VIRGINIA IT AGENCY

Commonwealth of Virginia

Enterprise Architecture Standard (EA-225)

Enterprise Technical Architecture [ETA]

vita.virginia.gov

February 15, 2023

Revision History

Enterprise Technical Architecture (ETA) Requirements: Version History		
Revision	**Date**	**Description**
1.0	07-10-2006	Initial document created
2.0	02-15-2023	Complete rewrite

Review Process
This requirements document was posted on VITA's Online Review and Comment Application (ORCA). All agencies, stakeholders, and the public were encouraged to provide their comments through ORCA. All comments were evaluated, and individual commenters were notified of action(s) taken.

Requirements and Agency Exceptions
The requirements included within this document are mandatory. Agencies deviating from these requirements must request an exception for each desired deviation, and receive an approved *Enterprise Architecture Exception* via Archer, prior to developing, procuring, or deploying such technology, or not complying with a requirement specified in this document. The instructions for completing and submitting an exception request are contained within the *Commonwealth Enterprise Architecture Policy*.

Glossary
As appropriate, terms and definitions used in this document are in the COV ITRM IT Glossary. The COV ITRM IT Glossary is available on the VITA website: https://www.vita.virginia.gov/it-governance/glossary/cov-itrm-glossary/

Contents

Enterprise Technical Architecture (ETA) 4
Purpose 5
Authority 5
Scope 6
Business 6
COV Technology Roadmaps 6
Technology Roadmap Requirements 8
Other Business Requirements 10
Design/Architecture 10
Availability/ Performance 12
Capacity 13
Continuity 13
Integration/Interoperability 14
Technology 14
Security 16
Definitions and Terminology 17

Enterprise Technical Architecture (ETA)

Enterprise architecture (EA) provides direction, recommendations, and requirements for supporting the business, information, solution, technical, and security architectures of an organization. Each architecture consists of supporting strategies, policies, requirements, briefs, and roadmaps where applicable.

