Information	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security

Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of

Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of

June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)

Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images

June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)

Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images

Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
    - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.

Known Improvement Efforts:

- Other MDM solutions are being considered such as Jamf in lieu of AirWatch.
- Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.
- Delta is in negotiations (or plans to negotiate) outsourcing support of Macs.
    - CDW Direct, LLC SoW for End-to-End Mac support is being drafted.

Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
    - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.

Known Improvement Efforts:

- Other MDM solutions are being considered such as Jamf in lieu of AirWatch.
- Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.
- Delta is in negotiations (or plans to negotiate) outsourcing support of Macs.
    - CDW Direct, LLC SoW for End-to-End Mac support is being drafted.

	○ Other companies, such as Stratix/Apple Business, are being considered.	○ Other companies, such as Stratix/Apple Business, are being considered.
Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta’s Information Security Standards. Notes are included where controls are established, but compliance with Delta’s standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch,	(Section symbol (§) refers to a section in Delta’s Information Security Standards. Notes are included where controls are established, but compliance with Delta’s standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch,

	a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to	a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to

	be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product	be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product

	updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Recommended Mitigating Controls	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived

	because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.	because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.
	1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example.	1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example.

	3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks	3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks

	(as is currently done for other systems). ○ Security Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.	(as is currently done for other systems). ○ Security Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.
Remediation Strategy	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear

	business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA)	business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA)

			○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options	○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options
		Days to Expiration	140	139
		Review Stage	Awaiting Director Review	Awaiting Author Submission to Manager
9/25/2017 2:30 PM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591|886654|886656|886662|886685|1879553	464195|886591|886654|886656|886662|886685|1879553|1879554
9/25/2017 2:28 PM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591|886654|886656|886662|886685	464195|886591|886654|886656|886662|886685|1879553
9/25/2017	Calculation Agent,	Days to Expiration	141	140

5:30 AM	Archer			
9/24/2017 9:29 AM	Calculation Agent, Archer	Days to Expiration	142	141
9/23/2017 8:47 AM	Calculation Agent, Archer	Days to Expiration	143	142
9/22/2017 3:14 AM	Calculation Agent, Archer	Days to Expiration	144	143
9/21/2017 2:55 AM	Calculation Agent, Archer	Days to Expiration	145	144
9/20/2017 10:30 AM	Calculation Agent, Archer	Days to Expiration	146	145
9/19/2017 9:28 AM	Calculation Agent, Archer	Days to Expiration	147	146
9/18/2017 2:54 AM	Calculation Agent, Archer	Days to Expiration	148	147
9/17/2017 4:42 AM	Calculation Agent, Archer	Days to Expiration	149	148
9/16/2017 8:11 AM	Calculation Agent, Archer	Days to Expiration	150	149
9/15/2017 4:54 AM	Calculation Agent, Archer	Days to Expiration	151	150
9/14/2017 2:58 AM	Calculation Agent, Archer	Days to Expiration	152	151
9/13/2017 10:15 AM	Calculation Agent, Archer	Days to Expiration	153	152
9/12/2017 12:23 PM	Calculation Agent, Archer	Days to Expiration	154	153
9/11/2017 4:10 AM	Calculation Agent, Archer	Days to Expiration	155	154
9/10/2017 5:22 AM	Calculation Agent, Archer	Days to Expiration	156	155
9/9/2017 6:31 AM	Calculation Agent, Archer	Days to Expiration	157	156
9/8/2017 3:48 AM	Calculation Agent, Archer	Days to Expiration	158	157
9/7/2017 2:44 AM	Calculation Agent, Archer	Days to Expiration	159	158
9/6/2017 3:25 AM	Calculation Agent, Archer	Days to Expiration	160	159
9/5/2017 3:30 AM	Calculation Agent, Archer	Days to Expiration	161	160
9/4/2017 4:47 AM	Calculation Agent, Archer	Days to Expiration	162	161
9/3/2017 4:48 AM	Calculation Agent, Archer	Days to Expiration	163	162
9/2/2017 9:40 AM	Calculation Agent, Archer	Days to Expiration	164	163
9/1/2017 6:56 AM	Calculation Agent, Archer	Days to Expiration	165	164

