Esri Managed Cloud Services – Advanced Plus
Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) 3.0.1
March 2021

Attached are Esri's self-assessment answers to the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) for Esri Managed Cloud Services (EMCS) Advanced Plus offering. The questionnaire published by the CSA, provides a way to reference and document what security controls exist in Esri's EMCS Advanced Plus offering. The questionnaire provides a set of 133 questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.

The CSA is a "not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing" (https://cloudsecurityalliance.org/about/). A wide range of industry security practitioners, corporations, and associations participate in this organization to achieve its mission. Esri has been providing answers for the CSA CCM since 2013 and will update this document focused on EMCS Advanced Plus for newer CCM revisions in the future.

Significant changes to version 3.x CCM from the previous version 1.x CCM include:

- Five new control domains that address information security risks over the access of, transfer to, and securing of cloud data: Mobile Security; Supply Chain Management, Transparency & Accountability; Interoperability & Portability; and Encryption & Key Management
- Improved harmonization with the Security Guidance for Critical Areas of Cloud Computing v3
- Improved control auditability throughout the control domains and an expanded control identification naming convention
- Incremental updates/corrections of version 3.0.1 questions are made available by the CSA. We've incorporated updates for version 3.0.1 10/6/2016 within this document.

EMCS Advanced Plus has achieved Federal Risk and Authorization Management Program (FedRAMP) compliance at the "Moderate" level. This offering provides the ArcGIS platform securely in the cloud and is offered under Managed Cloud Services within Esri. EMCS Advanced Plus can be used as a standalone solution, or to augment existing implementations of ArcGIS Online and/or On-Premises deployments using a hybrid approach. The EMCS Advanced Plus and AWS cloud infrastructure federal authorizations can be validated on the FedRAMP Marketplace.

EMCS Advanced Plus utilizes Amazon Web Services (AWS) East/West US Regions to provide Infrastructure-as-a-Service (IaaS) for the solution.
AWS is also FedRAMP Moderate compliant and listed on the CSA registry. Additional information about EMCS Advanced Plus, ArcGIS product security and privacy, as well as links to CSM CCM answers for ArcGIS Online are available on the ArcGIS Trust site at trust.arcgis.com.

The latest version of the EMCS Advanced Plus CSA CCM answers, with a glossary of acronyms at the end, is available at:
http://downloads.esri.com/resources/enterprisegis/EMCS_CSA_CCM.pdf

NOTE: These answers are for assurance only for the EMCS Advanced Plus offering, not ArcGIS Online, which has a separate set of CSA CCM answers available in the CSA STAR registry. Also, the security controls specified within this document are NOT applicable to other EMCS offerings (Standard and Advanced).

For any questions/concerns/feedback, please contact the EMCS Security team at:

AES_Security@esri.com

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	As part of the FedRAMP process, EMCS Advanced Plus was designed and developed to be a hardened environment that limits exposed services and minimizes potential attack surface. Automated scanners and manual testing are performed against application and programming interfaces to align with industry standards such as OWASP. This is a mandatory requirement as part of FedRAMP Continuous Monitoring and ensures potential threats are identified, tracked and mitigated to provide constant security assurance.	NIST SP 800-53 R4 SA-8 NIST SP 800-53 R4 SC-2 NIST SP 800-53 R4 SC-4 NIST SP 800-53 R4 SC-5 NIST SP 800-53 R4 SC-6 NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (3) NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-7 (5) NIST SP 800-53 R4 SC-7 (7) NIST SP 800-53 R4 SC-7 (8) NIST SP 800-53 R4 SC-7 (12) NIST SP 800-53 R4 SC-7 (13) NIST SP 800-53 R4 SC-7 (18)	45 CFR 164.312(e)(2)(i)	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Customers will review and agree to terms of use prior to being granted access to EMCS Advanced Plus applications and infrastructure. Customers are responsible for managing access to their data hosted in the EMCS Advanced Plus environment.	NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CA-5 NIST SP 800-53 R4 CA-6		A9.1.1.
Application & Interface Security Data Integrity	AIS-03	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	EMCS Advanced Plus uses relational databases to manage the integrity of feature data sets uploaded by customers. Industry standard encryption is used to maintain data integrity through all phases of transmission, storage and processing. The cloud infrastructure providers also align with FedRAMP Moderate baseline to ensure integrity is maintained at all levels for EMCS Advanced Plus.	NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-5 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 SI-2 NIST SP 800-53 R4 SI-2 (2) NIST SP 800-53 R4 SI-3 NIST SP 800-53 R4 SI-3 (1) NIST SP 800-53 R4 SI-3 (2) NIST SP 800-53 R4 SI-4 NIST SP 800-53 R4 SI-4 (2) NIST SP 800-53 R4 SI-4 (4) NIST SP 800-53 R4 SI-4 (5) NIST SP 800-53 R4 SI-6 NIST SP 800-53 R4 SI-7 NIST SP 800-53 R4 SI-7 (1) NIST SP 800-53 R4 SI-7 (7) NIST SP 800-53 R4 SI-10 NIST SP 800-53 R4 SI-11	45 CFR 164.312 (c)(1) 45 CFR 164.312 (c)(2) 45 CFR 164.312(e)(2)(i)	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4
Application & Interface Security Data Security / Integrity	AIS-04	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alteration, or destruction.	Interconnection Security Agreements (ISA) are established between service providers and Esri to maintain data confidentiality, integrity and availability. Access to the EMCS environment is strictly controlled, delineated and limited to approved users and administrators.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-4 NIST SP 800-53 R4 SC-1 NIST SP 800-53 R4 SC-8 NIST SP 800-53 R4 SC-8 (1)		A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4
Audit Assurance & Compliance Audit Planning	AAC-01	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	As a part FedRAMP authorization, EMCS Advanced Plus is subjected to a Continuous Monitoring Plan and regular review of security controls to ensure effectiveness. This ensures the appropriate technical and organizational measures are in place to provide customers with the assurance that their data is protected. A yearly third-party audit by approved FedRAMP auditors is done yearly to ensure transparency.	NIST SP 800-53 R4 CA-2 NIST SP 800-53 R4 CA-2 (1) NIST SP 800-53 R4 CA-7	45 CFR 164.312(b)	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1
Audit Assurance & Compliance Independent Audits	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	An independent review of security controls, vulnerability assessment and penetration testing occur annually by an accredited third party auditor as mandated by FedRAMP. The scope of the control review spans both organizational measures (policy, procedures) and technical review.	NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CA-2 NIST SP 800-53 R4 CA-2 (1) NIST SP 800-53 R4 CA-6 NIST SP 800-53 R4 CA-8 NIST SP 800-53 R4 RA-5 NIST SP 800-53 R4 RA-5 (1) NIST SP 800-53 R4 RA-5 (2) NIST SP 800-53 R4 RA-5 (3) NIST SP 800-53 R4 RA-5 (6)	45 CFR 164.308 (a)(8) 45 CFR 164.308(a)(1)(ii)(D)	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Audit Assurance & Compliance Information System Regulatory Mapping	AAC-03	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	A System Security Plan (SSP) for EMCS Advanced Plus is maintained and reviewed at a minimum annually or when a significant change to the system occurs.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CP-1 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-7 NIST SP 800-53 R4 IR-1 NIST SP 800-53 R4 MA-1 NIST SP 800-53 R4 MP-1 NIST SP 800-53 R4 PE-1 NIST SP 800-53 R4 PL-1 NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 RA-1 NIST SP 800-53 R4 RA-2 NIST SP 800-53 R4 SA-1 NIST SP 800-53 R4 SC-1 NIST SP 800-53 R4 SC-13 NIST SP 800-53 R4 SI-1 NIST SP 800-53 R4 SI-7		Clauses 4.2(b), 4.4, 5.2(c), 5.3(ab), 6.1.2, 6.1.3, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3 9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1, A.18.1.1, A.18.1.3, A.18.1.4, A.18.1.5
Business Continuity Management & Operational Resilience Business Continuity Planning	BCR-01	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Esri maintains a detailed plan outlining continuity plans for EMCS that involves the following: roles and responsibilities of key personnel, notification and escalation procedures, recovery plans, recovery time objective (RTO) and recovery point objective (RPO) and a clearly defined communication process.	NIST SP800-53 R4 CP-1 NIST SP800-53 R4 CP-2 NIST SP800-53 R4 CP-2 (1) NIST SP800-53 R4 CP-2 (2) NIST SP800-53 R4 CP-3 NIST SP800-53 R4 CP-4 NIST SP800-53 R4 CP-4 (1) NIST SP800-53 R4 CP-6 NIST SP800-53 R4 CP-6 (1) NIST SP800-53 R4 CP-6 (3) NIST SP800-53 R4 CP-7 NIST SP800-53 R4 CP-7 (1) NIST SP800-53 R4 CP-7 (2) NIST SP800-53 R4 CP-7 (3) NIST SP800-53 R4 CP-8 NIST SP800-53 R4 CP-8 (1) NIST SP800-53 R4 CP-8 (2) NIST SP800-53 R4 CP-9 NIST SP800-53 R4 CP-9 (1)	45 CFR 164.308 (a)(7)(i) 45 CFR 164.308 (a)(7)(ii)(B) 45 CFR 164.308 (a)(7)(ii)(C) 45 CFR 164.308 (a)(7)(ii)(E) 45 CFR 164.310 (a)(2)(i) 45 CFR 164.312 (a)(2)(ii)	Clause 5.1(h) A.17.1.2 A.17.1.2
Business Continuity Management & Operational Resilience Business Continuity Testing	BCR-02	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra- supply chain business process dependencies.	As per FedRAMP requirements, Incident Response training is done annually to information system users where it is consistent with assigned roles and responsibilities. Likewise, Incident Response plans and Business Continuity are tested annually. Testing uses Incident Handling scenarios from Appendix A of NIST SP 800-61.	NIST SP800-53 R4 CP-2 NIST SP800-53 R4 CP-2 (1) NIST SP800-53 R4 CP-2 (2) NIST SP800-53 R4 CP-3 NIST SP800-53 R4 CP-4 NIST SP800-53 R4 CP-4 (1) NIST SP800-53 R4 IR-9 (2) NIST SP800-53 R4 IR-9 (3)	45 CFR 164.308 (a)(7)(ii)(D)	A17.3.1
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP800-53 R4 IR-9 (4) NIST SP800-53 R4 PE-1 NIST SP800-53 R4 PE-4 NIST SP800-53 R4 PE-13 NIST SP800-53 R4 PE-13 (2) NIST SP800-53 R4 PE-13 (3) NIST SP800-53 R4 PE-14 (2)		A11.2.2, A11.2.3
Business Continuity Management & Operational Resilience Documentation	BCR-04	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Information system documentation and architecture diagrams are fully detailed in the System Security Plan (SSP) for FedRAMP. The information system is already configured in a way where the security requirements align with FedRAMP Moderate requirements. Users can also refer to general product security best practices by referring to the trust.arcgis.com website.	NIST SP 800-53 R4 AC-6 (5) NIST SP 800-53 R4 CP-9 NIST SP 800-53 R4 CP-9 (1) NIST SP 800-53 R4 CP-9 (3) NIST SP 800-53 R4 CP-10 NIST SP 800-53 R4 CP-10 (2) NIST SP 800-53 R4 SA-4 (1) NIST SP 800-53 R4 SA-4 (2)		Clause 9.2(g) A12.1.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Business Continuity Management & Operational Resilience Environmental Risks	BCR-05	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP800-53 R4 PE-1 NIST SP800-53 R4 PE-13 NIST SP800-53 R4 PE-13 (2) NIST SP800-53 R4 PE-13 (3) NIST SP800-53 R4 PE-14 NIST SP800-53 R4 PE-15	45 CFR 164.308 (a)(7)(i) 45 CFR 164.310(a)(2)(ii)	A11.1.4, A11.2.1 A11.2.2
Business Continuity Management & Operational Resilience Equipment Location	BCR-06	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP800-53 R4 IR-9 (4) NIST SP800-53 R4 PE-1 NIST SP800-53 R4 PE-5 NIST SP800-53 R4 PE-14 NIST SP800-53 R4 PE-15	45 CFR 164.310 (c)	A11.2.1
Business Continuity Management & Operational Resilience Equipment Maintenance	BCR-07	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	The Esri System Maintenance Policy is adopted by EMCS and details policies and procedures all staff take with regards to maintenance. Technical measures are in place to ensure continuity of operations during maintenance. Many maintenance controls are inherited by IaaS provider AWS.	NIST SP 800-53 R4 IR-3 (2) NIST SP 800-53 R4 MA-2 NIST SP 800-53 R4 MA-3 NIST SP 800-53 R4 MA-3 (1) NIST SP 800-53 R4 MA-3 (2) NIST SP 800-53 R4 MA-3 (3) NIST SP 800-53 R4 MA-4 NIST SP 800-53 R4 MA-4 (2) NIST SP 800-53 R4 MA-5 NIST SP 800-53 R4 MA-6	45 CFR 164.310 (a)(2)(iv)	A11.2.4
Business Continuity Management & Operational Resilience Equipment Power Failures	BCR-08	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically- specific business impact assessment.	EMCS Advanced Plus is a redundant configuration across two (2) separate AWS availability zones (data centers). Customer data backups are stored in a separate US Region, should the primary region become unreachable. There may be some ArcGIS Enterprise Extensions that deviate from the standard redundant configuration. In these cases, customers are required to approve this exception.	NIST SP800-53 R4 CP-8 NIST SP800-53 R4 CP-8 (1) NIST SP800-53 R4 CP-8 (2) NIST SP800-53 R4 IR-3 (2) NIST SP800-53 R4 PE-1 NIST SP800-53 R4 PE-9 NIST SP800-53 R4 PE-10 NIST SP800-53 R4 PE-11 NIST SP800-53 R4 PE-12 NIST SP800-53 R4 PE-13 NIST SP800-53 R4 PE-13 (2) NIST SP800-53 R4 PE-13 (3) NIST SP800-53 R4 PE-14		A.11.2.2, A.11.2.3, A.11.2.4
Business Continuity Management & Operational Resilience Impact Analysis	BCR-09	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	The EMCS Contingency Plan contains a detailed process for assessing the impact of a service disruption. The includes the identification of critical services, impacts of disruption, recovery procedures and established Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for the system.	NIST SP 800-53 R4 CP-1 NIST SP 800-53 R4 CP-2 NIST SP 800-53 R4 CP-2 (3) NIST SP 800-53 R4 CP-2 (8) NIST SP 800-53 R4 RA-3	45 CFR 164.308 (a)(7)(ii)(E)	A.17.1.1 A.17.1.2
Business Continuity Management & Operational Resilience Policy	BCR-10	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery, and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	EMCS Advanced Plus has a detailed Roles and Responsibilities Matrix as part of the System Security Plan (SSP) and security training materials have been developed for all aspects of the system. Esri employees accessing EMCS Advanced Plus must sign a Rules of Behavior (RoB) that outlines employee technical and organizational responsibilities related to access and use.	NIST SP 800-53 R4 CM-2 NIST SP 800-53 R4 CM-2 (1) NIST SP 800-53 R4 CM-2 (3) NIST SP 800-53 R4 CM-2 (7) NIST SP 800-53 R4 CM-3 NIST SP 800-53 R4 CM-4 NIST SP 800-53 R4 CM-5 NIST SP 800-53 R4 CM-6 NIST SP 800-53 R4 CM-6 (1) NIST SP 800-53 R4 CM-9 NIST SP 800-53 R4 IR-9 (2) NIST SP 800-53 R4 MA-4		Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	To align with FedRAMP Moderate requirements, data is retained for a minimum of three (3) months or as required by a specific customer. Backup and Recovery measures are tested at a minimum of annually to ensure effectiveness.	NIST SP 800-53 R4 CP-2 NIST SP 800-53 R4 CP-2 (1) NIST SP 800-53 R4 CP-2 (2) NIST SP 800-53 R4 CP-6 NIST SP 800-53 R4 CP-6 (1) NIST SP 800-53 R4 CP-6 (3) NIST SP 800-53 R4 CP-7 NIST SP 800-53 R4 CP-7 (1) NIST SP 800-53 R4 CP-7 (2) NIST SP 800-53 R4 CP-7 (3) NIST SP 800-53 R4 CP-8 NIST SP 800-53 R4 CP-8 (1) NIST SP 800-53 R4 CP-8 (2) NIST SP 800-53 R4 CP-9 NIST SP 800-53 R4 CP-9 (1)	45 CFR 164.308 (a)(7)(ii)(A) 45 CFR 164.310 (d)(2)(iv) 45 CFR 164.308(a)(7)(ii)(D) 45 CFR 164.316(b)(2)(i) (New)	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1 A.8.2.3
Change Control & Configuration Management New Development / Acquisition	CCC-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network, and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	EMCS Advanced Plus Configuration Change Control procedures adhere to the Esri Corporate Change Management policy. This document details the types of changes to the information system that are configuration controlled. Any changes to the system are subjected to a documented workflow to ensure they are tracked and authorized prior to being implemented.	NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CM-9 NIST SP 800-53 R4 PL-1 NIST SP 800-53 R4 PL-2 NIST SP 800-53 R4 SA-1 NIST SP 800-53 R4 SA-3 NIST SP 800-53 R4 SA-4 NIST SP 800-53 R4 SA-4 (1) NIST SP 800-53 R4 SA-10 (1)		A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7 A.18.1.3 A.18.1.4
Change Control & Configuration Management Outsourced Development	CCC-02	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	The Esri System and Service Acquisition Policy details external information system services and associated compliance requirements. Esri requires external information system service providers to employ Security Baseline controls that align with FedRAMP Moderate requirements as well as applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.	NIST SP 800-53 R4 SA-4 NIST SP 800-53 R4 SA-4 (1) NIST SP 800-53 R4 SA-4 (2) NIST SP 800-53 R4 SA-4 (9) NIST SP 800-53 R4 SA-5 NIST SP 800-53 R4 SA-8 NIST SP 800-53 R4 SA-9 NIST SP 800-53 R4 SA-9 (1) NIST SP 800-53 R4 SA-10 NIST SP 800-53 R4 SA-10 (1) NIST SP 800-53 R4 SA-11 NIST SP 800-53 R4 SA-11 (1)		A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5
Change Control & Configuration Management Quality Testing	CCC-03	Organizations shall follow a defined quality change control and testing process (e.g., ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	Each change request submitted for EMCS Advanced Plus must include a change description, implementation plan, assessed level of risk, impact analysis, backout plan, assigned resources and a test plan prior to being approved. All changes are tested and validated in a staging environment prior to being pushed to production.	NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CM-2 NIST SP 800-53 R4 CM-2 (1) NIST SP 800-53 R4 CM-2 (2) NIST SP 800-53 R4 CM-2 (3) NIST SP 800-53 R4 CM-2 (7) NIST SP 800-53 R4 SA-3 NIST SP 800-53 R4 SA-4 NIST SP 800-53 R4 SA-4 (1) NIST SP 800-53 R4 SA-4 (2) NIST SP 800-53 R4 SA-5 NIST SP 800-53 R4 SA-8 NIST SP 800-53 R4 SA-10 NIST SP 800-53 R4 SA-10 (1) NIST SP 800-53 R4 SA-11 NIST SP 800-53 R4 SA-11 (1)		A.6.1.1 A.12.1.1 A.12.1.4 A.14.2.9 A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* partial A.14.2.2 8.1* partial A.14.2.3 8.1* partial A.14.2.4 A.12.6.1 A.16.1.3 A.18.2.2 A.18.2.3
Change Control & Configuration Management Unauthorized Software Installations	CCC-04	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end- point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Endpoint protection is used within EMCS Advanced Plus to continuously monitor all managed systems in real time to detect the presence of unauthorized software. Unauthorized software components are quarantined and Security Administrators are notified. Any software to be added to any EMCS Advanced Plus system must be authorized through existing change control procedures.	NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CM-2 NIST SP 800-53 R4 CM-2 (1) NIST SP 800-53 R4 CM-2 (3) NIST SP 800-53 R4 CM-2 (7) NIST SP 800-53 R4 CM-3 NIST SP 800-53 R4 CM-5 NIST SP 800-53 R4 CM-5 (1) NIST SP 800-53 R4 CM-5 (3)		A.6.1.2 A.12.2.1 A.9.4.4 A.9.4.1 A.12.5.1 8.1* (partial) A.14.2.4