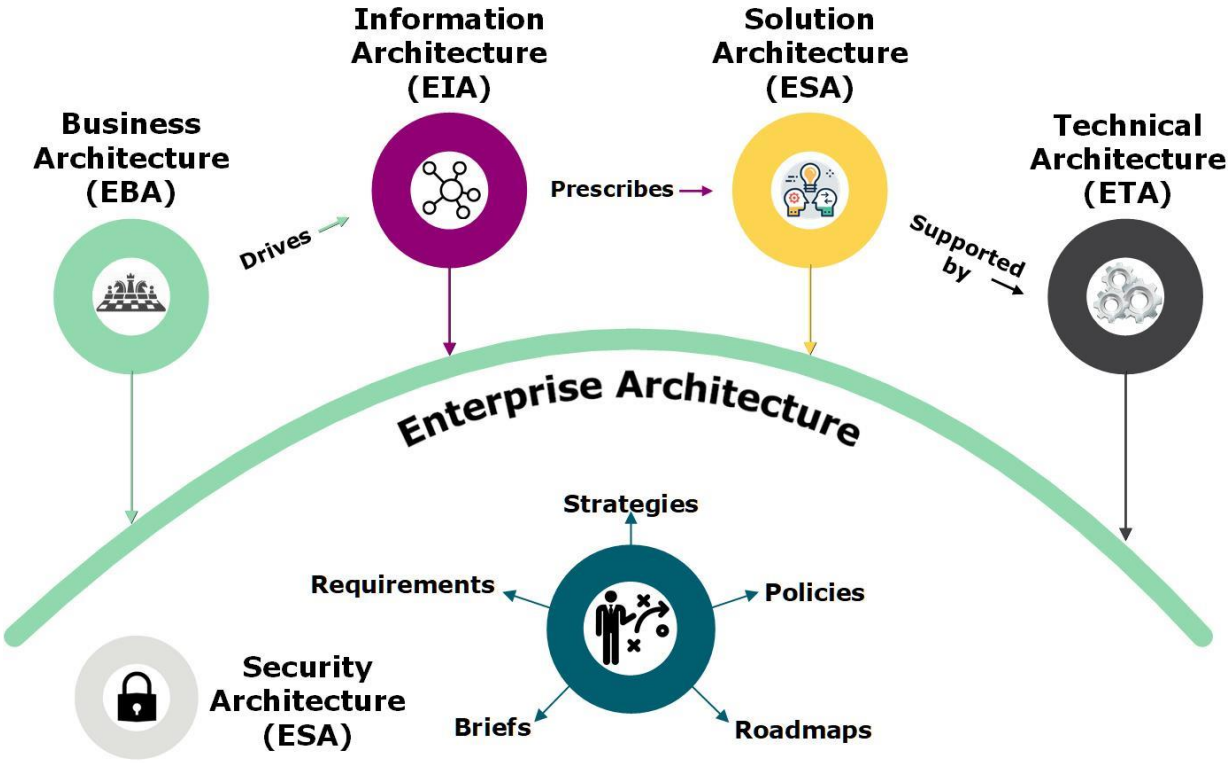

Figure 1: EA Main Model

All of these ETA documents can be referenced from the: Enterprise Architecture Standard (EA225) and Enterprise Architecture web pages.

Enterprise Technical Architecture (ETA) Vision and Strategy
Vision
COV will utilize best-of-breed technologies that integrate into a toolset that supports the hosting, development, and support for the IT solutions that enable COV employees to perform the business of the commonwealth effectively.
Strategy
In order to achieve this vision, COV technologies shall be current and fully supported. This will enable COV IT solutions and services to be secure, scalable, available, reliable, maintainable, robust, stable, portable, interoperable, supportable, testable, and usable. **Objective 1: Technology Currency** The versions of COV technologies used to support COV IT services will be current and fully supported The versions of COV technologies consumed by agencies to support and deploy their IT solutions will be current and fully supported. **Objective 2: Technology Choices** Agencies will have choices for COV approved technologies The number of choices for COV approved technologies will be governed in order to reduce risk and complexity

Purpose

The intent of these requirements is to guide the purchase, design, implementation, and on-going operation of the COV technologies used to provide, host, support, manage, monitor, or develop:

- COV IT services
- COV IT solutions that store, process, and/or transmit Commonwealth data

Authority

- Code of Virginia, §2.2-2007. Powers of the CIO
- Code of Virginia, §2.2-2007.1. Additional duties of the CIO relating to information technology planning and budgeting
- Code of Virginia, §2.2-2009(A). Additional duties of the CIO relating to security of government information
- Code of Virginia, §2.2-2012(A). Additional powers and duties related to the procurement of information technology

Scope

This standard is applicable to all Executive Branch state agencies (hereinafter collectively referred to as "agencies") that are responsible for the management, development, purchase and use of information technology resources in the Commonwealth of Virginia. This standard does not apply to research projects, research initiatives, or instructional programs at public institutions of higher education.

ETA requirements apply to all COV technologies. COV technology roadmaps apply to all COV technologies included within those roadmaps located at: COV Technology Roadmaps.

In addition to the requirements below all COV IT technologies shall comply with the standards found on the VITA Policies Standards & Guidelines page.

There are eight perspectives in this document.

