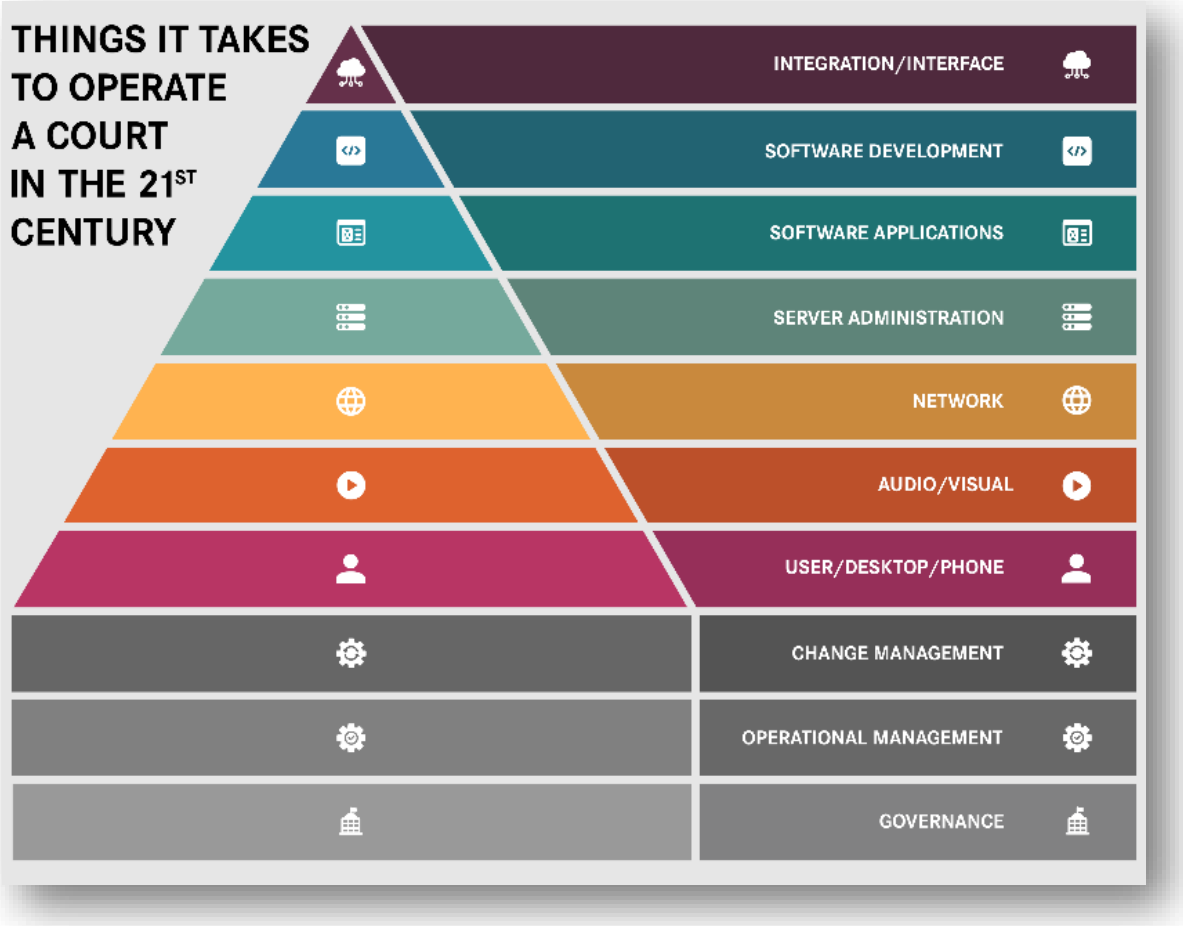
COT-Approved Changes 6/12/2025

Gap Reporting for New Court IT Operational Standards:



NOTES: 1) Any need for the support organization to exempt itself from a requirement needs to be reviewed and approved by the governance board or local court management.
2) "Certification" includes vendor-specific credentials as well as industry-recognized credentials as approved by Commission on Technology, e.g., CompTIA, Pluralsight, BrainBench, etc.

COT-Approved Changes 6/12/2025

ONLY COMPLETE THE TABLES FOR DOMAINS THAT ARE ACTIVELY RELIED UPON BY YOUR COURT, REGARDLESS OF IT RESPONSIBILITY.

Court Leadership Approval Signatures

Presiding Judge (required)

Signature	(Print Name)	Date

Elected Clerk of Court (when applicable)

Signature	(Print Name)	Date

Court Administrator (when applicable)

Signature	(Print Name)	Date

COT-Approved Changes 6/12/2025

User/Desktop/Phone Support

Specialized support necessary to address end-users' incidents, service requests, and maintenance needs by technicians to ensure optimal performance.
Recommend, procure, install, inventory, maintain, and troubleshoot all end-user devices owned and managed locally
Use standard image and configurations, monitor replacement lifecycle, maintain accurate inventory, use vulnerability scanning tool and remediate exposures, keep end-user licensing legal
Any changes to the end-user environment are approved by management, standard image is maintained and deployed via templates. PC imaging should be accomplished using a dedicated tool such as MDT or System Center. Technicians are trained in all areas they support, including for any new equipment added.
Users are prevented from installing software that violates policy.