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Change Control & Configuration Management Production Changes	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	All changes made to EMCS Advanced Plus must be authorized by appropriate personnel and fully tested prior to deployment to production. All changes are tracked and correspond directly to a specific change request.	NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CA-6 NIST SP 800-53 R4 CA-7 NIST SP 800-53 R4 CM-2 NIST SP 800-53 R4 CM-2 (1) NIST SP 800-53 R4 CM-2 (2) NIST SP 800-53 R4 CM-2 (3) NIST SP 800-53 R4 CM-2 (7) NIST SP 800-53 R4 CM-3 NIST SP 800-53 R4 CM-5 NIST SP 800-53 R4 CM-5 (1) NIST SP 800-53 R4 CM-5 (5) NIST SP 800-53 R4 CM-6 NIST SP 800-53 R4 CM-6 (1)	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.12.1.4 8.1* (partial) A.14.2.2 8.1* (partial) A.14.2.3
Data Security & Information Lifecycle Management Classification	DSI-01	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Customers are responsible for categorization of their owned data in EMCS Advanced Plus.	NIST SP 800-53 R4 AC-4 NIST SP 800-53 R4 RA-2		A.8.2.1
Data Security & Information Lifecycle Management Data Inventory / Flows	DSI-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's geographically distributed (physical and virtual) applications and infrastructure network and systems components and/or shared with other third parties to ascertain any regulatory, statutory, or supply chain agreement (SLA) compliance impact, and to address any other business risks associated with the data. Upon request, provider shall inform customer (tenant) of compliance impact and risk, especially if customer data is used as part of the services.	EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and all data remains on U.S. soil. All ingress into the EMCS Advanced Plus boundary is encrypted and restricted to port 443. Some inbound and some outbound network traffic can be limited to a customer-supplied IP whitelist.			Clause 4.2 5.2, 7.5, 8.1
Data Security & Information Lifecycle Management Ecommerce Transactions	DSI-03	Data related to electronic commerce (ecommerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	No e-commerce data is handled in EMCS Advanced Plus.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-22 NIST SP 800-53 R4 SC-8 NIST SP 800-53 R4 SC-8 (1) NIST SP 800-53 R4 SI-7	45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(i)	A.8.2.1 A.13.1.1 A.13.1.2 A.14.1.2 A.14.1.3 A.18.1.4
Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	DSI-04	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Customers maintain control of their data resident within EMCS Advanced Plus and are responsible for enforcing the procedures for handling it accordingly. In exceptional cases where data may be provided to Esri via physical media, it will marked for distribution limitations, handling caveats and applicable security markings.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 MP-1 NIST SP 800-53 R4 MP-3 NIST SP 800-53 R4 PE-16 NIST SP 800-53 R4 SI-1 NIST SP 800-53 R4 SI-12		A.8.2.2 A.8.3.1 A.8.2.3 A.13.2.1
Data Security & Information Lifecycle Management Non-Production Data	DSI-05	Production data shall not be replicated or used in non-production environments. Any use of customer data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	EMCS Advanced Plus has separate production and staging environments. At no time, shall production data ever be replicated or used outside the boundary of the production environment without customer permission.	NIST SP 800-53 R4 AC-4 (21) NIST SP 800-53 R4 SA-11 NIST SP 800-53 R4 SA-11 (1)	45 CFR 164.308(a)(4)(ii)(B)	A.8.1.3 A.12.1.4 A.14.3.1 8.1* (partial) A.14.2.2.
Data Security & Information Lifecycle Management Ownership / Stewardship	DSI-06	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Customers retain ownership of their data at all times in EMCS Advanced Plus and are responsible for associating organizational stewards for their data.	NIST SP 800-53 R4 AC-4 (21) NIST SP 800-53 R4 MP-7 (1) NIST SP 800-53 R4 PS-2 NIST SP 800-53 R4 RA-2 NIST SP 800-53 R4 SA-2	45 CFR 164.308 (a)(2)	A.6.1.1 A.8.1.2 A.18.1.4
Data Security & Information Lifecycle Management Secure Disposal	DSI-07	Policies and procedures shall be established with supporting business processes and technical measures implemented for the secure disposal and complete removal of data from all storage media, ensuring data is not recoverable by any computer forensic means.	Use of customer data outside of the EMCS Advanced Plus boundary is prohibited. The EMCS Advanced Pus environment is completely virtualized and resides on AWS IaaS resources and therefore physical media protection controls are inherited by AWS. In rare cases, where sensitive data is provided to Esri physically, the data is handled according to the existing Media Protection Policy for federally regulated data.	NIST SP 800-53 R4 AC-4 (21) NIST SP 800-53 R4 PE-1	45 CFR 164.310 (d)(2)(i) 45 CFR 164.310 (d)(2)(ii)	A.11.2.7 A.8.3.2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Datacenter Security Asset Management	DCS-01	Assets must be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards. At the PaaS and SaaS level, virtualized assets are classified and marked in terms of criticality and regularly reviewed / updated within the EMCS system inventory.	NIST SP 800-53 R4 MP-7 NIST SP 800-53 R4 MP-7 (1)		Annex A.8
Datacenter Security Controlled Access Points	DCS-02	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 PE-2 NIST SP 800-53 R4 PE-3 NIST SP 800-53 R4 PE-6 NIST SP 800-53 R4 PE-6 (1) NIST SP 800-53 R4 PE-8		A.11.1.1 A.11.1.2
Datacenter Security Equipment Identification	DCS-03	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Authentication to EMCS Advanced Plus uses a customer's SAML-compliant identity provider. EMCS Administrators connect from whitelisted IP addresses require multi-factor authentication.	NIST SP 800-53 R4 IA-3 NIST SP 800-53 R4 IA-4 NIST SP 800-53 R4 IA-4 (4)		
Datacenter Security Off-Site Authorization	DCS-04	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Any relocation of data outside the boundary of the EMCS Advanced Plus environment is restricted. EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-17 NIST SP 800-53 R4 AC-17 (1) NIST SP 800-53 R4 AC-17 (2) NIST SP 800-53 R4 AC-17 (3) NIST SP 800-53 R4 AC-17 (4) NIST SP 800-53 R4 MA-1 NIST SP 800-53 R4 PE-1 NIST SP 800-53 R4 PE-16 NIST SP 800-53 R4 PE-17	45 CFR 164.310 (c) 45 CFR 164.310 (d)(1) 45 CFR 164.310 (d)(2)(i)	A.11.2.6 A.11.2.7
Datacenter Security Off-Site Equipment	DCS-05	Policies and procedures shall be established for the secure disposal of equipment (by asset type) used outside the organization's premises. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	Use of customer data outside of the EMCS Advanced Plus boundary is prohibited. The EMCS Advanced Pus environment is completely virtualized and resides on AWS IaaS resources and therefore physical media protection controls are inherited by AWS. In rare cases, where sensitive data is provided to Esri physically, the data is handled according to the existing Media Protection Policy for federally regulated data.	NIST SP 800-53 R4 CM-8 NIST SP 800-53 R4 CM-8 (1) NIST SP 800-53 R4 CM-8 (3) NIST SP 800-53 R4 CM-8 (5) NIST SP 800-53 R4 MP-6 NIST SP 800-53 R4 MP-6 (2)	45 CFR 164.310 (d)(2)(iii)	A.8.1.1 A.8.1.2
Datacenter Security Policy	DCS-06	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive information.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 PE-2 NIST SP 800-53 R4 PE-3 NIST SP 800-53 R4 PE-4 NIST SP 800-53 R4 PE-5 NIST SP 800-53 R4 PE-6 NIST SP 800-53 R4 PE-6 (1)	45 CFR 164.310(a)(1) 45 CFR 164.310(a)(2)(ii) 45 CFR 164.310(b) 45 CFR 164.310 (c) (New)	A.11.1.1 A.11.1.2
Datacenter Security Secure Area Authorization	DCS-07	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 PE-16		A.11.1.6
Datacenter Security Unauthorized Persons Entry	DCS-08	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 MA-1 NIST SP 800-53 R4 MA-2 NIST SP 800-53 R4 MA-5 (1) NIST SP 800-53 R4 PE-16 NIST SP 800-53 R4 SC-39	45 CFR 164.310 (d)(1)	A.11.2.5 8.1* (partial) A.12.1.2
Datacenter Security User Access	DCS-09	Physical access to information assets and functions by users and support personnel shall be restricted.	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards.	NIST SP 800-53 R4 MA-5 (1) NIST SP 800-53 R4 PE-2 NIST SP 800-53 R4 PE-3 NIST SP 800-53 R4 PE-6 NIST SP 800-53 R4 PE-6 (1)		A.11.1.1
Encryption & Key Management Entitlement	EKM-01	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Within the EMCS Boundary, Administration and Infrastructure keys are managed through key management which aligns with FedRAMP Moderate security requirements.			Annex A.10.1 A.10.1.1 A.10.1.2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Encryption & Key Management Key Generation	EKM-02	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	The EMCS Advanced Plus uses cryptographic protections to protect customer data at rest and all data-in-transit leaving the authorization boundary. All cryptographic algorithms being used to protect data throughout the Application Infrastructure are FIPS 140-2 compliant including: 2048-bit (or higher) RSA asymmetric keys, AES 256-bit symmetric keys and SHA-256 hashing. The Agency data is encrypted at rest with AES-256 using Amazon EBS encryption.	NIST SP 800-53 R4 SC-12 NIST SP 800-53 R4 SC-13 NIST SP 800-53 R4 SC-17 NIST SP 800-53 R4 SC-28 (1)	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312(e)(1)	Clauses 5.2(c) 5.3(a) 5.3(b) 7.5.3(b) 7.5.3(d) 8.1 8.3 9.2(g) A.8.2.3 A.10.1.2 A.18.1.5
Encryption & Key Management Sensitive Data Protection	EKM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Customers and EMCS Administrators must connect to EMCS infrastructure using TLS only. EMCS only permits connections on port 443. The confidentiality and integrity of customer data at rest is protected by using AES-256 FIPS 140-2 compliant encryption.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-18 NIST SP 800-53 R4 AC-18 (1) NIST SP 800-53 R4 IA-7 NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-8 NIST SP 800-53 R4 SC-8 (1) NIST SP 800-53 R4 SC-13 NIST SP 800-53 R4 SC-23 NIST SP 800-53 R4 SC-28 NIST SP 800-53 R4 SC-28 (1) NIST SP 800-53 R4 SI-8	45 CFR 164.312 (a)(2)(iv) 45 CFR 164.312 (e)(1) 45 CFR 164.312 (e)(2)(ii)	A.13.1.1 A.8.3.3 A.13.2.3 A.14.1.3 A.14.1.2 A.10.1.1 A.18.1.3 A.18.1.4
Encryption & Key Management Storage and Access	EKM-04	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e., at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	EMCS uses AES-256 encryption and FIPS 140-2 compliant algorithms for both data in transit and at rest respectively. For EMCS Administrators, key management and key usage duties are separated. Customers have the implementation option available to use their trusted key management solution to avoid having their keys stored in the cloud.	NIST SP 800-53 R4 SC-12 NIST SP 800-53 R4 SC-12 (2) NIST SP 800-53 R4 SC-12 (3)		Annex A.10.1 A.10.1.1 A.10.1.2
Governance and Risk Management Baseline Requirements	GRM-01	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory, and regulatory compliance obligations. Deviations from standard baseline configurations must be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements must be reassessed at least annually unless an alternate frequency has been established and authorized based on business needs.	EMCS security controls align with FedRAMP Moderate requirements. Any changes to the baseline configuration is tracked and authorized through established change control policies and procedures. A full security control review is conducted annually along with a vulnerability assessment and penetration testing to ensure compliance. Otherwise, compliance with the baseline is constantly monitored through the FedRAMP required Continuous Monitoring Plan.	NIST SP 800-53 R4 CM-2 NIST SP 800-53 R4 CM-2 (1) NIST SP 800-53 R4 CM-2 (3) NIST SP 800-53 R4 CM-2 (7) NIST SP 800-53 R4 CM-10 (1) NIST SP 800-53 R4 CM-11 NIST SP 800-53 R4 SA-2 NIST SP 800-53 R4 SA-4 NIST SP 800-53 R4 SA-4 (1)		A.14.1.1 A.18.2.3

Governance and Risk Management
Data Focus Risk Assessments
	GRM-02	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following:
		• Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure
		• Compliance with defined retention periods and end-of-life disposal requirements
		• Data classification and protection from unauthorized use, access, loss, destruction, and falsification
			The customers are responsible for the categorization and classification of their owned data hosted within EMCS Advanced Plus. Security controls aligning with FedRAMP Moderate ensure sensitive data is stored in secured locations within EMCS Advanced Plus, encrypted in-transit and at-rest and monitored by a 24/7 Security Operations Center (SOC) for unauthorized access. This protects the confidentiality, integrity and availability of resident data. Vulnerability assessments occur monthly by EMCS Security Administrators and a full risk assessment including security control review, vulnerability assessment and penetration testing occur annually by an accredited third party auditor.	NIST SP 800-53 R4 AC-6 (9) NIST SP 800-53 R4 AC-21 NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 RA-2 NIST SP 800-53 R4 RA-3 NIST SP 800-53 R4 SI-12	45 CFR 164.308(a)(1)(ii)(A)
					45 CFR 164.308(a)(8)
						Clauses 5.2(c)
						5.3(a)
						5.3(b)
						6.1.2
						6.1.2(a)(2)
						6.1.3(b)
						7.5.3(b)
						7.5.3(d)
						8.1
						8.2
						8.3
						9.2(g)