Business

COV Technology Roadmaps

COV Technology Classifications	
Approved	*Approved* technologies/solutions are available for current and future deployments because they have been evaluated, and where applicable, support is in place to keep them secure and updated.
Emerging	*Emerging* technologies/solutions are those of interest to an agency or supplier, in order to meet current or future, and technical or business Commonwealth needs, but are unapproved. *Emerging* technologies/solutions are not ready for deployment, because they lack essential factors, such as hardening templates, service packs, support, or Commonwealth domain expertise. *Emerging* "Pilot" technologies/solutions are eligible for controlled and limited evaluation. Note: Agencies who choose to use *Emerging* technologies/solutions beyond the scope of the definition must submit an Enterprise Architecture (EA) exception that is subsequently approved, prior to use. The following provides a couple examples to help with understanding context and intent: 1) For example, with products that engage long-term lifecycle updates (e.g., Microsoft, Red Hat, Oracle, et.al.) and where suppliers and agencies are not ready to support the product when it initially appears under general availability (GA), because of hardening template creation, staff training, gold-image building, etc.; a supplier and agency would enter an EA exception request. Once that exception request is approved, they could proceed with getting the bulk of their testing/validation processes completed on the major version, rather than waiting until the software version update is *Approved* first, and then working on testing/validation for software implementation and use. Then when the first service pack is available, the supplier and agency would have minimal additional testing prior to completion and deployment of the large update. This would help to shorten the products time-to implementation once it became *Approved*. 2) And for products that engage short-term lifecycles (more frequent updates) suppliers and agencies desiring to move forward with proactive version testing of software already deployed in the enterprise, in anticipation of that software version update most likely being *Approved*, would enter an EA exception request. Once approved, they could proceed with their testing/validation processes, rather than waiting until the software version update is *Approved* first, and then working on testing/validation for software implementation and use. This would also help to shorten the software's time-to-implementation once it became *Approved*.

Projected	Projected technologies/solutions are predicted future versions of currently *Approved* technologies/solutions based on a pattern of previous releases. Note: *Projected* dates will be estimates based on best-available information at the time.
Divest	*Divest* technologies/solutions are no longer approved. Agencies and suppliers of COV IT services shall not make any procurements or additional deployments of *Divest* technologies/solutions. There are two phases within *Divest*:
Plan	In the *Divest*: *Plan* phase, agencies must develop and submit their plan to migrate off of these technologies/solutions within their IT Strategic Plan. The plans must result in the migration off *Divest* technologies/solutions before they become *Prohibited*.
Execution	In the *Divest: Execution* phase, agencies and suppliers of COV IT services must execute their migration plans for these technologies/solutions. For agencies, execution may include performing the following entries in their IT Strategic Plans: • CIO approved IBC (Investment Business Case) and IBC Addendum for projects and supporting BreTs (Business Requirements for Existing Technology) • Inclusion of any needed procurements These migrations must be completed before the technologies become *Prohibited*.
Prohibited	Agencies and suppliers of COV IT services shall not use *Prohibited* technologies/solutions without an approved EA Exception because they are no longer supported by the Commonwealth. *Prohibited* technologies/solutions represent substantial risk. Agencies and suppliers of COV IT services shall execute their migration plans for these technologies/solutions and report to EA on their progress in accordance with Project Management Division (PMD) requirements. Any agency use of *Prohibited* technologies must be mitigated by adding the following to their IT Strategic Plan: • Migration plans • CIO approved IBC (Investment Business Case) and IBC Addendum for projects and supporting BreTs • Inclusion of any needed procurements
Skipped	Skipped technologies/solutions means they will be *Skipped*. *Skipped* versions are not considered when establishing N or N-1.
Vendor End of support	Agencies and suppliers of COV IT services shall not use technologies/solutions beyond their end of support date without an approved EA Exception. For IT software, support is defined as a minimum of having available and deployable security patching.

COV Technology Roadmaps can be found at COV Technology Roadmaps. If you would like a software product added to the roadmaps, please send your request to ea@vita.virginia.gov.

Enterprise Architecture (EA) Exceptions can be requested using Archer:
https://itgrcs.vita.virginia.gov/apps/ArcherApp/Home.aspx

Technology Roadmap Requirements

Approved

ETA-01 Agencies shall only use *Approved* versions of the technologies covered within the COV Technology Roadmaps for any new IT deployments.

ETA-02 Suppliers of COV IT services and technologies shall only use *Approved* versions of the technologies covered within the COV Technology Roadmaps.

ETA-03 For technologies that are not covered within COV Technology Roadmaps:

- Agencies shall only use versions or models of IT technology that are current (N and N-1) and have vendor or equivalent support for any new IT deployments.
- Suppliers of COV IT services shall only use versions or models of IT technology that are current (N and N-1) and have vendor or equivalent support.

Note 1: support is defined as a minimum of having available and deployable security patching for IT software

Note 2: it is not allowed to utilize an IT solution or technology that requires an unsupported or N-2 or older technology to work.