User/Desktop/Phone Support Details	Responsible Entity	Gap Details / Exceptions
Qualifications -- 1. CompTIA A+ (strongly recommended, not required) 2. Certification(s) for specific equipment deployed	List end-user items:	List certifications by item:
Procuring -- 1. Specify standard end-user technology a. Desktops b. Laptops c. Peripherals d. Software 2. Identify refresh cycle as part of procurement to ensure technology does not fall out of support or go end-of-life (for local city/county hardware) 3. Purchasing 4. Decommissioning		
Installing -- 1. Standard image is maintained and deployed. Imaging should be done with a tool such as MDT or System Center as a best practice.		

COT-Approved Changes 6/12/2025

User/Desktop/Phone Support Details	Responsible Entity	Gap Details / Exceptions
2. All images are scanned with a vulnerability scanning tool to ensure the security of the system. 3. Perform ongoing refresh and recertification of images annually.		
Supporting/Maintaining -- 1. All end-user equipment lifecycles are monitored. 2. A refresh plan is identified and documented to maintain a secure environment 3. All equipment has active warranties through the vendor for the entire lifecycle. a. If devices cannot stay in warranty throughout the documented lifecycle, spares should be available with sufficient funding to procure individual replacements. In addition, all firmware should be updated.		
Change Management -- Formal change management process is documented. Any changes to the production image and environment are approved by management. Once changes have been approved and implemented, checks are completed to ensure no issues have occurred.		
Triage -- 1. Set and follow standard escalation levels (e.g., Level 1, 2, 3) 2. Initial incident and troubleshooting is documented at the help desk level prior to escalation 3. Use formal incident tracking with reporting functionality 4. Problem considered resolved once the business or user has confirmed operations restored		
Documentation / Training -- 1. User support requests are logged in a ticketing system or another means that is searchable by user, type of issue, etc. 2. Standard equipment is documented including printers/MFPs, etc. 3. New user requests are approved and maintained per judicial minimum security requirements		

COT-Approved Changes 6/12/2025

User/Desktop/Phone Support Details	Responsible Entity	Gap Details / Exceptions
4. Support technicians are trained in all areas they support, including for any new equipment added a. Training can be conducted in various ways: training partners, online, book, vendor supplied, peers		
Asset Management (Inventory/Replacement/Repair) -- 1. All hardware and software is inventoried 2. Software licenses are documented and audited to ensure sufficient licensing is present 3. All replaced/repaired hardware purchased has warranty from vendor/reseller, onsite spares, or ready access to spares		
Consider the Risk/Mitigation Strategies -- 1. Computer Network Security training provided annually to all court employees 2. On core-network-attached PCs/laptops, users are prevented from installing software without appropriate controls 3. On core-network-attached PCs/laptops, peripherals attached to devices (including IoT items) must be documented and management-approved beforehand		
Budgeting / Staffing -- 1. Appropriate budget / plan exists to meet the refresh cycle associated with technology procurement 2. Staffing is appropriate to meet local support requirements		

User/Desktop/Phone Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Audio/Visual Support
Specialized support necessary to install and maintain courtroom audio/visual technologies that support remote appearance, display technologies, and digital recording of the record at one of three levels of complexity.
Keep all audiovisual applications in compliance with court rules; consult with judicial officers on use of equipment within the rules
Perform installations, support, documentation, training, and troubleshooting/repairs by onsite court staff or by having staff perform incident triage with a contracted vendor providing further support services.
Ensure latest patches and firmware have been installed in a/v equipment, use formal incident tracking and change management procedures, maintain active warranties or vendor-support contracts throughout equipment lifecycle

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
Tier 1 – Single video system connected to single display device Tier 2 – Audio/Visual system containing multiple inputs and outputs with manual video switching capabilities and without audio integration Tier 3 – Large audio/visual system containing multiple inputs and outputs using controlled switching and integrated audio capabilities.		Enter Court Tier Here: _____
Qualifications/Assessment -- Tier 1 – Basic level of video switching. Tier 2 – Basic level of video switching, knowledge of video formats and video converters.		