8/31/2017 3:24 AM	Calculation Agent, Archer	Days to Expiration	166	165
8/30/2017 2:50 AM	Calculation Agent, Archer	Days to Expiration	167	166
8/29/2017 2:40 AM	Calculation Agent, Archer	Days to Expiration	168	167
8/28/2017 3:46 PM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591|886654|886656|886662	464195|886591|886654|886656|886662|886685
8/28/2017 3:46 PM	Advanced Workflow Service, Archer	Review Stage	Awaiting Governor Review	Awaiting Director Review
		Governor Review Date		08/28/2017 00:00:00
		Governor Review Status	Awaiting Governor Review	Sent to Approver
8/28/2017 1:58 PM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591|886654|886656	464195|886591|886654|886656|886662
8/28/2017 1:58 PM	Advanced Workflow Service, Archer	Review Stage	Awaiting Manager Review	Awaiting Governor Review
		Manager Review Date		08/28/2017 00:00:00
		Manager Review Status	Awaiting Review	Approved
		Governor Review Status		Awaiting Governor Review
8/28/2017 1:58 PM	Lewis, Robert	Business Background Information	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Risk Assessment Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of June 2017, AirWatch reports 150 enrolled Mac OSX devi

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of June 2017, AirWatch reports 150 enrolled Mac OSX devi

	ces (excludes iOS)	ces (excludes iOS)
	Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.	**Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.
	Current Mac Onboarding: • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers	**Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers

	via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are

	established, but compliance with Delta's standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection	established, but compliance with Delta's standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection

	○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with	○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with

        “must meet baseline security standards” because none have been formally established.) (§ 11.5.3)

- Software Updates
    - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
        - (NOTE: Updates are not centrally managed. (§ 10.1.3))
    - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
    - Devices are

“must meet baseline security standards” because none have been formally established.) (§ 11.5.3)

- Software Updates
    - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
        - (NOTE: Updates are not centrally managed. (§ 10.1.3))
    - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
    - Devices are

	assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Recommended Mitigating Controls	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and

complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.

1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced.
2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs.
   - Review Windows workstation controls (and process/procedures governing those controls) as an example.
3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs.
   - One component of configuration

complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.

1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced.
2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs.
   - Review Windows workstation controls (and process/procedures governing those controls) as an example.
3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs.
   - One component of configuration

should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security Standard	should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security Standard

		12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.	12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.
	Remediation Strategy	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is

	feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Pasword policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build	feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Pasword policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build

	/ configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options	/ configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options
Manager Comments		Approved
Peer Review Comments	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.

8/28/2017 9:36 AM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591|886654	464195|886591|886654|886656
8/28/2017 9:36 AM	Advanced Workflow Service, Archer	Review Stage	Awaiting Author Submission to Manager	Awaiting Manager Review
		Author Status	Awaiting Submission to Manager	Submitted to Manager
		Manager Review Status		Awaiting Review
		Date Submitted to Manager		08/28/2017 00:00:00
8/28/2017 9:36 AM	Edwards, Alex	Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	Aggregate Risk of the Current State of MacOS Device Use at Delta
		Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:**	**Risk Assessment Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
      - As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)

Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the

involved have requested a risk assessment of the current state of MacOS device use at Delta.

Risk Assessment Scope: This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta's Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

System Purpose and Use: Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers.

System Scope:

- Known departments where Macs are used:
  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Development
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program

purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.

Support
  - (Other Miscellaneous)
- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)

Data Classification:
Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in

- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.

Known Improvement Efforts:

- Other MDM solutions are being considered such as Jamf in lieu of AirWatch.
- Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination.
- Delta is in negotiations (or plans to negotiate) outsourcing support of Macs.
  - CDW Direct, LLC SoW for End-to-End Mac support is being drafted.
  - Other companies, such as Stratix/Apple Business, are being considered.

IShop request by Supply Chain.

  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations.