Example: an IT management utility that only works with a EOL database or N-2 operating system

Note 3: many N and N-1 versions are defined in the COV Technology Roadmaps

Emerging

ETA-04 Agencies and suppliers of COV IT services and technologies shall only use *Emerging* versions of the technologies covered within the COV Technology Roadmaps for non-production pilots, evaluation, and testing. Agencies shall report on any lessons learned using *Emerging* technologies to ea@vita.virginia.gov.

ETA-05 *Emerging* technologies shall only be used for pilots if the related service is in a service portfolio and lifecycle management (SPLM) phase that allows pilots and there is an approved EA exception.

Projected

ETA-06 Agencies and suppliers of COV IT services and technologies shall not use beta or early pre-release versions of the technologies covered within the COV Technology Roadmaps.

Note: If agencies need to use beta or pre-release version of software, they will need to apply for an EA exception via Archer.

Divest

ETA-07 Agencies and suppliers of COV IT services and technologies shall not make any procurements or additional deployments of *Divest* versions of the technologies covered within the COV Technology Roadmaps.

ETA-08 Agencies and suppliers of COV IT services and technologies shall not make any procurements or additional deployments of N-2 or older versions of the technologies not covered within the COV Technology Roadmaps.

Divest: Plan

ETA-09 Agencies shall develop and submit their plan to migrate off any *Divest: Plan* and N-2 and older technologies within their agency IT Strategic Plan.

ETA-10 Suppliers of COV IT services and technologies shall report on their plan to migrate off any *Divest: Plan* and N-2 or older technologies within their Annual Technology Plan and Refresh and Technical Currency Report.

Divest: Execution

ETA-11 Agencies and suppliers of COV IT services and technologies shall execute their migration plans for any *Divest: Execution* technologies.

Note: These migrations must be completed before the technologies become *Prohibited*

ETA-12 Agencies shall add the following entries in their IT Strategic Plans as required by COV ITRM Policies and Standards for any use of *Divest: Execution technologies*:

- CIO approved IBC (Investment Business Case) and IBC Addendum for projects and supporting BreTs (Business Requirements for Existing Technology)
  - Inclusion of any needed procurements

Prohibited

ETA-13 Agencies and suppliers of COV IT services and technologies shall not use *Prohibited* technologies or *Prohibited* versions of the technologies covered within the COV Technology Roadmaps.

Skipped

ETA-14 Agencies and suppliers of COV IT services and technologies shall not use *Skipped* versions of the technologies covered by the COV Technology Roadmaps.

Vendor End of support

ETA-15 Agencies and suppliers of COV IT services and technologies shall only use technologies and versions of technologies that have vendor support. This shall include current available and deployable patching at a minimum.

Other Business Requirements

ETA-16 No devices shall be deployed as part of supplier services that are only available utilizing that supplier's service contract with COV.

Note: If the COV contract ends, the COV must have a way of procuring and supporting the devices that were deployed under the supplier contract

ETA-17 COV technologies/devices shall have all warranty work performed by appropriate parties as defined in the Service Management Manuals (SMM).

ETA-18 In the event of a major problem or incident, Suppliers of COV technologies shall provide additional resources upon request by VITA or the MSI.

Note: Additional resources can include personnel, devices, after hours availability, etc.

ETA-19 All COV technologies, IT solutions and services as well as everything supporting those COV technologies, IT solutions, and services shall comply with VITA Rules.

Note: This includes processes, IT solutions, technologies, devices, personnel, etc.

Design/Architecture

These requirements relate to overall architecture characteristics.

ETA-20 All new COV technologies utilized by IT service suppliers or provided to COV customers shall appear on the supplier's high-level service model diagram. This diagram shall include all technology and service components.