COT-Approved Changes 6/12/2025

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
Tier 3 – Certification from vendor(s) whose equipment is installed (e.g., Kramer, Biamp, Crestron, Extron) OR vendor contract to provide required support and services to ensure equipment remains operational. All audiovisual applications must be in compliance with court rules surrounding audio and video appearances. Obtain written vendor requirements/pre-requisites for equipment being installed Comply with direction in administrative code and court rules Define roles and responsibilities for all aspects of courtroom technology support		
Procuring -- 1. Specify target audio and video equipment included in Arizona Judicial Branch Enterprise Architecture Standards (Tiers 2 and 3) a. Video system b. Audio DSP c. Video switch d. Video controller e. Microphone types f. Devices capable of being controlled via RS232, IR, or network. g. Standardize on all courtroom displays using same manufacture capable of 1080p minimum resolution. h. Input devices (Blu Ray, Doc Cam, etc., capable of minimum 1080p resolution) 2. Consider a secure local internet access point outside of the courts network for any video codec and remotely serviced equipment, at a minimum (Tier 3). 3. Identify refresh cycle as part of procurement to ensure technology does not fall out of support or go end-of-life 4. Require vendor submittal of source code at the completion of the implementation.		

COT-Approved Changes 6/12/2025

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
Installing -- Tier 1 1. Design drawings referencing: a. All inputs and outputs b. Courtroom user manual. Tier 2 1. Design drawings referencing: a. All inputs and outputs b. Connectivity method c. Courtroom user manual d. Document type of connections / formats are necessary to connect into system 2. Utilize standard video switch (see Arizona Judicial Branch Enterprise Architecture Standards and applicable local standards) 3. Identify local secure internet connection to support A/V system. All A/V devices excluding the video codec should reside on separate internal network with internet access Tier 3 1. Design drawings and documentation referencing: a. All inputs and outputs b. External device control methods c. External device ports d. Connectivity method e. Control logic f. All device IP addresses used per system g. Courtroom user manual explaining each functionality of the touch panel and casting functionality. h. Document type of connections / formats are necessary to connect into system 2. Build in user buttons to return all systems back to default		

COT-Approved Changes 6/12/2025

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
3. Change default controller and DSP passwords. 4. Identify local secure internet connection to support A/V system. All A/V devices excluding the video codec should reside on separate internal network with internet access. 5. Test system 6. Back up configuration of DSP and controller		
Supporting/Maintaining -- 1. All end-user equipment lifecycles are monitored. 2. A refresh lifecycle plan that evaluates, at an 8-year maximum, the continued viability of all A/V equipment. 3. Ensure latest patches and firmware have been installed in video controller DA, video switch and DSP, and indicated as current in the documentation. 4. All video systems below should have active warranties through the entire lifecycle, onsite spares, or ready access to spares. a. Video switch b. Audio DSP c. Video DA d. Amplifier e. Video converters 5. Preventive maintenance is performed at least annually to ensure operational reliability.		
Change Management -- 1. Formal change management process is documented. Any changes to the environment are approved by the governance body or court management. Once changes have been approved and implemented, checks are completed to ensure no issues have occurred.		

COT-Approved Changes 6/12/2025

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
Triage – 1. Use formal incident tracking with reporting functionality 2. Problem considered resolved once the business or user has confirmed operations restored		
Training – 1. Court users and staff are trained on the general use of system 2. Technical staff reviews operational switching, wiring and logic on controls		
Asset Management (Inventory/Replacement/Repair) – 1. All hardware equipment is inventoried and tracked. 2. A copy of currently installed configuration files and firmware are maintained in a backup repository and labeled as current for the applicable equipment. (Tier 2 and 3)		
Consider the Risk/Mitigation Strategies -- 1. Review documentation and firmware levels and ensure that spares are functional 2. Maintain a continuity of operations plan for remote proceedings which may include: a. maintaining an inventory of pre-configured spares of identical equipment (Tier 2 and 3 rural courts) or b. having a vendor support agreement in place that meets business-critical SLAs (urban courts) or c. having a backup solution documented ahead of time in accordance with the continuity of operations plan.		
Documentation -- The system documentation should contain the following items 1. All final design drawings a. Wiring layout		

COT-Approved Changes 6/12/2025

Audio/Visual Support Details for Rooms Used for Court Proceedings	Responsible Entity	Gap Details / Exceptions
b. IP Addresses for all equipment c. Control method d. Switching layout e. Audio inputs / output designation 2. User manual 3. Backup configuration file locations. 4. Equipment userIDs and passwords.		
Security -- 1. Tier 2 and 3 components should have all default passwords changed.		
Budgeting -- 1. Appropriate budget / plan exists to meet the refresh cycle associated with technology procurement. 2. Staffing is appropriate to meet local support requirements.		

Audio/Visual Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Network Support

Performing necessary activities using established methods, procedures, and specialized tools to administrate, operate, and reliably maintain computer network systems that provide connectivity to other computer systems and ensure quality of service.
Recommend, procure, install, troubleshoot local network devices. Perform capacity planning to ensure sufficient bandwidth and quality of service.
Use standard equipment and configurations, monitor access logs, maintain inventory/diagrams, maintain environmental controls, perform vulnerability scanning, maintain firewall rules and access controls.