Governance and Risk Management Management Oversight	GRM-03	Managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Individuals assigned to work on EMCS Advanced Plus in any capacity must complete initial training on topics including security responsibilities, security architecture overview, indicators of insider threats and advanced persistent threats, defending against phishing and social engineering attacks, cloud security procedures, EMCS security controls and reporting responsibilities. Role-based training is also mandated for employees working on EMCS Advanced Plus.	NIST SP 800-53 R4 AT-2 NIST SP 800-53 R4 AT-3 NIST SP 800-53 R4 AT-4 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CA-5 NIST SP 800-53 R4 CA-6 NIST SP 800-53 R4 CA-7		Clause 7.2(a,b) A.7.2.1 A.7.2.2 A.9.2.5 A.18.2.2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Governance and Risk Management Management Program	GRM-04	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	The Esri Security Awareness and Training Policy documents corporate policies and have been adapted for EMCS Advanced Plus. As part of FedRAMP alignment, EMCS must maintain compliance across an expansive 17 control families including: • Access Control • Awareness and Training • Audit and Accountability • Security Assessment and Authorization • Configuration Management • Contingency Planning • Identification and Authentication • Incident Response • Maintenance • Media Protection • Physical and Environmental Protection • Planning • Personnel Security • Risk Assessment • System and Services Acquisition • System and Communications Protection • System and Information Integrity	NIST SP 800-53 R4 AC-6 (5) NIST SP 800-53 R4 PL-2 (3)	45 CFR 164.308(a)(1)(i) 45 CFR 164.308(a)(1)(ii)(B) 45 CFR 164.316(b)(1)(i) 45 CFR 164.308(a)(3)(i) (New) 45 CFR 164.306(a) (New)	All in sections 4, 5, 6, 7, 8, 9, 10. A.6.1.1 A.13.2.4 A.6.1.3 A.6.1.4 A.18.2.1
Governance and Risk Management Management Support/Involvement	GRM-05	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Corporate security policies are reviewed at least every three years by the Esri CISO or delegate and updated as necessary. EMCS Advanced Plus specific policies and procedures are reviewed yearly as part of the control review.	NIST SP 800-53 R4 CM-1	45 CFR 164.316 (b)(2)(ii) 45 CFR 164.316 (b)(2)(iii)	All in section 5 plus clauses 4.4 4.2(b) 6.1.2(a)(1) 6.2
Governance and Risk Management Policy	GRM-06	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies must be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	As part of the FedRAMP process, Esri Corporate Security policies must be signed and authorized by the Esri CISO and are submitted as part of the package to FedRAMP. Security roles and responsibilities within EMCS Advanced Plus are clearly defined and role- based security training is required for all personnel with assigned security roles.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IR-1 NIST SP 800-53 R4 MA-1 NIST SP 800-53 R4 MP-1 NIST SP 800-53 R4 PE-1 NIST SP 800-53 R4 PL-1 NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 SA-1 NIST SP 800-53 R4 SC-1 NIST SP 800-53 R4 SI-1	45 CFR 164.316 (a) 45 CFR 164.316 (b)(1)(i) 45 CFR 164.316 (b)(2)(ii) 45 CFR 164.308(a)(2)	Clause 4.3 Clause 5 4.4 4.2(b) 6.1.2(a)(1) 6.2 6.2(a) 6.2(d) 7.1 7.4 9.3 10.2 7.2(a) 7.2(b) 7.2(c)
Governance and Risk Management Policy Enforcement	GRM-07	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures must be stated in the policies and procedures.	Prior to accessing EMCS Advanced Plus, all employees must acknowledge and sign a Rules of Behavior (RoB) document that outlines technical and organizational responsibilities related to the access and use of EMCS Advanced Plus, a FedRAMP Moderate system. Key security policies are also highlighted in the document. The RoB is reviewed, updated and re-signed annually.	NIST SP 800-53 R4 PL-4 NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 PS-8	45 CFR 164.308 (a)(1)(ii)(C)	A7.2.3
Governance and Risk Management Policy Impact on Risk Assessments	GRM-08	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	As part of the continuous monitoring process, a full security control review and risk assessment is conducted annually which includes associated policies and procedures as they relate to EMCS Advanced Plus. This yearly review is conducted by an accredited FedRAMP third party assessment organization (3PAO). The EMCS Advanced Plus IaaS provider undergoes the same assessment as part of maintaining their FedRAMP Moderate compliance.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CP-1 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IR-1 NIST SP 800-53 R4 MA-1 NIST SP 800-53 R4 MP-1 NIST SP 800-53 R4 PE-1 NIST SP 800-53 R4 PL-1 NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 RA-1 NIST SP 800-53 R4 RA-3 NIST SP 800-53 R4 SC-1 NIST SP 800-53 R4 SI-1		Clause 4.2.1 a, 4.2(b) 4.3 c, 4.3(a&b) 4.4 5.1(c) 5.1(d) 5.1(e) 5.1(f) 5.1(g) 5.1(h) 5.2 5.2 e, 5.2(f) 5.3 6.1.1(e)(2),

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Governance and Risk Management Policy Reviews	GRM-09	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	As part of the FedRAMP process, EMCS policies must be signed and authorized by the Esri CISO and are submitted as part of the package to FedRAMP. These policies are reviewed at a minimum of annually to ensure they align with industry and FedRAMP Moderate standards.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CP-1 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-5 NIST SP 800-53 R4 IA-5 (1) NIST SP 800-53 R4 IA-5 (2) NIST SP 800-53 R4 IA-5 (3) NIST SP 800-53 R4 IA-5 (6)	45 CFR 164.316 (b)(2)(iii) 45 CFE 164.306€	Clause 8.1 A.5.1.2

Governance and Risk Management
Risk Assessments
	GRM-10	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	As part of the continuous monitoring process, a full security control review and risk assessment is conducted annually which includes associated policies and procedures as they relate to EMCS Advanced Plus. This yearly review is conducted by an accredited FedRAMP third party assessment organization (3PAO). The EMCS Advanced Plus IaaS provider, AWS, undergoes the same assessment as part of maintaining their FedRAMP Moderate compliance.	NIST SP 800-53 R4 RA-1 NIST SP 800-53 R4 RA-2 NIST SP 800-53 R4 RA-3	45 CFR 164.308 (a)(1)(ii)(A)	Clause 4.2(b),
						6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)
						6.1.2(d)(1) 6.1.2(d)(2)

Governance and Risk Management
Risk Management Framework
	GRM-11	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	To comply with FedRAMP Moderate requirements, any items with a residual risk of "High" will be mitigated within 30 days, "Moderate" level items mitigated within 90 days and "Low" level items mitigated within 180 days. Outstanding items are maintained in the Plan of Actions and Milestones (POAM) and are reviewed at a minimum of monthly to ensure stated time frames are met.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CA-6 NIST SP 800-53 R4 CA-7 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 PL-1 NIST SP 800-53 R4 RA-1 NIST SP 800-53 R4 RA-2 NIST SP 800-53 R4 RA-3 NIST SP 800-53 R4 SA-9 (1) NIST SP 800-53 R4 SI-4 NIST SP 800-53 R4 SI-4 (2)
				NIST SP 800-53 R4 SI-4 (4)
				NIST SP 800-53 R4 SI-4 (5)
					45 CFR 164.308 (a)(8)
					45 CFR 164.308(a)(1)(ii)(B)
						Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)
						6.1.2(d)(1) 6.1.2(d)(2)
						6.1.2(d)(3) 6.1.2(e)
						6.1.2(e)(1) 6.1.2(e)(2)

Human Resources Asset Returns	HRS-01	Upon termination of workforce personnel and/or expiration of external business relationships, all organizationally- owned assets shall be returned within an established period.	When an Esri employee assigned to EMCS Advanced Plus announces separation from Esri, for any reason, the EMCS Program Manager and ISSO are notified. Credentials to EMCS Advanced Plus systems are then subsequently revoked. In case of termination for cause, credentials are revoked from the system prior to the individual being notified.	NIST SP 800-53 R4 PS-4	45 CFR 164.308 (a)(3)(ii)(C)	A.8.1.1 A.8.1.2 A.8.1.4
Human Resources Background Screening	HRS-02	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Esri conducts background investigation/screening for all new employees. All employees assigned to EMCS Advanced Plus accessing customer data are confirmed U.S. persons. Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions	NIST SP 800-53 R4 PS-2 NIST SP 800-53 R4 PS-3 NIST SP 800-53 R4 PS-3 (3)		A.7.1.1
Human Resources Employment Agreements	HRS-03	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets	Newly hired personnel are required to sign an agreement covering adherence to established governance and security policies. In addition, employees requiring access to EMCS must fill out an additional Access Request form and sign a Rules of Behavior document annually that outlines technical and organizational responsibilities.	NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 PS-2 NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 PS-7	45 CFR 164.310(a)(1) 45 CFR 164.308(a)(4)(i)	A.13.2.4 A.7.1.2
Human Resources Employment Termination	HRS-04	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Roles and responsibilities for employment termination or transfer are clearly assigned, documented and communicated for EMCS Advanced personnel.	NIST SP 800-53 R4 PS-2 NIST SP 800-53 R4 PS-4 NIST SP 800-53 R4 PS-5 NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 PS-8	45 CFR 164.308 (a)(3)(ii)(C)	A.7.3.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Human Resources Mobile Device Management	HRS-05	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Esri has a mobile device policy that must be acknowledge by all employees. No mobile devices are used to administer EMCS Advanced Plus systems.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-17 NIST SP 800-53 R4 AC-17 (1) NIST SP 800-53 R4 AC-17 (2) NIST SP 800-53 R4 AC-17 (3) NIST SP 800-53 R4 AC-17 (4) NIST SP 800-53 R4 AC-18 NIST SP 800-53 R4 AC-18 (1) NIST SP 800-53 R4 AC-19 NIST SP 800-53 R4 MP-2 NIST SP 800-53 R4 MP-4 NIST SP 800-53 R4 MP-7	45 CFR 164.310 (d)(1)	A.8.2.1 A.8.3.1 A.8.3.2 A.8.3.3 A.6.2.1 A.6.2.2 A.18.1.4
Human Resources Non-Disclosure Agreements	HRS-06	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed at planned intervals.	Non-disclosure agreements are reviewed annually to ensure accuracy. SLAs are signed and enforced for third parties associated with EMCS Advanced Plus.	NIST SP 800-53 R4 PL-4 NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 SA-9 NIST SP 800-53 R4 SA-9 (1)		A.13.2.4
Human Resources Roles / Responsibilities	HRS-07	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	All roles and responsibilities for EMCS Advanced Plus personnel are clearly defined in the System Security Plan (SSP). This is done to provide clear context as well as to ensure appropriate segregation of duties to align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 PL-4 NIST SP 800-53 R4 PS-1 NIST SP 800-53 R4 PS-2 NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 PS-7		Clause 5.3 A.6.1.1 A.6.1.1
Human Resources Technology Acceptable Use	HRS-08	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	All Esri employees must acknowledge an acceptable use policy. Furthermore, Esri employees with access to EMCS Advanced Plus have encryption at-rest on both their issued workstations.	NIST SP 800-53 R4 AC-8 NIST SP 800-53 R4 AC-20 NIST SP 800-53 R4 AC-20 (1) NIST SP 800-53 R4 AC-20 (2) NIST SP 800-53 R4 PL-4	45 CFR 164.310 (b)	A.8.1.3
Human Resources Training / Awareness	HRS-09	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	In addition to the corporate security policy within Esri, there is specific security awareness training for employees that develop and maintain EMCS. Role-based training and annual refresher training is required and enforced through a series of tests. Security awareness training includes but is not limited to topics such as: insider threats, security responsibilities, advanced persistent threats, anti-phishing, mobile, social engineering awareness and cloud security.	NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AT-2 NIST SP 800-53 R4 AT-3 NIST SP 800-53 R4 AT-4	45 CFR 164.308 (a)(5)(i) 45 CFR 164.308 (a)(5)(ii)(A)	Clause 7.2(a), 7.2(b) A.7.2.2
Human Resources User Responsibility	HRS-10	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	In addition to role-based training for employees accessing and administering EMCS Advanced Plus, security awareness training and mandated refresher training is in place. This ensures compliance with FedRAMP Moderate requirements.	NIST SP 800-53 R4 AT-2 NIST SP 800-53 R4 AT-3 NIST SP 800-53 R4 AT-4 NIST SP 800-53 R4 PL-4	45 CFR 164.308 (a)(5)(ii)(D)	Clause 7.2(a), 7.2(b) A.7.2.2 A.9.3.1 A.11.2.8
Human Resources Workspace	HRS-11	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	All EMCS employees abide by a clean-desk policy. In addition to established lockout in place for workstations, sessions within EMCS Advanced Plus are also locked after a period of inactivity.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 (5) NIST SP 800-53 R4 AC-11 NIST SP 800-53 R4 AC-12 NIST SP 800-53 R4 MP-1 NIST SP 800-53 R4 MP-2 NIST SP 800-53 R4 MP-3 NIST SP 800-53 R4 MP-4		Clause 7.2(a), 7.2(b) A.7.2.2 A.11.1.5 A.9.3.1 A.11.2.8 A.11.2.9
Identity & Access Management Audit Tools Access	IAM-01	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segregated and access restricted to prevent inappropriate disclosure and tampering of log data.	EMCS Advanced Plus security infrastructure exists on an isolated private network subnet. SIEM agents collect and store logs in an off-site Security Operations Center. Current implementation ensures only EMCS Advanced Plus Administrators can read logs. Collected logs may not be modified or deleted by anyone.	NIST SP 800-53 R4 AC-17 (9) NIST SP 800-53 R4 AU-9 NIST SP 800-53 R4 AU-9 (2) NIST SP 800-53 R4 AU-9 (4)		