Note: This applies to technology components not specific devices (Servers vs. a particular Dell model)

ETA-21 All new and changes to COV technologies shall be documented at three levels within an Architecture Overview Document (AOD):

- High-level section (HL) - required to be approved prior to starting the project to build the architecture
- Detailed Design section (DD) - contains the information needed to build or rebuild the system and needs to be completed prior to service going live. It contains not only the system configuration, but also the configurations from any other suppliers that they need to do to bring your system online.
- As built (AB) - contains any variances from the Detailed Design and their configurations. It needs to be completed prior to project closeout

Note: The three levels may be within separate sections of the same AOD

ETA-22 All technology components used by a service supplier or provided to COV customers shall indicate the AOD where that technology component is documented within the supplier's high-level service model diagram.

ETA-23 All new and changes to COV technologies shall go through a formal VITA approved architecture review process utilizing a template for high-level, detail-level, and as-built designs. The designs need to cover the following architectural viewpoints:

- **Context** – describes the relationships, dependencies, and interactions between the system and its environment (the people, systems, and external entities with which it interacts)
- **Functional** – describes the system's runtime elements, their responsibilities, interfaces, and primary interactions
- **Information** – describes the way that the architecture stores, manipulates, manages, and distributes information
- **Concurrency** – describes the concurrency structure of the system and maps functional elements to concurrency units to clearly identify the parts of the system that can execute concurrently and how this is coordinated and controlled
- **Development** – describes the architecture that supports the software development process
- **Deployment** – describes the environment into which the system will be deployed and the dependencies that the system has on elements of it
- **Operational** – describes how the system will be operated, administered, and supported when it is running in its production environment

The following architectural perspectives cut across all the above views:

- **Security** – the ability of the system to reliably control, monitor, and audit who can perform what actions on which resources and the ability to detect and recover from security breaches
- **Performance and Scalability** – the ability of the system to predictably execute within its mandated performance role and to handle increased processing volumes in the future if required
- **Availability and Resilience** – the ability of the system to be fully or partly operational as and when required and to effectively handle failures that could affect system availability
- **Accessibility** – the ability of the system to be used by people with disabilities
- **Development Resource** – the ability of the system to be designed, built, deployed, and operated within known constraints related to people, budget, time, and materials
- **Usability** – the ease with which people who interact with the system can work effectively
- **Regulation** – the ability of the system to conform to local and international laws, quasi-legal regulations, policies, and other rules and standards
- **Evolution** – the ability to be flexible in the face of the inevitable change that all systems experience after deployment, balanced against the costs of providing such flexibility

Reference: Viewpoints, perspectives, and their definitions are from, *Software Systems Architecture,* 2nd Edition, Nick Rozanski and Eoin Woods

ETA-24 COV technologies shall support and utilize a minimum of 64-bit architecture operating systems.

ETA-25 COV approved naming conventions shall be used for all deployed devices/technologies.

ETA-26 VITA shall maintain a repository for device naming convention documents.

Availability/ Performance

Availability relates to any stop actions that are planned or unplanned. An unplanned action example is equipment failure. A planned action is system maintenance.

Performance relates to a systems responsiveness to execute an action within a given time interval – it is a quality metric.

ETA-27 Agencies shall define performance and availability requirements for the COV technologies that they consume.

Note: These requirements shall be provided to VITA upon request

Example: Performance metric examples include average transaction counts/rates, transaction peaks, latency, etc.

ETA-28 COV IT technologies shall have recommended configuration settings that meet the documented performance and availability requirements.

Note: The system design document for technologies and services should detail how the solution meets these requirements

ETA-29 Suppliers of COV technologies shall monitor and report quarterly on all aspects of device performance including appropriate real-time and analysis of historical performance data.

ETA-30 COV technologies and devices shall have defined expected and quarterly measured Mean Time Between Failure (MTBF) metrics.

ETA-31 Suppliers of COV on-premise technology/devices shall perform or obtain proactive failure trend analysis and report on the when the predicted MTBF increases from the expected.

ETA-32 COV technologies shall be tested for performance against COV documented requirements prior to the technology being deployed, annually, and on request. Results of the analysis and any recommendations shall be reported to COV.

ETA-33 COV devices shall be tested and be determined to be free of defects prior to deployment.