Known Improvement Efforts:

- Other MDM solutions are being considered such as Jamf in lieu of AirWatch.
- Opening MacOS OSX VPN access to business (non-IT) users requested by

				Project Coordination. - Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
		Regulatory Contstraints Comments	Because present/authorized assets (data in use/data at rest) on Mac devices are not thoroughly identified, applicability is not known. From the list above TechOps and departments that contact PCI are known to use Macs.	Because present/authorized assets (data in use/data at rest) on Mac devices are not thoroughly identified, applicability of regulatory contraints is not known.
		Peer Review Comments	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.
		Regulatory Constraints - Source	Payment Card Industry Data Security Standard v3.1	
8/28/2017 9:08 AM	Advanced Workflow Service, Archer	Open Tasks/Activities	464195|886591	464195|886591|886654
8/28/2017 9:08 AM	Advanced Workflow Service, Archer	Review Stage	Awaiting Peer Review	Awaiting Author Submission to Manager
		Author Status	Submitted to Peer Reviewer	Awaiting Submission to Manager
		Peer Review Date		08/28/2017 00:00:00

		Peer Review Status	Awaiting Review	Submitted to Author
8/28/2017 9:08 AM	Brooks, Tarika	Peer Review Comments	Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does, the data classification would not be internal	Good write-up. Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does violate PCI, the data classification would not be internal and there should be a recommended mitigating control or remediation strategy to achieve compliance. If you are unsure that the use of MacOS violates PCI, I would recommend not including it as a regulatory constraint.
8/28/2017 8:57 AM	Brooks, Tarika	Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.

Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX

devices (excludes iOS)	devices (excludes iOS)
Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.	**Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.
Current Mac Onboarding: • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering	**Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering

		administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
	Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are

	included where controls are established, but compliance with Delta’s standards are partial or unknown.)	included where controls are established, but compliance with Delta’s standards are partial or unknown.)
	• AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint	• AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint

	Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant	Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant

	with “must meet baseline security standards” because none have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other	with “must meet baseline security standards” because none have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other

	○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Recommended Mitigating Controls	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during	Because of Mac usage’s wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during

	development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of	development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of

	configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security	configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security

	Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.	Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.
Remediation Strategy	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if

	that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image	that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration ○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image

			○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options	○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options
		Peer Review Comments		Suggested edits - move the Purpose and Scope statements from the Subject section to the Business Background section. You only need a very short description for the subject, i.e. to allow the purchase and use of MacOS devices in the Delta environment. Also, it's not clear to me if you are saying that the use of MacOS violates PCI. If it does, the data classification would not be internal
8/28/2017 2:53 AM	Calculation Agent, Archer	Days to Expiration	169	168
8/27/2017 2:48 AM	Calculation Agent, Archer	Days to Expiration	170	169
8/26/2017 2:50 AM	Calculation Agent, Archer	Days to Expiration	171	170
8/25/2017	Advanced Workflow	Open Tasks/Activities	464195	464195|886591

5:41 PM	Service, Archer			
8/25/2017 5:41 PM	Advanced Workflow Service, Archer	Review Stage	Awaiting Author Completion	Awaiting Peer Review
		Author Status	Awaiting Submission to Peer Review	Submitted to Peer Reviewer
		Date Submitted to Peer Review		08/25/2017 00:00:00
		Peer Review Status		Awaiting Review
8/25/2017 5:41 PM	Edwards, Alex	Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.
		Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are

	used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information	used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information

	Security Standard 7.3.1, unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client &	Security Standard 7.3.1, unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Management). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client &

	Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are established, but compliance with Delta's standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are established, but compliance with Delta's standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15

	Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirme	Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows scan times. ▪ (NOTE: Routine updates are not confirme

	d, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none	d, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none

	have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering.	have been formally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering.

	(§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	(§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Recommended Mitigating Controls	Because of Mac usage's wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.	Because of Mac usage's wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established.

	1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.	1. Before starting, establish clear ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced. 2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs. ○ Review Windows workstation controls (and process/procedures governing those controls) as an example. 3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs. ○ One component of configuration should be OS hardening. ▪ Established capability to remotely configure Mac OSX (e.g.