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Identity & Access Management Credential Lifecycle / Provision Management	IAM-02	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures must incorporate the following: • Procedures, supporting roles, and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible	EMCS supports integration with SAML compliant Identity Providers (IdP) to ensure users can leverage existing authentication mechanisms as well as existing organization- approved policies, procedures and processes for account provisioning through revocation. Esri employees working on EMCS Advanced Plus obtain account privileges through existing account provisioning processes and approval must be obtained from the EMCS Advanced Plus ISSO. Multi-factor authentication is required by EMCS Advanced Plus administrators and access to the infrastructure is limited by segmentation and using a bastion host. Any employee with access to EMCS Advanced Plus will have credentials revoked if transferred, dismissed or leaving the organization based on existing revocation procedures. In addition, the system audits creation, modification, enabling and removal actions for accounts that is automatically monitored by a 24/7 Security Operations Center.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 (9) NIST SP 800-53 R4 AC-2 (10) NIST SP 800-53 R4 AC-7 NIST SP 800-53 R4 AC-10 NIST SP 800-53 R4 AC-14 NIST SP 800-53 R4 AC-17 (9) NIST SP 800-53 R4 CM-7 (5) NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-2 (11) NIST SP 800-53 R4 RA-5 (8)	45 CFR 164.308 (a)(3)(i) 45 CFR 164.312 (a)(1) 45 CFR 164.312 (a)(2)(ii) 45 CFR 164.308(a)(4)(ii)(B) 45 CFR 164.308(a)(4)(ii)(c)	A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5 A.9.1.2 A.9.4.1
Identity & Access Management Diagnostic / Configuration Ports Access	IAM-03	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Customer users may only access their application over port 443.EMCS is a hardened environment that implements strict port control by using the principle of least privilege for all EMCS Advanced Plus Administrators and by restricting access to ports using AWS security groups.	NIST SP 800-53 R4 CM-7 NIST SP 800-53 R4 CM-7 (1) NIST SP 800-53 R4 CM-7 (5) NIST SP 800-53 R4 MA-3 NIST SP 800-53 R4 MA-3 (1) NIST SP 800-53 R4 MA-3 (2) NIST SP 800-53 R4 MA-3 (3) NIST SP 800-53 R4 MA-4 NIST SP 800-53 R4 MA-4 (2) NIST SP 800-53 R4 MA-5		A.13.1.1 A.9.1.1 A.9.4.4
Identity & Access Management Policies and Procedures	IAM-04	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Account management (create, modify, delete, disable) requests are logged into an incident management system to track all events. Accounts are centrally managed within the EMCS Advanced Plus infrastructure. All Esri personnel accessing EMCS Advanced Plus have been approved by EMCS ISSO and are confirmed U.S. persons. All accounts and associated privileges are reviewed at a minimum of annually as part of compliance with FedRAMP Moderate requirements.	NIST SP 800-53 R4 IA-2 (5)		Annex A.9.2 A.9.2.1 A.9.2.2 A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6
Identity & Access Management Segregation of Duties	IAM-05	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Customers are advised to leverage their SAML compliant Identity Provider (IdP) to process authorization for their application within EMCS Advanced Plus. It is the customer's responsibility to restrict user access as defined in their policies and procedures. EMCS Advanced Plus Administrators are segregated based on organizational and administrative roles. Role-based access control is used to assign different privileges to support specific functions including, but not limited to, Security, Application, and Infrastructure administration.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 (1) NIST SP 800-53 R4 AC-2 (2) NIST SP 800-53 R4 AC-2 (3) NIST SP 800-53 R4 AC-2 (4) NIST SP 800-53 R4 AC-2 (7) NIST SP 800-53 R4 AC-2 (9) NIST SP 800-53 R4 AC-5 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AC-6 (1) NIST SP 800-53 R4 AC-6 (2) NIST SP 800-53 R4 AC-6 (9) NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 AU-2 NIST SP 800-53 R4 AU-6 NIST SP 800-53 R4 AU-6 (1) NIST SP 800-53 R4 AU-6 (3) NIST SP 800-53 R4 SI-4 NIST SP 800-53 R4 SI-4 (2) NIST SP 800-53 R4 SI-4 (4)	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308(a)(4)(ii)(A) 45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.6.1.2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Identity & Access Management Source Code Access Restriction	IAM-06	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	EMCS Advanced Plus is made up of Esri COTS software. Customer-driven custom software implementation, where applicable is managed and maintained by Esri under role-based access restricted source control. All Esri personnel accessing EMCS Advanced Plus are subject to strict role-based access control policies and procedures. Customers are responsible for managing their user access to the application by leveraging a SAML compliant Identity Provider (IdP).	NIST SP 800-53 R4 AC-6 (5) NIST SP 800-53 R4 CM-5 NIST SP 800-53 R4 CM-5 (1) NIST SP 800-53 R4 CM-5 (5)		Clause 5.2(c) 5.3(a), 5.3(b), 7.5.3(b) 7.5.3(d) 8.1, 8.3 9.2(g) A.9.4.5 A.18.1.3
Identity & Access Management Third Party Access	IAM-07	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	EMCS Advanced Plus enforces ISAs and Service Level Agreements with external third party organizations which specifies the types of communications in place and associated security controls in alignment with FedRAMP Moderate compliance.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 (5) NIST SP 800-53 R4 AC-21 NIST SP 800-53 R4 AT-1 NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 CA-1 NIST SP 800-53 R4 CM-1 NIST SP 800-53 R4 CP-1 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-4 NIST SP 800-53 R4 IA-5 NIST SP 800-53 R4 IA-5 (1) NIST SP 800-53 R4 IA-5 (2) NIST SP 800-53 R4 IA-5 (3) NIST SP 800-53 R4 IA-5 (6) NIST SP 800-53 R4 IA-5 (7) NIST SP 800-53 R4 IA-8		A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.5
Identity & Access Management Trusted Sources	IAM-08	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Esri personnel with access to EMCS Advanced Plus have privileges that are assigned based on role and through using the principle of least-privilege as mandated by FedRAMP Moderate requirements.			Annex A.9.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3, A.9.4.5