ETA-34 COV technologies/devices that support services and IT solutions that require high availability shall be connected to maintained Uninterruptable Power Supplies (UPS) or have internal batteries capable of providing stand-by power to operate with full functionality for at least 3 hours.[1]

Note: Maintained can cover: UPS system maintenance agreements with defined response times and care levels; preventative maintenance; on-site service; repair depot service; battery replacement programs

ETA-35 COV technologies deployed along the path between the end-user and the IT solutions they are accessing shall have approved performance metrics and those metrics shall be monitored and reported on VITA accessible dashboards.

Note: Examples of performance related data are path counts, transmission times, and issue counts

[1] Per U.S. Energy Information Administration, the average power outage not associated with major events is less than 2 hours

Capacity

These requirements relate to such capacity areas as upgrades, tuning, and monitoring. Capacity is concerned with meeting both current and future capacity, and the performance needs of the IT infrastructure.

ETA-36 VITA shall establish and publish capacity thresholds for all COV technologies.

Note 1: These thresholds shall be based on doubling how long it takes to obtain additional capacity

Note 2: VITA will determine where the thresholds will be published within six months of the publication of this standard

ETA-37 Initial capacity for a technology shall be provided based on a model tied to measurable quantities.

Examples: Number of users, amount of data sent and received, amount of storage, etc.

ETA-38 Suppliers of COV technologies shall monitor, track, and perform trend analysis on the capacity of COV technologies against the established documented thresholds.

ETA-39 Exceeding a capacity threshold shall result in the ordering of additional capacity, a redesign, or reconfiguration unless otherwise approved by COV.

Continuity

These requirements relate to IT infrastructure components and resources (internal and external) such as facilities, equipment, systems, applications, data, and networks that are required to restore minimum acceptable service levels during an event, incident, or disaster.

Note: IT Information Security Standard (SEC501) addresses the requirements for the recovery of COV IT systems and data that support COV mission essential functions as determined in the agency's Business Impact Analysis. Moreover, the Virginia Department of Emergency Management (VDEM) defines COV continuity planning requirements.

ETA-40 Suppliers of COV technologies shall recommend service recovery point objectives (RPO) and recovery time objectives (RTO) for COV to review and approve.

ETA-41 COV technologies shall meet designed, configured, and deployed defined service recovery point objectives (RPO) and recovery time objectives (RTO).

ETA-42 Suppliers of COV technologies shall implement a spare parts strategy to meet approved RTO.

ETA-43 A Complex Event shall be declared when any technology supporting Mission Critical services and IT solutions is unavailable for 8 hours.

ETA-44 If a Complex Event occurs and the expectation is that the technology supporting a highly available Enterprise Service will not be fully reestablished for 24 hours or more beyond the approved RTO and RPO, then the incident shall be referred to Commonwealth CIO for consideration of being declared a disaster.

ETA-45 Any technologies supporting Mission Critical services and IT solutions shall estimate the RTOs and RPOs should a Complex Event occur. Those estimates shall be included within the system design documentation for that technology as follows:

Complex Event		
Percentage of service restored	Hours needed to achieve	
	RTO	RPO
50%		
75%		
90%		
100%		

Integration/Interoperability

Enterprise integration deals with multiple applications running on multiple platforms in differing locations. Integration architectures and platforms enable digital business by connecting applications, processes, APIs, and data.

ETA-46 COV Technologies capable of data exchange shall have those interfaces documented (i.e. APIs, web services).

Technology

ETA-47 All COV technologies shall have a documented lifecycle including information on currency, general availability, and support (end of service life and end of support).

Note: See COV Technology Roadmaps for more information

ETA-48 COV Technology roadmaps shall not only document the lifecycle of a product but also the planned migration from one product to another within a technology classification.

ETA-49 Agencies and Suppliers of COV IT Services and technologies shall document all versions of software technologies that their IT Solutions consume. This includes all software that the agencies and service providers use to host, develop, support, test, and deploy their IT solutions (operating systems, languages, databases, editors, etc.)

Note 1: This documentation will be entered into a COV repository in the future

Note 2: This requirement does not apply to SaaS (addressed by ECOS process)

ETA-50 Agencies shall create and maintain a technology currency roadmap indicating when they will update software versions to maintain currency and support.