	: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on	: MDM policy deployment similar to Active Directory GPOs), ▪ Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems). ○ Security Standard 12.1.1 required analysis must be completed early in this process. 2. Deploy these controls on existing and future Macs (or monitor any vendor’s continuing operations to ensure all Macs are compliant.) ○ Based on

	the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.	the requirements established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.
Remediation Strategy	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration	• Ensure total compliance with Information Security Policy and Standards starting with the steps in the above section. ○ Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible. • Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed): ○ Active Directory Integration

	○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap	○ MacOS Client Directory integration ▪ Kerberos ▪ SSO ▪ Password policies ▪ Local accounts vs mobile ▪ Admin accounts vs standard ○ Print queues ○ SharePoint / DFS ○ Wireless (e.g., 802.1x, Certs, WPA) ○ VPN ○ Cisco ISE ○ Cisco FastLane ○ Proxy servers ○ Airwatch enrollment ○ Build a new standard configuration / new image ○ Current build / configuration process ○ Onboarding / off-boarding process ○ Reporting ○ Airwatch access ○ Recommended settings for MacOS ○ Windows vs MacOS security gap

			analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options	analysis ○ Role of Airwatch in security ○ Profile build outs and discussions ○ Password policies ○ Encryption ○ Antivirus options ○ Lost Mode, Remote Wipe, Activation Lock ○ Best practices ○ Endpoint backup options
8/25/2017 5:32 PM	Edwards, Alex	Control Standards Impacted		Access Control to Program Source Code|Administrator and Operator Logs|Asset Inventory|Authorized Access|Automated Audit Tools|Classification Guidelines|Controls against Malicious Code|Cryptographic Controls|Designated Owner|Documented Operating Procedures|Evaluating Network Security|Fault Logging|Hardening Network Devices|IT Business Continuity Operational Plans|IT Business Impact Analysis|Identification of Applicable Legislation|Information Handling Procedures|Log Retention|Monitoring System Use|Password Management Program|Privileged User Access|Remote Access Process|Security Requirements|Session Time-out|System Documentation|System Patches|User Access Review
8/25/2017 5:27 PM	Edwards, Alex	Regulatory Contstraints Comments		Because present/authorized assets (data in use/data at rest) on Mac devices are not thoroughly identified, applicability is not known. From the list above TechOps and departments that contact PCI are known to use Macs.
		Regulatory Constraints - Source		Payment Card Industry Data Security Standard v3.1
8/25/2017 5:25 PM	Edwards, Alex	Remediation Strategy		• Ensure total compliance with

Information Security Policy and Standards starting with the steps in the above section.

  - Acquire individual, formal exceptions as required during development of Mac support only after a clear business need is established. Recurring exceptions should not be requested in place of efforts to developing controls if that effort is feasible.

- Address, establish, and execute standard operating procedure for maintenance of areas including, but not limited to (taken from the CDW Direct, LLC SoW draft as an example of areas that may be addressed):
  - Active Directory Integration
  - MacOS Client Directory integration
    - Kerberos
    - SSO
    - Password policies
    - Local accounts vs mobi

le

    - Admin accounts vs standard

- Print queues
- SharePoint / DFS
- Wireless (e.g., 802.1x, Certs, WPA)
- VPN
- Cisco ISE
- Cisco FastLane
- Proxy servers
- Airwatch enrollment
- Build a new standard configuration / new image
- Current build / configuration process
- Onboarding / off-boarding process
- Reporting
- Airwatch access
- Recommended settings for MacOS
- Windows vs MacOS security gap analysis
- Role of Airwatch in security
- Profile build outs and discussions
- Password policies
- Encryption
- Antivirus options
- Lost Mode, Remote Wipe, Activation Lock
- Best

				practices o Endpoint backup options
8/25/2017 5:25 PM	Edwards, Alex	Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.
		Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce

	o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.	o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS) **Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
  - Quote acquired from Best Buy for Business by Supply Chain.
  - Quote submitted in IShop request by Supply Chain.
  - Macs shipped to Delta.
  - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
  - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch.
- Simone Thomas

	(Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	(Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta’s Information Security Standards. Notes are included where controls are established, but compliance with Delta’s standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3)	(Section symbol (§) refers to a section in Delta’s Information Security Standards. Notes are included where controls are established, but compliance with Delta’s standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3)

        - (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2))
    - In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1)
- Symantec Endpoint Protection
    - Installed and configured to match Windows scan times.
        - (NOTE: Routine updates are not confirmed, compliance