Network Support Details	Responsible Entity	Gap Details / Exceptions
Qualifications/Assessment – 1. Certifications for Wiring 2. Network Certification		
Procuring -- 1. Identify current standards and work with contracted vendor to acquire new technologies. Review current standard before procurement of additional items of existing technologies. 2. Identify refresh cycle as part of procurement to ensure technology does not fall out of support or go end-of-life		
Installing -- 1. All network equipment is installed per vendor requirements 2. Each device installation follows vendor's best practices for the specific product application		
Supporting/Maintaining -- 1. All network equipment lifecycles are monitored		

COT-Approved Changes 6/12/2025

Network Support Details	Responsible Entity	Gap Details / Exceptions
2. A refresh plan is identified and documented to maintain a secure and highly available environment 3. All equipment has warranties through the appropriate vendor. Warranty is renewed prior to expiration. A different product must be selected when a warranty is no longer available.		
Change Management -- 1. Formal change management process is documented. Changes to the network environment having potential direct user impact are approved by appropriate court management. Once changes have been approved and implemented, checks should be completed to ensure no issues have occurred. 2. Downstream network users are informed of changes prior to implementation		
Triage -- 1. Standard escalation levels (e.g., Level 1, 2, 3) 2. Initial incident and troubleshooting documented at the help desk level prior to escalation 3. Incident tracking 4. Problem considered resolved once the business or user has confirmed operations restored		
Training -- 1. Training should be conducted internally or externally by approved trainers. 2. Training should apply directly to supported systems and emerging technologies. 3. Training may also consist of online resources and books.		
Asset Management (Inventory/Replacement/Repair) -- 1. All hardware, software, and communication lines are inventoried per documentation requirements below.		

COT-Approved Changes 6/12/2025

Network Support Details	Responsible Entity	Gap Details / Exceptions
2. Software licenses are documented and audited to ensure sufficient licensing is present 3. All hardware is purchased with warranty from vendor/reseller a. If any hardware issues occur, warranty covers repair/replacement b. If no warranty is available, a different product should be selected or be replaced		
Consider the Risk/Mitigation Strategies -- 1. Network design considers scalability and critical failures. Any critical system is designed for sufficient scope and redundancy to maintain connectivity for business operations. 2. All network equipment is scanned by an approved vulnerability scanning tool regularly to ensure compliance. In addition, all network firmware must remain within current vendor guidelines 3. All network equipment is secured with strong passwords and no access is allowed by generic accounts		
Future Forecasting -- 1. Refresh cycles and rolling equipment replacement plan are identified for network equipment and related purchases 2. Capacity planning is in place to provide for scaling bandwidth over time		
Documentation -- 1. All network configurations are backed up to a secure location 2. A current network topology/map exists 3. Inventory of all network equipment 4. Firmware levels 5. Vulnerability scan results with remediation plans		
Security -- 1. Application-specific or outside agency security requirements (e.g., ACJIS, PCI) are complied with, where applicable.		

COT-Approved Changes 6/12/2025

Network Support Details	Responsible Entity	Gap Details / Exceptions
2. Vendor-recommended hardening is considered across all network equipment a. Deviation from vendor recommendations is documented and approved by management 3. Equipment complies with Judicial Branch Minimum Security Standards 4. Traps and audit logs are monitored and should be offloaded to a log manager/SIEM 5. Access to network equipment is controlled by identity management software 6. Intrusion detection is performed 7. Any network supporting judicial information has port security in place and enforced 8. Public network connectivity is provided separate from the judicial information network 9. No non-court-managed devices may connect directly to the court network 10. Any non-court-managed device connecting indirectly to the secured court network must be approved by senior court management and meet judicial standards		
Performance Monitoring / Management -- 1. Network bandwidth utilization, availability, and reliability are monitored and forecast 2. Anomalous behavior is detected, alerted and addressed 3. Critical network components have alerting mechanisms in place		
Disaster Recovery -- An approved continuity of operations plan exists for addressing network outages		
Facilities / Environmental Controls -- 1. All equipment resides in a secure facility only accessible by IT with logged entry 2. Facilities are equipped with vendor-required environmental controls, including monitoring and alerts		

COT-Approved Changes 6/12/2025

Network Support Details	Responsible Entity	Gap Details / Exceptions
Budgeting -- 1. Appropriate budget / plan exists to meet the ongoing support as well as refresh cycle associated with procurement 2. Staffing is appropriate to meet continuous operation requirements for networking		

Network Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Server Administration/Support
Server administration involves managing and monitoring the performance of local computer servers, both physical and virtual, managing user accounts, and allocating system resources to ensure systems run efficiently with minimal unplanned downtime.
Critical systems are designed to maintain connectivity for business operations; facility is secured with environmental monitoring and alerts
All permissions set to allow only IT Administrators, System Logs are maintained, implement security remediations, maintain firewall rules, conduct mock recovery on a bi-annual basis to ensure the integrity of backups.