ETA-51 All COV technologies shall have an easy and authoritative way (linked references) to determine the software version, firmware version, currency (N, N-1), end of service life date (EOSLD), and end of life date (EOLD). Reference links for that information shall be provided within the Architecture Overview Documents (AOD).

ETA-52 All non-security related IT technology components, devices, and supporting software (physical and virtual) shall have patches applied to systems to an n-1 patch level within 90 days of a patch release. (e.g., operating system security patches, performance patches, firmware, service packs).

ETA-53 Agencies and suppliers of COV IT services shall only use IT hardware whose firmware is current, stable, and has vendor support.

Note: Securing the firmware layer is often overlooked, but is a single point of failure in devices, and is one of the stealthiest methods in which an attacker can compromise devices at scale. Over the past few years, hackers have increasingly targeted firmware to launch devastating attacks." – U.S. Dept. of Commerce and Homeland Security, 24 Feb 2022

ETA-54 Authenticated update mechanisms shall ensure that BIOS update images have been digitally signed and that the digital signature can be verified using a key stored or verified by the RTU before updating the BIOS.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-147B.pdf

ETA-55 The COV working with the suppliers shall provide and maintain a testing lab where devices, technologies and integration between services can be tested.

Note: The agencies shall be able to use the lab to test their applications for use with new technologies and devices

ETA-56 Suppliers of COV technologies shall provide and utilize an automated regression test tool/bed.

ETA-57 Suppliers of COV IT Services and technologies shall provide and utilize hardware from more than one manufacturer for each category of COV IT devices (switch, PCs, phones, servers).

Note: Utilizing hardware from more than one manufacturer reduces risk

ETA-58 Suppliers of COV technologies shall offer COV IT devices that support and or comply with VITA-approved operating systems and software, architecture standards, hardware manufacturer recommendations, and COV Technology Roadmaps.

ETA-59 COV shall follow a formal process for reviewing and approving suppliers' of COV IT services baselines (includes core images, and configurations).

ETA-60 All technologies supported by the suppliers of COV IT services shall have defined and approved baselines for all supported technologies.

The baseline documentation shall include:

- All of the security control settings and configurations available to be configured for the system component the baseline is being written for
- The description of the security control settings and configurations and what they do
- The baseline settings from an industry recognized framework (if available) or an explanation of why one is not available for that particular system component
- The recommendation from the supplier if the security control setting or configuration will be enabled or disabled
- An explanation or rational statement for that recommendation
- An explanation if there is a difference between the supplier recommendation and the industry recognized framework

Note: Examples of baselines are Center for Internet Security (CIS) and Department of Defense (DoD) Security Technical Implementation Guides (STIGs)

ETA-61 Suppliers of COV IT services shall follow the COV baseline process for all supported technologies and shall review baseline documentation at least annually and update as required.

ETA-62 Baseline images and configurations for COV IT devices shall at a minimum be reviewed annually and updated as required.

ETA-63 All COV IT devices shall have a defined and approved lifecycle which drives refresh schedules.

ETA-64 COV agencies wishing to delay a device refresh or replacement, shall submit an Enterprise Architecture exception via Archer for review and approval.

Note: If COV IT device or software on the device has reached end of service or end of life, the agency is obligated to refresh the device to maintain security and support for the device

ETA-65 Suppliers of COV IT technologies shall provide reliable messaging for alerts and notifications using multiple approaches (emails, texts, instant messages).

ETA-66 Impact on other COV services of a new or updated technology shall be assessed, modeled, and reported prior to that technology's deployment.

Example: COV wants to reduce potential latency experienced by end users from the use of new technologies such as virtualization, containerization, and microservice architectures

Note: This information may be reported within the architecture review process

Security

These requirements relate to consistency of the security infrastructure across the enterprise and the protection of enterprise IT assets, while managing risk to an acceptable/usable level.

ETA-67 All COV IT technologies, solutions, and services shall implement and document technology components (AOD) and device configurations (documented baselines).