        - (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2))
    - In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1)
- Symantec Endpoint Protection
    - Installed and configured to match Windows scan times.
        - (NOTE: Routine updates are not confirmed, compliance

	with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none have been form	with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet baseline security standards” because none have been form

	ally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault	ally established.) (§ 11.5.3) • Software Updates ○ Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3) ▪ (NOTE: Updates are not centrally managed. (§ 10.1.3)) ○ Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product). • Other ○ Devices are assigned a name (X/WATLMAC0000x) ○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault

	Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Recommended Mitigating Controls	Because of Mac usage's wide scope as an asset, CSG recommends the following high level steps to reduce risk exposure during development and maturity of Mac support. Unofficial Mac use is not a typical scenario where a Standard is waived because of a business need. Rather, non-compliance is due to a lack of current controls after devices came into use before the required security oversight was established. There is no need for different mitigating controls in place of compliance (except for those arising from individual exceptions during development). Mitigation and complete remediation would follow the same path. Risk would be increasingly mitigated as official support is developed and matured. Upon completion, these steps should mitigate the aggregated risk of having no official support (and no official security). These actions may be taken before or during any vendor support takeover and passed to vendor support after the relationship is established. 1. Before starting, establish clear	

ownership within Delta for Mac support including procurement, configuration, maintenance, and support. Maintain Delta ownership in a supervisory role if these functions are outsourced.

2. Evaluate Delta’s Information Security Policy and Standards to identify all applications where controls must be implemented on Macs.
    - Review Windows workstation controls (and process/procedures governing those controls) as an example.
3. Create a formal methodology with documentation for procurement, configuration, maintenance, and management of security controls on Macs.
    - One component of configuration should be OS hardening.
        - Established capability to remotely configure Mac OSX (e.g.: MDM

policy deployment similar to Active Directory GPOs),

            - Contact CSG to discuss adaptation of the Mac OSX CIS Benchmarks (as is currently done for other systems).

        - Security Standard 12.1.1 required analysis must be completed early in this process.

2. Deploy these controls on existing and future Macs (or monitor any vendor's continuing operations to ensure all Macs are compliant.)

    - Based on the requirements

				established from Standard 12.1.1 analysis, develop and implement controls keeping in mind Standard 12.1.2.
		Review Attachments		Apple Support SOW_CDW_5.18.2017 Rev 4.doc|DRAFT#2_2017_MacOS Devices_RA.doc
		Requestor	Edwards, Alex	Lewis, Robert
8/25/2017 5:19 PM	Edwards, Alex	Expiration Date		02/12/2018 00:00:00
		Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.
		Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise

	Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)	Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments where Macs are used: o Marketing o Delta.com / Ecommerce o Delta.com Development o IT engineering o Social Media o Video Services o ATL Worldport o FlightOps training o TechOps o Cargo o Res training o GA Tech o Innovation o IFS Program Support o (Other Miscellaneous) • All or most are assumed to be under AirWatch (Mobile Device Management) control. ▪ As of June 2017, AirWatch reports 150 enrolled Mac OSX devices (excludes iOS)

	Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Managemen	**Data Classification:** Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment. However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default. **Current Mac Onboarding:** • Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG. • Known elements of de facto process: ○ Quote acquired from Best Buy for Business by Supply Chain. ○ Quote submitted in IShop request by Supply Chain. ○ Macs shipped to Delta. ○ Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.) ○ Client Engineering administers via AirWatch (Mobile Device Managemen

	t). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.	t). **Current De Facto Owners:** • Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support. • Ken Gleason/Sam Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are established, but compliance with Delta's standards are partial or unknown.)	(Section symbol (§) refers to a section in Delta's Information Security Standards. Notes are included where controls are established, but compliance with Delta's standards are partial or unknown.)

	• AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows	• AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session timeout: 15 Min. (§ 11.4.3) ▪ (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2)) ○ In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1) • Symantec Endpoint Protection ○ Installed and configured to match Windows

	scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet	scan times. ▪ (NOTE: Routine updates are not confirmed, compliance with § 10.4.6 unknown.) ○ (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3)) • Pulse Client (VPN Access) ○ Access requested via Ishop. ○ Certificate deployed by AirWatch. (§ 11.5.3) ○ Requires SEP and AirWatch to be installed before allowing connections. ▪ (NOTE: May not be compliant with “must meet

baseline security standards” because none have been formally established.) (§ 11.5.3)

- Software Updates
  - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
    - (NOTE: Updates are not centrally managed. (§ 10.1.3))
  - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
  - Devices are assigned a name (X/WATLMAC0000x)

baseline security standards” because none have been formally established.) (§ 11.5.3)

- Software Updates
  - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
    - (NOTE: Updates are not centrally managed. (§ 10.1.3))
  - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
  - Devices are assigned a name (X/WATLMAC0000x)

	○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))	○ Device is associated with a user ID and device information is stored in a SQL database by Client Engineering. (§ 7.1.1) ○ All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1) ▪ (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))
Risk Condition W/O		Current use is assumed to be limited to specific non-critical functions. Despite this, no documentation exists and security controls are minimal, ad-hoc, or totally absent in some areas. While availability and integrity may not be at much risk, use of Mac devices with these weak controls as an attack vector is a major concern. Business impact will increase as more Macs are onboarded for use at Delta.
Business Impact W/O	0	3
Risk Condition		Mitigation may be skipped entirely as current controls are unofficial, undocumented, and minimal. Current efforts are looking to outsource all support, including security, to a vendor. This will essentially

				be a complete overhaul rather than a mitigation. However, full support may also bring widespread adoption and reliance increasing business impact. Level of control will be assumed at 2 instead of 1 until the vendor relationship and operations mature and all previous instances of Mac use is brought into compliance. Business impact may increase as more Macs are onboarded for use at Delta.
		Days to Expiration		171
		Potential Impact		High (3.000000)
		Probability		Low (1.000000)
		Business Impact	0	3
		Are there recommended mitigating controls?		Yes
		Risk Score after implementing mitigating controls		Low
		Range	0	6
		Level of Control		2
		Potential Impact W/O		High (3.000000)
		Probability W/O		Low (1.000000)
		Range W/O	0	15
		Risk Score before implementing mitigating contols		Medium
		Level of Control W/O		5
		Exception Duration		180 Days
		Risk Approval Level Needed		Director
		Manager		Lewis, Robert
		Vice President Approver		Blanchard, Daniel
		Managing Director Approver		Blanchard, Daniel
		Director Approver		Moss, Wayne
		General Manager Approver		Smith, Jimmy
		Peer Reviewer		Brooks, Tarika
		Governor		Brooks, Tarika
8/16/2017 1:44 PM	Advanced Workflow Service, Archer	Open Tasks/Activities		464195
8/16/2017 1:44 PM	Advanced Workflow Service, Archer	Review Stage	Awaiting Requestor Submission	Awaiting Author Completion
		Requestor Submission Status	Awaiting Submission	Submitted
		Date of Request		08/16/2017 00:00:00

		Author Status	Awaiting Submission to Peer Review
8/16/2017 1:42 PM	Edwards, Alex	Risk Assessment Name	2017_464194_RA_Information Technology_MacOS Use
		Overall Status	In Process
		Assessment Type	RA
		Issue	MacOS Use
		Subject	**Purpose:** Currently, Delta allows the purchase of MacOS devices and use on their network. However, Delta does not officially support these devices or their security controls. MacOS instances at Delta were provisioned on an ad hoc basis using the de facto baseline controls mentioned below. Delta is seeking to “sun rise” official support of MacOS and those involved have requested a risk assessment of the current state of MacOS device use at Delta. **Scope:** This assessment will consider the current state of MacOS use at Delta, their security controls, and gaps pertaining to compliance with Delta’s Information Security Policies and Standards. This does not include other Apple devices that may use iOS. Because of the broad scope, individual threat events will not be addressed directly. Instead, individual standards will be addressed to identify points where improvements must be made to mature future MacOS security posture.
		Business Background Information	**System Purpose and Use:** Mac devices are not supported officially, however purchase is allowed for Delta use. According to Enterprise Apps, until recently, Macs were only permitted for purchase for Adobe Cloud Design and Video work, but has now been opened to others such as Developers. **Scope:** • Known departments

where Macs are used:

  - Marketing
  - Delta.com / Ecommerce
  - Delta.com Developmen t
  - IT engineering
  - Social Media
  - Video Services
  - ATL Worldport
  - FlightOps training
  - TechOps
  - Cargo
  - Res training
  - GA Tech
  - Innovation
  - IFS Program Support
  - (Other Miscellaneo us)

- All or most are assumed to be under AirWatch (Mobile Device Management) control.
    - As of June 201 7, AirW atch repo rts 150 enro lled Mac OSX devi ces (excl udes iOS)

Data Classification: Because it appears that Macs are used primarily for media and interactive purposes, **Internal Use** is the highest assumed classification of data on these devices for the purpose of this assessment.