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Identity & Access Management User Access Authorization	IAM-09	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners, and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Customers are responsible for managing access to the application portion of EMCS by leveraging a SAML compliant Identity Provider for identity federation. Esri personnel who are accessing EMCS Advanced Plus for the purpose of maintenance and administration. Account access is strictly controlled using approved policies and procedures that align with FedRAMP Moderate requirements. All access to EMCS must first be authorized by the EMCS ISSO.	NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 AC-2 (9) NIST SP 800-53 R4 AC-2 (12) NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-5 NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AC-6 (1) NIST SP 800-53 R4 AC-6 (2) NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 IA-2 (1) NIST SP 800-53 R4 IA-2 (2) NIST SP 800-53 R4 IA-2 (3) NIST SP 800-53 R4 IA-2 (8) NIST SP 800-53 R4 IA-4 NIST SP 800-53 R4 IA-4 (4) NIST SP 800-53 R4 IA-5	45 CFR 164.308 (a)(3)(i) 45 CFR 164.308 (a)(3)(ii)(A) 45 CFR 164.308 (a)(4)(i) 45 CFR 164.308 (a)(4)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C) 45 CFR 164.312 (a)(1)	A.9.2.1, A.9.2.2 A.9.2.3 A.9.1.2 A.9.4.1
Identity & Access Management User Access Reviews	IAM-10	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	As customers manage user access to their application within EMCS Advanced Plus, they are responsible for revalidating access. User access is reviewed quarterly for Esri personnel accessing EMCS Advanced Plus systems.	NIST SP 800-53 R3 AC-2 NIST SP 800-53 R4 AC-2 (1) NIST SP 800-53 R4 AC-2 (2) NIST SP 800-53 R4 AC-2 (3) NIST SP 800-53 R4 AC-2 (4) NIST SP 800-53 R4 AC-2 (7) NIST SP 800-53 R4 AC-2 (9) NIST SP 800-53 R4 AC-2 (10) NIST SP 800-53 R4 AC-6 (9) NIST SP 800-53 R4 AU-6 NIST SP 800-53 R4 AU-6 (1) NIST SP 800-53 R4 AU-6 (3) NIST SP 800-53 R4 CM-7 (2) NIST SP 800-53 R4 PS-3 (3) NIST SP 800-53 R4 PS-6 NIST SP 800-53 R4 PS-	45 CFR 164.308 (a)(3)(ii)(B) 45 CFR 164.308 (a)(4)(ii)(C)	A.9.2.5
Identity & Access Management User Access Revocation	IAM-11	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change, or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Customers manage access to their EMCS Advanced Plus application using a SAML compliant Identity Provider (IdP). As such, customers are able to use existing de-provisioning procedures to disable access to the application. In alignment with FedRAMP Moderate requirements, EMCS Advanced Plus Security Administrators are notified when: 1. Accounts are no longer required, so they may be disabled 2. When users are terminated or transferred, so the accounts may be disabled 3. When need-to-know changes, so that privileges may be re-assessed and adjusted	NIST SP 800-53 R4 AC-2 (1) NIST SP 800-53 R4 AC-2 (2) NIST SP 800-53 R4 AC-2 (3) NIST SP 800-53 R4 AC-2 (4) NIST SP 800-53 R4 AC-2 (7) NIST SP 800-53 R4 AC-2 (10) NIST SP 800-53 R4 AC-6 (9) NIST SP 800-53 R4 PS-4 NIST SP 800-53 R4 PS-5	45 CFR 164.308(a)(3)(ii)(C)	Annex A A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.3
Identity & Access Management User ID Credentials	IAM-12	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re- use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Customers are to provide a SAML compliant Identity Provider (IdP) to leverage their existing enterprise authentication mechanisms (PKI, smartcards, tokens) and are therefore responsible for managing user credentials according to organization policies, procedures and processes. All Esri personnel accessing EMCS Advanced Plus authenticate using multi-factor authentication managed based on role. Access is assigned using the principle of least-privilege based on industry standard practices. EMCS Advanced Pus account credentials are managed from instantiation through revocation through robust processes that align with FedRAMP Moderate requirements. Service accounts are uniquely instantiated for each customer.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-2 NIST SP 800-53 R4 AC-2 (10) NIST SP 800-53 R4 AC-3 NIST SP 800-53 R4 AC-11 NIST SP 800-53 R4 AC-11 (1) NIST SP 800-53 R4 AU-2 NIST SP 800-53 R4 AU-2 (3) NIST SP 800-53 R4 AU-11 NIST SP 800-53 R4 IA-1 NIST SP 800-53 R4 IA-2 NIST SP 800-53 R4 IA-2 (1) NIST SP 800-53 R4 IA-2 (2) NIST SP 800-53 R4 IA-2 (3) NIST SP 800-53 R4 IA-2 (8) NIST SP 800-53 R4 IA-5 NIST SP 800-53 R4 IA-5 (1) NIST SP 800-53 R4 IA-5 (2) NIST SP 800-53 R4 IA-5 (3) NIST SP 800-53 R4 IA-5 (6) NIST SP 800-53 R4 IA-5 (7) NIST SP 800-53 R4 IA-6 NIST SP 800-53 R4 IA-8 NIST SP 800-53 R4 SC-10	45 CFR 164.308(a)(5)(ii)(c) 45 CFR 164.308 (a)(5)(ii)(D) 45 CFR 164.312 (a)(2)(i) 45 CFR 164.312 (a)(2)(iii) 45 CFR 164.312 (d)	A.9.2.6 A.9.1.1 A.9.2.1, A.9.2.2 A.9.2.4 A.9.2.5 A.9.4.2

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Identity & Access Management Utility Programs Access	IAM-13	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	All EMCS Advanced Plus administrators are assigned role-based privileges based on the principle of least privilege. Access to supporting physical, network, and hypervisor infrastructure is restricted to Security and Infrastructure teams only and implement multi-factor authentication protocols. To align with FedRAMP Moderate requirements, separation of duties guidelines are enforced to prevent access control conflicts of interest.	NIST SP 800-53 R4 AC-6 NIST SP 800-53 R4 AC-6 (1) NIST SP 800-53 R4 AC-6 (2) NIST SP 800-53 R4 CM-7 NIST SP 800-53 R4 CM-7 (1) NIST SP 800-53 R4 CM-7 (2) NIST SP 800-53 R4 CM-7 (5)		A.9.1.2 Deleted A.9.4.4
Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	IVS-01	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Logs within EMCS are fed in an enterprise Security Information and Event Management (SIEM) system to perform correlation of potentially suspicious behavior based on both signature and heuristic analysis. Examples of some of the events that are logged are: successful login events, unsuccessful login events, account management, object access, policy change and privilege functions. The logs capture sufficient to detail to conduct proper audit and investigative measures if suspicious activity has been noticed. All audit records are maintained for a minimum of ninety (90) days to align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 AU-2 NIST SP 800-53 R4 AU-2 (3) NIST SP 800-53 R4 AU-3 NIST SP 800-53 R4 AU-3 (1) NIST SP 800-53 R4 AU-4 NIST SP 800-53 R4 AU-5 NIST SP 800-53 R4 AU-6 NIST SP 800-53 R4 AU-6 (1) NIST SP 800-53 R4 AU-6 (3) NIST SP 800-53 R4 AU-7 NIST SP 800-53 R4 AU-7 (1) NIST SP 800-53 R4 AU-9 NIST SP 800-53 R4 AU-9 (4) NIST SP 800-53 R4 AU-11	45 CFR 164.308 (a)(1)(ii)(D) 45 CFR 164.312 (b) 45 CFR 164.308(a)(5)(ii)©	A.12.4.1 A.12.4.1 A.12.4.2, A.12.4.3 A.12.4.3 A.12.4.1 A.9.2.3 A.9.4.4 A.9.4.1 A.16.1.2 A.16.1.7 A.18.2.3 A.18.1.3
Infrastructure & Virtualization Security Change Detection	IVS-02	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g., dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g., portals or alerts).	EMCS uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards. AWS ensures the integrity of the Amazon Machine Images (AMI).	NIST SP 800-53 R4 SA-10 (1)		Annex A.12.1.2 A.12.4, A.12.4.1, A.12.4.2, A.12.4.3, A.12.6.1, A.12.6.2, A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7
Infrastructure & Virtualization Security Clock Synchronization	IVS-03	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	The EMCS Advanced Plus system utilizes the Windows Time Service (W32Time) to generate time stamps for audit records for all components of the system. The EMCS Advanced Plus system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC), synchronized to the central secured NTP (provided by the Active Directory PDC) server hosted within the infrastructure to the nearest 15 milliseconds. The central secured Active Directory NTP server is then synchronized to four (4) time-g.nist.gove NTP servers to the nearest 15 milliseconds.	NIST SP 800-53 R4 AU-1 NIST SP 800-53 R4 AU-8 NIST SP 800-53 R4 AU-8 (1)		A.12.4.1 A.12.4.4
Infrastructure & Virtualization Security Information System Documentation	IVS-04	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	System design and architecture requirements are gathered prior to onboarding EMCS Advanced Plus customer systems. For third party components, EMCS Advanced Plus utilizes vendor best practice recommendations for capacity planning efforts. In addition, there are network level tools in place to monitor capacity and performance for all components within EMCS Advanced Plus.	NIST SP 800-53 R4 SA-4 NIST SP 800-53 R4 SA-4 (1)		A.12.1.3

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Infrastructure & Virtualization Security Vulnerability Management	IVS-05	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g., virtualization aware).	All security vulnerability assessment tools accommodate virtualization technologies.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1),
Infrastructure & Virtualization Security Network Security	IVS-06	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, ports, and by compensating controls.	Customers accessing their application are restricted to using port 443 (HTTPS) and all traffic passes through a Web Application Firewall (WAF). Infrastructure is logically separated to isolate customer data flows from administrative data flows using Virtual Private Cloud (VPCs). All changes to these rules must be documented and approved according to EMCS Advanced Plus configuration management processes and all traffic flow exceptions for instances within EMCS are reviewed annually to align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 AC-4 (21) NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CA-3 (3) NIST SP 800-53 R4 CA-3 (5) NIST SP 800-53 R4 CA-9 NIST SP 800-53 R4 CM-7 NIST SP 800-53 R4 CM-7 (1) NIST SP 800-53 R4 CM-7 (2) NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (3) NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-7 (5) NIST SP 800-53 R4 SC-7 (7) NIST SP 800-53 R4 SC-7 (8) NIST SP 800-53 R4 SC-7 (12) NIST SP 800-53 R4 SC-7 (13) NIST SP 800-53 R4 SC-7 (18) NIST SP 800-53 R3 SC-20 NIST SP 800-53 R4 SC-21 NIST SP 800-53 R4 SC-22		A.13.1.1 A.13.1.2 A.14.1.2 A.12.4.1 A.9.1.2 A.13.1.3 A.18.1.4
Infrastructure & Virtualization Security OS Hardening and Base Controls	IVS-07	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	EMCS Advanced Plus has developed mandatory security configuration settings to align with industry best practices such as CIS benchmarks. Anti-virus, logging and Intrusion Detection System (IDS) capabilities are ensured and monitored on all systems within EMCS Advanced Plus.			Annex A.12.1.4 A.12.2.1 A.12.4.1 A.12.6.1
Infrastructure & Virtualization Security Production / Non-Production Environments	IVS-08	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	A completely separate staging environment is maintained for EMCS Advanced Plus. All changes must be documented through change control processes and authorized by the EMCS ISSO.	NIST SP 800-53 R4 AC-4 (21) NIST SP 800-53 R4 SC-2		A.12.1.4 A.14.2.9 A.9.1.1 8.1,partial, A.14.2.2 8.1,partial, A.14.2.3 8.1,partial, A.14.2.4
Infrastructure & Virtualization Security Segmentation	IVS-09	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed, and configured such that provider and customer (tenant) user access is appropriately segmented from other tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive user data, and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory, and regulatory compliance obligations	All customers (tenants) must access the EMCS Advanced Plus application tier using HTTPs (over port 443). At the application and data tier, customers (tenants) have separate instantiations of GIS infrastructure. Data isolation processes align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 AC-4 NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CA-3 (3) NIST SP 800-53 R4 CA-3 (5) NIST SP 800-53 R4 CA-9 NIST SP 800-53 R4 SC-2 NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (3) NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-7 (5) NIST SP 800-53 R4 SC-7 (7) NIST SP 800-53 R4 SC-7 (8) NIST SP 800-53 R4 SC-7 (12) NIST SP 800-53 R4 SC-7 (13) NIST SP 800-53 R4 SC-7 (18) NIST SP 800-53 R4 SC-39	45 CFR 164.308 (a)(4)(ii)(A)	A.13.1.3 A.9.4.1 A.18.1.4
Infrastructure & Virtualization Security VM Security - Data Protection	IVS-10	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	EMCS Advanced Plus administrators and customers alike, may only access EMCS Advanced Plus systems via HTTPS (utilizing the TLS protocol for encryption) over port 443.	NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CA-3 (3) NIST SP 800-53 R4 CA-3 (5)		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Infrastructure & Virtualization Security Hypervisor Hardening	IVS-11	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	All EMCS Advanced Plus administrators must authenticate to a bastion host in an encrypted session (TLS) using multi-factor authentication. EMCS Advanced Plus is a fully hardened network environment using Amazon security groups (firewalls) and monitored in real-time through an IDS and a 24/7 Security Operations Center. Furthermore, other security measures are present such as IP whitelisting for added assurance.	NIST SP 800-53 R4 AC-6 (5)		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)
Infrastructure & Virtualization Security Wireless Security	IVS-12	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	EMCS Advanced Plus may only be accessed over port 443 (using TLS) and data is therefore encrypted in transit. Robust firewall rules are implemented using Amazon security groups as part of existing network hardening procedures for EMCS Advanced Plus as documented in IVS-06 above. All customer data is encrypted at rest using AES-256. No wireless components exist within the boundary of EMCS. EMCS Advanced Plus is front-ended by a Web Application Firewall (WAF) and an Intrusion Detection System (IDS) is deployed. These components (in addition to log data) are monitored by a 24/7 Security Operations Center that performs real-time analysis to detect malicious activity.	NIST SP 800-53 R4 AC-1 NIST SP 800-53 R4 AC-18 NIST SP 800-53 R4 AC-18 (1) NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CA-3 (3) NIST SP 800-53 R4 CA-3 (5) NIST SP 800-53 R4 CM-6 NIST SP 800-53 R4 CM-6 (1) NIST SP 800-53 R4 PE-4 NIST SP 800-53 R4 RA-5 (8) NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (3) NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-7 (5) NIST SP 800-53 R4 SC-7 (7) NIST SP 800-53 R4 SC-7 (8) NIST SP 800-53 R4 SC-7 (12) NIST SP 800-53 R4 SC-7 (13) NIST SP 800-53 R4 SC-7 (18) NIST SP 800-53 R3 SI-7	45 CFR 164.312 (e)(1)(2)(ii) 45 CFR 164.308(a)(5)(ii)(D) 45 CFR 164.312(e)(1) 45 CFR 164.312(e)(2)(ii)	A.8.1.1 A.8.1.2 A.8.1.3 A.11.2.1 A.11.2.4 A.13.1.1 A.13.1.2 A.13.2.1 A.8.3.3 A.12.4.1 A.9.2.1, A.9.2.2 A.13.1.3 A.10.1.1 A.10.1.2
Infrastructure & Virtualization Security Network Architecture	IVS-13	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black- holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	EMCS Advanced Plus is front-ended by a Web Application Firewall (WAF) that aids in DDoS mitigation. Furthermore, an IDS is deployed throughout EMCS Advanced Plus to work in conjunction with the WAF to detect signature-based and anomaly-based ingress/egress traffic for malicious activity. Data flow and architectural diagrams are maintained and updated annually or whenever a significant change occurs to ensure accuracy as part of FedRAMP Moderate compliance.	NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CA-3 (3) NIST SP 800-53 R4 CA-3 (5) NIST SP 800-53 R4 CA-9 NIST SP 800-53 R4 RA-5 (8) NIST SP 800-53 R4 SI-4 (1)		