ETA-68 Access to specified systems, services, and/or other technologies shall be granted to the Chief Information Officer, the Chief Information Security Officer for the Commonwealth of Virginia, or an identified designee with credentials upon request.

ETA-69 Suppliers of COV technologies shall monitor for and resolve suspicious activity or patterns that may be indicative of a device issue requiring resolution (e.g., virus, rogue application).

Note 1: If the device is compromised, the expectation is that the compromise will be contained.

Note 2: The resolution of suspicious activity or patterns shall include any needed triage and escalations.

ETA-70 All smart/mobile devices, systems and storage containing or processing COV data which are removed from COV owned or leased secured locations shall implement full disk encryption.

ETA-71 COV IT technologies used shall provide the ability to decrypt data in order to perform a forensic analysis of data system.

ETA-72 COV technologies shall be able to provide the capability for configurable alerts and notifications when security incidents are detected.

Note: To include SMS, email, phone, texts

Definitions and Terminology

The following terminology and definitions are applicable to the use of technologies:

Complex Event:

1. An incident that has caused a complete and immediate work stoppage across the Enterprise (affecting multiple agencies across multiple lines of business). The expectation is that the service will not be fully reestablished within the approved RTO and/or RPO.

   Examples: Failure that impacts a significant portion of the SAN, WAN, or private cloud

2. An incident that has caused a Mission Critical service to be unavailable to multiple agencies across multiple lines of business.

   Examples: Prolonged outages of email and active directory services

Current COV contracts and architecture governance restricts technology used to provide/host/deploy/support COV IT solutions to approved “N” or “N-1” versions even if some vendors have limited support for “N-2” or earlier versions.

Disaster means an event or series of events constituting a disaster under the terms of the Disaster Recovery Plan or under the Supplier Disaster Recovery Plans.

Disaster Recovery Plan (DRP) a set of documented procedures that identify the steps to restore essential business functions on a schedule that supports agency mission requirements. The plan to execute Disaster Recovery Services

Disaster Recovery Planning means, as defined by the ITIL, the series of processes that focus only upon the recovery processes, principally in response to physical disasters that are contained within BCM (Business Continuity Management).

Disaster Recovery (DR) (Services) means the process of following specific advance arrangements and procedures in response to a disaster, resumption of the critical business functions within a predetermined period of time, minimizing the amount of loss, and repairing or replacing the damaged facilities as soon as possible. The Disaster Recovery Services consist of the Disaster Recovery related Services and include support and coordination with the Business Continuity Services.

Event means an Incident, including failures of service delivery, security breaches, etc.

Incident means an event which is not part of the standard operation of a service, and which causes or may cause disruption to or a reduction in the quality of services and VITA and/or other customer productivity.

Mission-critical system consists of the IT solutions that support an agency or department mission-essential business function or back-office function (including infrastructure, people, resources, process, and data) for the organization that must be continued throughout, or resumed rapidly after, a disruption of normal day to day activities. It also includes statutory business functions required by the law or mission of the department or agency. A mission-critical system is also known as mission essential equipment or mission-critical application.

“N” is the most recent approved version of a technology.

“N-1” is the previous approved version.

Reliable messaging is the guarantee that a message sent by a sending application is indeed received at the other end, and only received once.

"**Supplier**" means any business entity, corporation, organization, firm, or individual, including any of its Affiliates (i.e., an entity that controls; is controlled by, or is under common control with Supplier) that provides IT related products or services to the Commonwealth of Virginia (COV).

Suppliers of COV IT services have contractual arrangements with COV to provide IT equipment, system software, IT solutions, network and voice components, messaging, security, integration, management, support, operation, or hosting of COV IT systems (for example: IaaS, PaaS, SaaS), solutions, and data.

Supported means that a technology is current and has security patching available via vendor or another equivalent entity. Vendors often use different and confusing terminology for support. For Microsoft, both mainstream and extended support provide security patching. For IBM, extended support may not include security patching. A vendor supplied support that allows the vendor to require updating to a more current version vs. supplying the security patch does not meet the COV definition of "supported".