However, per Information Security Standard 7.3.1, unclassified data must be considered **Confidential** by default.

Current Mac Onboarding:

- Mac provisioning is ad-hoc. No formal procedure documentation was found by CSG.
- Known elements of de facto process:
    - Quote acquired from Best Buy for Business by Supply Chain.
    - Quote submitted in IShop request by Supply Chain.
    - Macs shipped to Delta.
    - Enterprise Apps team configures and/or images Macs. (This may include install of OS, MS Office, Airwatch, Pulse, Certificates, Lync, Adobe Creative Cloud.)
    - Client Engineering administers via AirWatch (Mobile Device Management).

Current De Facto Owners:

- Karen Hagerman/Trey Engle (Enterprise Apps) – Build, configuration, and support.
- Ken Gleason/Sam

		Veng (Client & Mobile Engineering) – Management via AirWatch. • Simone Thomas (Project Coordination) & Emily Forbes (Supply Chain) – Acquisition and Outsourcing negotiations. **Known Improvement Efforts:** • Other MDM solutions are being considered such as Jamf in lieu of AirWatch. • Opening MacOS OSX VPN access to business (non-IT) users requested by Project Coordination. • Delta is in negotiations (or plans to negotiate) outsourcing support of Macs. ○ CDW Direct, LLC SoW for End-to-End Mac support is being drafted. ○ Other companies, such as Stratix/Apple Business, are being considered.
	Existing Mitigating Controls	(Section symbol (§) refers to a section in Delta’s Information Security Standards. Notes are included where controls are established, but compliance with Delta’s standards are partial or unknown.) • AirWatch (Mobile Device Management) ○ Enforces pin code policy: ▪ Session time out:

15 Min. (§ 11.4.3)

        - (NOTE: Does not satisfy password strength requirements (§ 11.4.2), but does satisfy Mobile Device Usage. (§ 11.2.2))
    - In AirWatch, a Mac is associated with a user ID. AirWatch has information about the device such as serial number. (§ 7.1.1)
- Symantec Endpoint Protection
    - Installed and configured to match Windows scan times.
        - (NOTE: Routine updates are not confi

rmed, compliance with § 10.4.6 unknown.)

    - (NOTE: Individual, host-based scans only, Macs are not covered by network vulnerability scanning. (§ 10.4.5, § 15.1.3))
- Pulse Client (VPN Access)
    - Access requested via Ishop.
    - Certificate deployed by AirWatch. (§ 11.5.3)
    - Requires SEP and AirWatch to be installed before allowing connections.
        - (NOTE: May not be compliant with “must meet baseline security standards” because non

e have been formally established.) (§ 11.5.3)

- Software Updates
  - Automatic updates for Mac OSX and MS Office are automatic. (§ 10.1.3)
    - (NOTE: Updates are not centrally managed. (§ 10.1.3))
  - Adobe product updates are managed by the Adobe Remote Update Server (consistant across all platforms using this product).
- Other
  - Devices are assigned a name (X/WATLMAC0000x)
  - Device is associated with a user ID and device information is stored in a SQL database by Client

Engineering. (§ 7.1.1)

- All Mac Laptops use FileVault Disk Encryption. (§ 10.7.1)
  - (NOTE: Mac Desktops are not set up with Disk Encryption. (§ 10.7.1))

Data Classification	Confidential
Business Impact W/O	0
Review Stage	Awaiting Requestor Submission
Business Impact	0
Range	0
Range W/O	0
Requestor Submission Status	Awaiting Submission
Is this a renewal or update?	No
Manual Approval Override	No
Review Stage Manual Override	Awaiting Manual Approval
Requestor	Edwards, Alex
Division	Information Technology
Author	Edwards, Alex
Automatic Record Permission	CyberSecurity Governance Team