Interoperability & Portability APIs	IPY-01	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	EMCS implements Esri published APIs available at: http://server.arcgis.com/en/server/latest/administer/windows /scripting-with-the-arcgis-rest-api.htm			Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)

Interoperability & Portability Data Request	IPY-02	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry- standard format (e.g., .doc, .xls, .pdf, logs, and flat files).	EMCS Advanced Plus customers retain ownership of their data at all times.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Interoperability & Portability Policy & Legal	IPY-03	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Esri terms of service include these aspects for our customers.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Interoperability & Portability Standardized Network Protocols	IPY-04	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	EMCS uses TLS FIPS 140-2 compliant and authenticated sessions. Customers can refer to ArcGIS Server API documentation and AWS API Reference (http://docs.aws.amazon.com/AWSEC2/latest/APIReference /Welcome.html)			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Interoperability & Portability Virtualization	IPY-05	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	EMCS Advanced Plus uses Amazon Web Services (AWS) as an Infrastructure as a Service (IaaS) and AWS aligns with both FedRAMP Moderate and ISO 27001 standards. Refer to AWS virtual machine link below: http://aws.amazon.com/ec2/vm-import/			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Anti-Malware	MOS-01	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	EMCS Advanced Plus personnel are required to complete security awareness training that includes mobile device security as described in HRM-09 above.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)
Mobile Security Application Stores	MOS-02	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Customers are responsible for documented approved application stores for their mobile devices accessing EMCS Advanced Plus. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus systems or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Approved Applications	MOS-03	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Customers are responsible for managing unauthorized applications on their mobiles devices according to existing organizational policy. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus systems or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Approved Software for BYOD	MOS-04	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	While Esri does have a BYOD policy, EMCS Advanced Plus staff do not use mobile devices for accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Awareness and Training	MOS-05	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Esri has a BYOD policy that is posted internally and mobile security and acceptable use is part of the awareness training program described in HRM-09 above.	NIST SP 800-53 R4 MP-7		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Cloud Based Services	MOS-06	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Customers are responsible for managing mobile devices that will be accessing their application within EMCS Advanced Plus. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Compatibility	MOS-07	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Customers are responsible validating mobile device tests to validate compatibility with their GIS application within EMCS. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Device Eligibility	MOS-08	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	While Esri does have a BYOD policy, EMCS Advanced Plus staff do not use mobile devices for accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Mobile Security Device Inventory	MOS-09	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	While Esri does have a BYOD policy, EMCS Advanced Plus staff do not use mobile devices for accessing and storing customer data.	NIST SP 800-53 R4 MP-7 (1)		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Mobile Security Device Management	MOS-10	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2)

Mobile Security Encryption	MOS-11	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices, and shall be enforced through technology controls.	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.	NIST SP 800-53 R4 AC-19 (5)		Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Mobile Security Jailbreaking and Rooting	MOS-12	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)

Mobile Security Legal	MOS-13	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e- discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case that a wipe of the device is required.	Esri's BYOD policy aligns with these requirements and clearly states language surrounding expectation of privacy and lost devices. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Lockout Screen	MOS-14	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	All mobile devices (BYOD or company-owned) within Esri must have an automatic lockout screen which is enforced via agent-based MDM. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Operating Systems	MOS-15	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Esri has an established BYOD policy. EMCS Advanced Plus staff do not use mobile devices for accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Passwords	MOS-16	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	All mobile devices (BYOD or company-owned) within Esri must have an automatic lockout screen and meet password complexity requirements which is enforced via agent-based MDM. EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Mobile Security Policy	MOS-17	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Remote Wipe	MOS-18	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b)
Mobile Security Security Patches	MOS-19	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	EMCS Advanced Plus staff do not use mobile devices for administering EMCS Advanced Plus or accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Mobile Security Users	MOS-20	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	While Esri does have a BYOD policy, EMCS Advanced Plus staff do not use mobile devices for accessing and storing customer data.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Security Incident Management, E-Discovery, & Cloud Forensics Contact / Authority Maintenance	SEF-01	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	To align with FedRAMP Moderate requirements, points of contact for law enforcement and other authorities are maintained. As detailed in the Incident Response Plan (IRP) for EMCS Advanced Plus, IR communication and involvement beyond Esri and the EMCS ISSO may include: the customer, Amazon, Law enforcement, US-CERT and others as necessary.	NIST SP 800-53 R4 IR-6 NIST SP 800-53 R4 IR-6 (1) NIST SP 800-53 R4 IR-9 NIST SP 800-53 R4 IR-9 (1) NIST SP 800-53 R4 SI-5		A.6.1.3 A.6.1.4
Security Incident Management, E-Discovery, & Cloud Forensics Incident Management	SEF-02	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	EMCS Incident Response policies, procedures and processes align with FedRAMP Moderate requirements. Through a combination of procedural and technical elements, security- related events are tracked from the identification phase all the way until resolution.	NIST SP 800-53 R4 IR-1 NIST SP 800-53 R4 IR-2 NIST SP 800-53 R4 IR-3 NIST SP 800-53 R4 IR-4 NIST SP 800-53 R4 IR-4 (1) NIST SP 800-53 R4 IR-5 NIST SP 800-53 R4 IR-7 NIST SP 800-53 R4 IR-7 (1) NIST SP 800-53 R4 IR-7 (2) NIST SP 800-53 R4 IR-8 NIST SP 800-53 R4 IR-9 NIST SP 800-53 R4 IR-9 (1) NIST SP 800-53 R4 IR-9 (3)	45 CFR 164.308 (a)(1)(i) 45 CFR 164.308 (a)(6)(i)	Clause 5.3 (a), 5.3 (b), 7.5.3(b), 5.2 (c), 7.5.3(d), 8.1, 8.3, 9.2(g), Annex A.16.1.1 A.16.1.2
Security Incident Management, E-Discovery, & Cloud Forensics Incident Reporting	SEF-03	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	As part of alignment with FedRAMP Moderate requirements, EMCS Advanced Plus personnel are required to report suspected security incidents to the organizational incident response capability within timelines recommended by US-CERT specified in NIST SP 800-61 (as amended).	NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 IR-2 NIST SP 800-53 R4 IR-6 NIST SP 800-53 R4 IR-6 (1) NIST SP 800-53 R4 IR-7 NIST SP 800-53 R4 IR-7 (1) NIST SP 800-53 R4 IR-7 (2) NIST SP 800-53 R4 IR-9 NIST SP 800-53 R4 IR-9 (1) NIST SP 800-53 R4 SI-4 NIST SP 800-53 R4 SI-4 (2) NIST SP 800-53 R4 SI-4 (4) NIST SP 800-53 R4 SI-4 (5) NIST SP 800-53 R4 SI-5	45 CFR 164.312 (a)(6)(ii) 16 CFR 318.3 (a) 16 CFR 318.5 (a) 45 CFR 160.410 (a)(1)	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Legal Preparation	SEF-04	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	EMCS Advanced Plus has a specific communication plan depending on the nature of the incident to ensure proper legal precautions are taken and chain of custody is maintained throughout an incident. The Incident Response (IR) plan, policies and procedures align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 AU-6 NIST SP 800-53 R4 AU-6 (1) NIST SP 800-53 R4 AU-6 (3) NIST SP 800-53 R4 AU-7 NIST SP 800-53 R4 AU-7 (1) NIST SP 800-53 R4 AU-9 NIST SP 800-53 R4 AU-9 (2) NIST SP 800-53 R4 AU-11 NIST SP 800-53 R4 IR-5 NIST SP 800-53 R4 IR-9 NIST SP 800-53 R4 IR-9 (3) NIST SP 800-53 R4 MP-5 NIST SP 800-53 R4 MP-5 (4) NIST SP 800-53 R4 SI-7	45 CFR 164.308 (a)(6)(ii)	Clause 5.2 (c), 5.3 (a), 5.3 (b), 7.2(a), 7.2(b), 7.2(c), 7.2(d), 7.3(b), 7.3(c) 7.5.3(b), 7.5.3(d), 8.1, 8.3, 9.2(g)
Security Incident Management, E-Discovery, & Cloud Forensics Incident Response Metrics	SEF-05	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	All security incidents are tracked from detection through resolution within existing systems as well as incorporate lessons learned to aid in future prevention. These processes align with FedRAMP Moderate requirements.	NIST SP 800-53 R4 IR-4 NIST SP 800-53 R4 IR-4 (1) NIST SP 800-53 R4 IR-5 NIST SP 800-53 R4 IR-8 NIST SP 800-53 R4 IR-9 NIST SP 800-53 R4 IR-9 (3) NIST SP 800-53 R4 SI-7 (7)	45 CFR 164.308 (a)(1)(ii)(D)	A.16.1.6
Supply Chain Management, Transparency, and Accountability Data Quality and Integrity	STA-01	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least- privilege access for all personnel within their supply chain.	As part of FedRAMP Moderate requirements, Esri maintains a System and Services Acquisition policy for managing risks from acquired information systems or services. Authorized EMCS Advanced Plus personnel actively work with cloud vendors and supply chain partners to address issues related to quality, error, and risk. This ensures security best practices (including separation of duties, principle of least-privilege and role based access control) are implemented with regards to enterprise procurement of information systems and services.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c) 6.1.2(c)(1), 6.1.2(c)(2) 6.1.2(d)
Supply Chain Management, Transparency, and Accountability Incident Reporting	STA-02	The provider shall make security incident information available to all affected customers and providers periodically through electronic methods (e.g., portals).	EMCS Advanced Plus customers can provide a point of contact for reporting security related issues. Esri does post security incident and security related-information for products on trust.arcgis.com.			Clause 6.1.1, 6.1.1(e)(2) 6.1.2 6.1.2(a)(1) 6.1.2(a)(2), 6.1.2(b) 6.1.2 (c)
Supply Chain Management, Transparency, and Accountability Network / Infrastructure Services	STA-03	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	EMCS Advanced Plus uses Commercial-off-the-shelf (COTS) components that are deployed according to vendor best practices to ensure functional and security requirements are met. EMCS Advanced Plus is a fully redundant system configured in an active-active configuration across two (2) separate AWS availability zones. In the event a primary instance fails, the second instance will automatically take on the additional load. This is transparent to end users. There may be some ArcGIS Enterprise Extensions that deviate from the standard Active-Active configuration. In these cases, customers are required to approve this exception. The entire EMCS is monitored in real-time to ensure maximum service and meet capacity requirements as detailed in IVS-04 above.	NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 CP-6 NIST SP 800-53 R4 CP-6 (1) NIST SP 800-53 R4 CP-6 (3) NIST SP 800-53 R4 CP-7 NIST SP 800-53 R4 CP-7 (1) NIST SP 800-53 R4 CP-7 (2) NIST SP 800-53 R4 CP-7 (3) NIST SP 800-53 R4 CP-8 NIST SP 800-53 R4 CP-8 (1) NIST SP 800-53 R4 CP-8 (2) NIST SP 800-53 R4 SA-4 (9) NIST SP 800-53 R4 SA-9 NIST SP 800-53 R4 SA-9 (1)		A.15.1.2 A.13.1.2