Server (Physical and Virtual) Administration/Support Details (including Operating Systems and Orchestration)	Responsible Entity	Gap Details / Exceptions
Qualifications/Assessment -- • Certification		
Procuring – 1. Identify current standards and work with contracted vendor to acquire new technologies. Review current standard before procurement of additional items of existing technologies. 2. Identify refresh cycle as part of procurement to ensure technology does not fall out of support or go end-of-life		
Installing – 1. Where applicable, a standard image will be used across the environment and be compliant with Arizona Judicial Branch Enterprise Architecture Standards. 2. All images are scanned with a vulnerability scanner to ensure the security of the system.		

COT-Approved Changes 6/12/2025

Server (Physical and Virtual) Administration/Support Details (including Operating Systems and Orchestration)	Responsible Entity	Gap Details / Exceptions
3. Each device installation follows vendor's best practice.		
Supporting/Maintaining – 1. All server lifecycles are monitored. 2. A refresh plan is identified and documented to maintain a secure and highly available environment. 3. All production equipment has active warranties through the appropriate vendor. Warranty is renewed prior to expiration. A different product must be selected when a warranty is no longer available.		
Change Management – 1. Formal change management process is documented. Any changes to the server environment are approved by management. Once changes have been approved and implemented, checks should be completed to ensure no issues have occurred. 2. Downstream server users are informed of changes prior to implementation		
Triage -- 1. Standard escalation levels (e.g., Level 1, 2, 3) 2. Initial incident and troubleshooting documented at the help desk level prior to escalation 3. Incident tracking 4. Problem considered resolved once the business or user has confirmed operations restored		
Training – 1. Training is conducted internally or externally by approved trainers. 2. Training applies directly to supported systems and emerging technologies. 3. Training may also consist of online resources and books.		
Asset Management (Inventory/Replacement/Repair) --		

COT-Approved Changes 6/12/2025

Server (Physical and Virtual) Administration/Support Details (including Operating Systems and Orchestration)	Responsible Entity	Gap Details / Exceptions
1. All hardware, software, and communication lines are inventoried per documentation requirements below. 2. Software licenses are documented and audited to ensure proper licensing and maintenance is present. 3. All hardware is purchased with warranty from vendor/reseller. • If any hardware issues occur, warranty covers repair/replacement.		
Consider the Risk/Mitigation Strategies – 1. Server architecture considers scalability and critical failures. Any critical system is designed for sufficient scope and redundancy to maintain connectivity for business operations. 2. All servers are scanned by an approved vulnerability scanning tool regularly to ensure compliance. In addition, all server firmware must remain within current vendor guidelines. 3. All servers are secured with strong passwords and no access is allowed by generic accounts. a. All access to servers is maintained with role-based access control.		
Documentation – 1. Operating System 2. Assigned memory 3. CPU 4. HDD 5. External Storage Arrays: SAN/NAS/JBOD 6. Management software: Managed by OS or vendor application 7. External Ports: Web Servers, SFTP, etc 8. IP Address: Assigned IP's, management interface, remote console 9. Appliances: Proxy, Firewall, etc 10. Configured Applications: Solarwinds, IBM, IIS, etc		

COT-Approved Changes 6/12/2025

Server (Physical and Virtual) Administration/Support Details (including Operating Systems and Orchestration)	Responsible Entity	Gap Details / Exceptions
11. Third-Party Software: Any software not shipped with installed OS 12. License details: Microsoft client/server, subscription services, etc		
Security -- 1. Antivirus installed 2. Firewall rules are set up based on access needs (ensure not all users have the same access). 3. All servers are built to meet Arizona Judicial Branch Enterprise Architecture Standards. In addition, any installed software is compliant and maintained. 4. All permissions are set to allow only IT Administrators access to the administrative layer of the server. a. On production servers, RDP is restricted to only approved subnets and users. b. Administrators to servers ratio is kept minimal c. No generic admin account is used to logon interactively. i. Administrative service accounts can be used but will be denied the right to log on locally. 5. Default administrator account is disabled or appropriate security controls are added. 6. System logs are maintained for a minimum of 30 days. 7. All file shares are restricted per enterprise requirements. 8. All critical and security vulnerabilities must be implemented promptly per AOC minimum security requirements.		
Performance Monitoring / Management – 1. Server resource utilization is monitored. 2. Critical components have alerting mechanisms in place. 3. Anomalous behavior is detected, alerted, and addressed.		
Future Forecasting –		

COT-Approved Changes 6/12/2025

Server (Physical and Virtual) Administration/Support Details (including Operating Systems and Orchestration)	Responsible Entity	Gap Details / Exceptions
1. Server lifecycles are documented. 2. Refresh plan is developed prior to end of life/end of support.		
Disaster Recovery – 1. A plan commensurate with the continuity of business operations is in place 2. Identify reputable backup vendor that supports current/future infrastructure 3. Determine retention period for all backups, giving consideration to the following: a. Define the minimum and the preferred number of days for retention. b. Storage requirements needed c. Off-site location identified and functioning i. Hot or cold site ii. Ability to bring up critical applications after disaster 4. Incremental, full, synthetic full 5. Validate the integrity and utility of backups periodically. a. Critical servers are prioritized and scheduled for recovery 6. Daily reports sent out indicating success/failure of all backups 7. Perform at least an annual recovery test		
Facilities / Environmental Controls – 1. All equipment resides in a secure facility only accessible by authorized staff, as governed by Judicial Branch Security Standards and local requirements 2. Facilities are equipped with proper cooling 3. Facilities have environmental monitoring and alerting set up		
Budgeting – 1. Appropriate budget / plan exists to meet the refresh cycle associated with technology procurement 2. Staffing is appropriate to meet local support requirements, including required skill sets and certifications to support the technology		

Server (Physical and Virtual) Administration Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Acquired Software Application Administration

Software application administrators evaluate, deploy, maintain, enhance, and manage all packaged software applications developed by vendors that run on court servers and infrastructure

Run defined projects to choose and deploy vendor software governed by business requirements

Monitor overall support cost, self-audit software licensing compliance, adhere to separation of duties and documented access request procedures, related server and database information must be documented in the application catalog, vendor access is governed by a process requiring advanced notice and specific timelines, plan and execute periodic release cycles, follow a documented change management process.

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
Tier 1 – Traditionally licensed and installed in local environment even if the vendor still manages the application there Tier 2 – Platform-as-a-service model where local IT performs software and infrastructure management within the vendor's environment Tier 3 – Software-as-a-service model where vendor hosts and performs all infrastructure and application management		
Qualifications/Assessment – 1. At least one IT staff member, contractor, or vendor is certified in the applicable database technology (Tiers 1 and 2)		

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
2. At least one BA is involved in the assessment effort (all tiers)		
Procuring/Licensing – (all tiers) 1. For new applications, a *Make or Buy* analysis should be conducted and communicated with governance authority for approval 2. For vendor applications, a *fit/gap* analysis should be performed using a standard methodology for determining best functional fit 3. Maintaining uniformity of frameworks and databases should be key drivers when purchasing or creating applications 4. Judicial Enterprise Architecture standards must be followed, unless excepted by a statewide governance body 5. Procurement policies must be complied with		
Installing -- 1. Local IT staff should be responsible for executing deployment activities with the guidance/direction of vendors to facilitate on-site knowledge of application architecture and deployments (Tier 1) 2. Vendors should only be allowed temporary, incident-based access that is governed by a process requiring advanced notice and specific timelines (Tier 1) 3. Significant deployments should include the following pre-deployment documentation at a minimum: (Tiers 1 and 2) a. Step-by-step deployment guide, b. Communication plan covering staff and user base, and c. Rollback plan. 4. For critical deployments, at least one trial deployment exercise should be performed and tested 5. Special attention and testing should be planned around any implementation requiring data conversion 6. Utilize, at the least, a rudimentary project management methodology that clarifies specific deliverables, including a schedule, a deployment plan, a		

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
communications plan, a test plan, specific requirements documents, and an overall cost estimate 7. Documentation must be current and accessible to all support personnel (Tiers 1 and 2)		
Supporting/Maintaining – (all tiers) 1. Responsible application administrator is named and approved by governance board or someone in court leadership who understands the implications and impact associated with delegation of this authority 2. Access to applications is governed by an official process that includes and requires initial request documentation (access forms) 3. Ongoing support costs are monitored and periodically reviewed		
Change Management – (all tiers) 1. Formal change management process is documented and followed - See *Management and Governance* for detailed change management information 2. A formal process for documenting change management within the application lifecycle management system is understood and followed by development team		
Triage – (all tiers) 1. Application triage is governed by a process of severity assessment and escalation through multiple tiers of the support organization (e.g., Level 1, 2, 3) that engages different resources based on level. 2. Initial application troubleshooting procedures are documented at the help desk level and followed before advancing to the next level.		
Training -- 1. For enterprise applications, a training document library is in place and updated as part of every significant release cycle. 2. For enterprise applications, standardized classes are created and provided to end users.		

COT-Approved Changes 6/12/2025

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
3. For all large releases, a training plan is included as a project management deliverable. 4. Training materials and training classes (for both IT staff and business users) should be included in any implementation contract with a vendor. 5. For any large application, time must be allocated for transition of technical knowledge from vendors or contractors to local IT staff.		
Asset Management (Inventory/Replacement/Repair) -- 1. For Tier 1 and Tier 2, a periodic process is in place to self-audit software licensing compliance for third-party libraries, frameworks, and databases 2. For Tier 1 and Tier 2, database licenses should be optimized to meet the right balance of performance and quantity of databases per core server licensing 3. For all tiers, age and supportability of applications are regularly assessed		
Consider the Risk/Mitigation Strategies -- • Consider business and technical risks along with ways to manage them: ○ Determine which tier is appropriate ○ Know the vendor's release cycle ○ Know the method of submitting enhancements/bugs • Consideration must be given to potential procedures that enforce *Separation of Duties* concepts depending on the function of the software application • Ensure a Business Continuity/Disaster Recovery plan is in place for all functions of the software application		
Documentation -- 1. For Tier 1 and Tier 2, all server and database information for a specific application must be documented in the organization's application catalog for reference when environmental changes are required 2. For Tier 1 and Tier 2, data dictionaries and/or ERDs (entity relationship diagrams) are required for all applications		Need COT reqts added for SaaS/Vendor systems 3/5/25