Supply Chain Management, Transparency, and Accountability Provider Internal Assessments	STA-04	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	As part of FedRAMP Moderate requirements, an accredited FedRAMP third party assessment organization (3PAO) performs an annual audit that includes a full review across the entire set of security controls, vulnerability assessments across web application, network, system and database as well as a penetration testing.
			
			Furthermore, internal vulnerability assessments are performed monthly and continuous monitoring of security controls occurs to ensure constant compliance.
						Clause
						6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)
						6.1.2(d)(1) 6.1.2(d)(2)
						6.1.2(d)(3)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Supply Chain Management, Transparency, and Accountability Supply Chain Agreements	STA-05	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry- acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization	Esri employs a System and Services Acquisition Policy for EMCS Advanced Plus that includes but is not limited to the provisions listed.	NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 MP-5 NIST SP 800-53 R4 MP-5 (4) NIST SP 800-53 R4 PS-7 NIST SP 800-53 R4 SA-9 NIST SP 800-53 R4 SA-9 (1) NIST SP 800-53 R4 SA-9 (4) NIST SP 800-53 R4 SA-9 (5)	45 CFR 164.308 (a)(4)(ii)(A) 45 CFR 164.308 (b)(1) 45 CFR 164.308 (b)(2)(i) 45 CFR 164.308 (b)(2)(ii) 45 CFR 164.308 (b)(2)(iii) 45 CFR 164.308 (b)(3) 45 CFR 164.308 (b)(4) 45 CFR 164.312(e)(2)(i) 45 CFR 164.312 (c)(1) 45 CFR 164.312(e)(2)(ii) 45 CFR 164.314 (a)(1)(i) 45 CFR 164.314 (a)(1)(ii)(A) 45 CFR 164.314 (a)(2)(i) 45 CFR 164.314 (a)(2)(i)(A) 45 CFR 164.314 (a)(2)(i)(B) 45 CFR 164.314 (a)(2)(i)(C) 45 CFR 164.314 (a)(2)(i)(D) 45 CFR 164.314 (a)(2)(ii)(A) 45 CFR 164.314 (a)(2)(ii)(A)(1) 45 CFR 164.314 (a)(2)(ii)(A)(2) 45 CFR 164.314 (a)(2)(ii)(B) 45 CFR 164.314 (a)(2)(ii)(C) 45 CFR 164.314 (b)(1) 45 CFR 164.314 (b)(2)	A.15.1.2, 8.1* partial, A.13.2.2, A.9.4.1 A.10.1.1

Supply Chain Management, Transparency, and Accountability Supply Chain Governance Reviews	STA-06	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Security requirements for third party partners are documented and providers must comply with organizational information security requirements and employ appropriate security controls.			Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)

Supply Chain Management, Transparency, and Accountability Supply Chain Metrics	STA-07	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall be performed at least annually and identify any non- conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	SLAs for EMCS Advanced Plus are reviewed annually and disparities addressed as necessary.			Clause
						6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)
						6.1.2(d)(1) 6.1.2(d)(2)

Supply Chain Management, Transparency, and Accountability Third Party Assessment	STA-08	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	Security requirements for third party providers are documented and providers must comply with organizational information security requirements and employ appropriate security controls.
			
			SLAs for EMCS Advanced Plus are reviewed annually and disparities addressed as necessary.
						Clause 6.1.1,
						6.1.1(e)(2)
						6.1.2
						6.1.2(a)(1)
						6.1.2(a)(2),
						6.1.2(b)
						6.1.2 (c) 6.1.2(c)(1),
						6.1.2(c)(2) 6.1.2(d)
						6.1.2(d)(1) 6.1.2(d)(2)

Control Domain	CCM V3.0 Control ID	Updated Control Specification	ECMS Advanced Plus Answers	Scope Applicability		
				FedRAMP Rev 4 Baseline --MODERATE IMPACT LEVEL--	HIPAA	ISO/IEC 27001:2013
Supply Chain Management, Transparency, and Accountability Third Party Audits	STA-09	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	EMCS Advanced Plus third-party providers are required to demonstrate compliance with baseline FedRAMP security controls. EMCS Advanced Plus leverages Cloud Service Providers (CSP) that are FedRAMP Moderate compliant and as such undergo annual assessments from an accredited third party assessment organization (3PAO) to maintain compliance.	NIST SP 800-53 R4 CA-3 NIST SP 800-53 R4 SA-9 NIST SP 800-53 R4 SA-9 (1) NIST SP 800-53 R4 SC-7 NIST SP 800-53 R4 SC-7 (3) NIST SP 800-53 R4 SC-7 (4) NIST SP 800-53 R4 SC-7 (5) NIST SP 800-53 R4 SC-7 (7) NIST SP 800-53 R4 SC-7 (8) NIST SP 800-53 R4 SC-7 (12) NIST SP 800-53 R4 SC-7 (13) NIST SP 800-53 R4 SC-7 (18)	45 CFR 164.308(b)(1) 45 CFR 164.308 (b)(4)	A.15.1.2 8.1* partial, 8.1* partial, A.15.2.1 A.13.1.2
Threat and Vulnerability Management Anti-Virus / Malicious Software	TVM-01	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	In alignment with FedRAMP Moderate requirements, EMCS ensures malware-protection is deployed on all end points including but not limited to: workstations, laptops, servers, database servers. Furthermore, EMCS Advanced Plus infrastructure is monitored by an Intrusion Detection System (IDS) to continuously monitor for signature and anomaly based attacks. A 24/7 Security Operations Center is monitoring these inputs in real- time and potential threat events are immediately communicated.	NIST SP 800-53 R4 AC-6 (10) NIST SP 800-53 R4 RA-5 (5) NIST SP 800-53 R4 RA-5 (8) NIST SP 800-53 R4 SC-5 NIST SP 800-53 R4 SI-3 NIST SP 800-53 R4 SI-3 (1) NIST SP 800-53 R4 SI-3 (2) NIST SP 800-53 R4 SI-5 NIST SP 800-53 R4 SI-7 NIST SP 800-53 R4 SI-7 (1) NIST SP 800-53 R4 SI-8	45 CFR 164.308 (a)(5)(ii)(B)	A.12.2.1
Threat and Vulnerability Management Vulnerability / Patch Management	TVM-02	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally- owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs customer (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	As part of FedRAMP Continuous Monitoring requirements, internal vulnerability assessments across web application interfaces and systems. Annual vulnerability assessments and penetration tests occur and are conducted by an accredited FedRAMP third party assessment organization (3PAO) in order to maintain FedRAMP Compliance. Any changes to systems occur through existing EMCS Advanced Plus change control processes that align with FedRAMP Moderate requirements. Patches and security fixes are fully tested in a staging environment prior to deployment on production systems. These are implemented in a timely manner to meet established FedRAMP moderate timelines for flaw remediation.	NIST SP 800-53 R4 CA-8 NIST SP 800-53 R4 CM-3 NIST SP 800-53 R4 CM-4 NIST SP 800-53 R4 RA-5 NIST SP 800-53 R4 RA-5 (1) NIST SP 800-53 R4 RA-5 (2) NIST SP 800-53 R4 RA-5 (3) NIST SP 800-53 R4 RA-5 (5) NIST SP 800-53 R4 RA-5 (6) NIST SP 800-53 R4 SA-11 (2) NIST SP 800-53 R4 SI-1 NIST SP 800-53 R4 SI-2 NIST SP 800-53 R4 SI-2 (2) NIST SP 800-53 R4 SI-2 (3) NIST SP 800-53 R4 SI-4 NIST SP 800-53 R4 SI-5 NIST SP 800-53 R4 SI-7 (7)	45 CFR 164.308 (a)(1)(i)(ii)(A) 45 CFR 164.308 (a)(1)(i)(ii)(B) 45 CFR 164.308 (a)(5)(i)(ii)(B)	8.1*partial, A.14.2.2, 8.1*partial, A.14.2.3 A.12.6.1
Threat and Vulnerability Management Mobile Code	TVM-03	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	All applications are administered by EMCS Advanced Plus personnel that must authenticate using multi-factor authentication. A Web Application Firewall (WAF) front-ends instances where mobile code is present and can provide immediate protection against common attack vectors such as SQL injection and Cross Site Scripting (XSS). The WAF works in conjunction with the Intrusion Detection System (IDS) to monitor for signature and anomaly based attacks through a 24/7 Security Operations Center (SOC). Customers may choose to build mobile web applications and will be responsible for providing implementation guidance for their developers to abide by secure coding best practices.	NIST SP 800-53 R4 CA-9 NIST SP 800-53 R4 RA-5 (5)		A.12.2.1