COT-Approved Changes 6/12/2025

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
3. For Tier 1 and Tier 2, organizations must maintain all system documentation for each application in official storage areas 4. Formal documentation around application *user roles* should be available		
Security – (all tiers) 1. Only applications that support judicial security standards are implemented 2. Include infrastructure review of new requirements/design documentation to identify any security concerns 3. Implement procedures that enforce *Separation of Duties* concepts within processes associated with software development/testing and application deployment (example: resources that design/code should not be the same resources that deploy code)		
Performance Monitoring / Management -- 1. Monitor application performance and provide feedback to the support organization, as applicable. 2. Utilize industry standard database monitoring tools that flag slow performing applications/databases (Tiers 1 and 2) 3. Utilize industry standard tools for database index optimization (Tiers 1 and 2) 4. To identify and remediate poor performance, plan and execute periodic release cycles (coordinated with vendors) (Tiers 1 and 2)		
Future Forecasting -- • Understand the total annual cost (labor, licensing, maintenance, infrastructure) of the application versus the current utility.		
Disaster Recovery – (all tiers) 1. For Tier 1 and Tier 2, utilize backup or replication monitoring software or implement scripting that sends notifications when backups are unable to be performed.		

COT-Approved Changes 6/12/2025

Acquired Software Applications Administration/Support Details	Responsible Entity	Gap Details / Exceptions
2. For Tier 1 and Tier 2, perform regular, redundant backups or replications at both a database level and a systems level 3. Maintain a cyclical process that simulates disaster and tests the restorability of critical enterprise applications 4. Document the business continuity plan to be enacted in the event automation services get interrupted		
Budgeting -- 1. Utilize a standard, uniform estimating methodology that takes into account ALL expenditures including labor, licensing fees, vendor/contractor costs, and future licensing and maintenance costs. 2. Regularly audit estimate results against actuals to adjust estimating techniques accordingly.		

Acquired Software Applications Administration Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Software Development and Support

Covers local design, development, and maintenance of unique technology solutions implemented via custom-coded software, including bolt-ons to statewide applications.

Software development and related maintenance requires detailed planning, a large set of skills, multiple environments, more than a single developer, and a collaboration platform.

Management, not IT staff, determines the need for a custom-developed application after all other possible solutions are ruled out. Requires industry-standard frameworks and tools, documentation and source code tools are vital because the resources designing and coding the application will not likely be present through its complete useful life. Software referenced within local code must remain supported and legal over time. Change to the application may affect infrastructure and other applications, so changes must be tested in an appropriate environment and promoted into production by following an orderly process.

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
Tier 1 – Local-only "helper" application created as a convenience and on which court operation doesn't depend Tier 2 – Applications that affect multiple court staff and support regular transactional business process Tier 3 – Strategic applications that support multiple users across multiple court departments underpinning multiple core business processes or a single process on which court business depends (Applications may grow from a lower tier to higher tier as further development occurs)		
Qualifications/Assessment --		

COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
1. When development relies on database administration, at least one IT staff member is certified in the applicable database technology (Tier 3) 2. Proven skills in appropriate development languages and environments, e.g., Microsoft .Net and SQL (Tiers 2 and 3) 3. Skills and experience working with applicable data transformation technologies (Tiers 2 and 3) 4. Skills with software code management (All Tiers)		
Requirements Documentation/Design/Testing -- 1. For new applications, a *Make or Buy* analysis is conducted and communicated with the governance authority for approval. Tier level must be designated at time of approval. (Tiers 2 and 3) 2. Maintain and utilize standardized requirements documentation, including agreed service levels, that requires stakeholder approval before development begins (Tiers 2 and 3) 3. Specifications for any new public-facing web application should include consideration for responsive design or mobile user functionality (Tiers 2 and 3) 4. All test cases should be documented, including functional and UAT test cases. (Tiers 2 and 3) 5. Utilize and create as needed (on demand) a regression test case library for critical applications. (Tier 3) 6. Employ load testing as part of large, critical application releases. (Tier 3) 7. Database data models are documented in an ERD (entity relationship diagram) or at least a data dictionary. (Tiers 2 and 3) 8. Implement database designs that follow best practices for *data normalization*. (Tiers 2 and 3) 9. Utilize experienced database administrators for database designs, particularly designs involving database triggers and their associated actions. (Tier 3)		

COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
10. For any new applications, do not utilize database connectivity methods that derive access credentials from any files accessible to users. (All Tiers) 11. Industry-standard, third-party tools and frameworks are employed for web design, forms wizards, bots, user interface widgets, database connectivity, requirements engineering, systems design, XML message development and troubleshooting. (Tiers 2 and 3) 12. Application requirements conform to national and state data standards and code standards. (Tiers 2 and 3)		
Development Environment / Development Lifecycle -- 1. Ensure all production applications have at least one (and ideally two) non-production environments (e.g., DEV, TEST, PROD) that reflects the production environment (representative data, production code, database objects, and stored procedures). (Tiers 2 and 3) 2. Adhere to an approved, standard software development methodology (Waterfall, Agile, etc). (Tiers 2 and 3) 3. Utilize an ALM (Application Lifecycle Management) tool to assign, document, and track work items [e.g., Microsoft Team Foundation Server (TFS), Azure DevOps, Rational, Jira, VersionOne, etc.] (Tiers 2 and 3) 4. A formal business process is documented in detail clarifying workflow within the ALM system (ex: TFS) (Tiers 2 and 3) 5. Maintain an official *unit testing* process/policy consistently performed by developers that is documented and tracked in the ALM tool. (Tiers 2 and 3) 6. Utilize a peer review process for development code reviews that is documented and tracked by work item in the ALM tool. (Tier 3) 7. Utilize a project management methodology that clarifies specific deliverables, including a schedule, a deployment plan, a communications plan, a test plan, specific requirements documents, and an overall cost estimate. (Tier 3)		

COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
Source Code Management -- 1. A current code repository is utilized, preferably one that interfaces easily to your ALM tool. (All Tiers) 2. An obvious visual indicator is presented by all applications within the UI that indicates which database environment is currently connected (test, QA, production, replica, etc). (Tier 3) 3. Version control functionality is required and should compare the actual code version to the version stored in the target database, then disallow startup without a match. (Tier 3) 4. Third-party code libraries are maintained within the vendor's support window with all security vulnerabilities addressed. A plan is in place to address any unsupported versions that do not contain known vulnerabilities. (Tier 3) 5. Code changes are accompanied by comments that include described functionality, author, and referenced work item from within the ALM tool. (Tier 3) 6. In-house coding standards are developed, and documented, and agreed upon by all developers and reviewed regularly. (Tier 3)		
Migration / Deployment -- 1. Standardize on a team collaboration platform (e.g., MS-Teams) within the development team and mandate its use, especially during deployment activities. (Tier 2 and 3) 2. Normal deployments are executed outside of regular court business hours at a time when a reasonable recovery period following deployment is available for rollback if necessary (Tier 2 and 3) 3. Significant deployments include the following pre-deployment documentation at a minimum (Tier 2 and 3): a. Step-by-step deployment guide b. Communication plan covering staff and user base		

COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
c. Step-by-step rollback plan 4. For critical deployments, at least one trial deployment exercise is performed and tested using the deployment guide (Tier 3)		
Supporting / Maintaining -- 1. Maintain redundancy of expertise within the development team to prepare for outages and turnover. (Tiers 2 and 3) 2. Maintain a schedule (and/or implement automation) for performance-based database indexing maintenance.		
Change Management -- • Formal change management process is documented and followed - See *Management and Governance* for detailed change management information. (Tiers 2 and 3)		
Production Environment / Support -- 1. Maintain a current application portfolio that cross references applications, databases, server environments, and technical contacts. (Tiers 2 and 3) 2. Utilize automated monitoring tools for all production databases (e.g., Idera or Spotlight) (Tiers 2 and 3)		
Support Documentation -- 1. Data dictionaries and/or ERDs (entity relationship diagrams) exist for all applications (Tiers 2 and 3) 2. Official document storage areas exist for each application that contain requirements documents, deployment plans, etc. unless the entirety of activities are documented in the organization's ALM system (Tiers 2 and 3) 3. Reusable regression test libraries are maintained for each application (Tier 3) 4. Documentation of application *user roles* should be available on demand (Tier 3)		

COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
5. User and support documentation are maintained, including system interdependencies and owners of dependent systems (Tier 2 and 3)		
Training -- 1. A training materials library is in place and updated as part of every release cycle. (Tier 3) 2. Standardized classes are created and provided to end users (Tier 3) 3. Training plan is included as a project management deliverable (Tier 3)		
Asset Management (Inventory/Replacement/Repair) -- • A periodic process should be in place to self-audit software licensing compliance for third-party libraries, frameworks, and databases (Tier 2 and 3)		
Consider the Risk/Mitigation Strategies -- • Implement procedures that enforce *Separation of Duties* concepts within processes associated with software development/testing and application deployment (example: resources that design/code should not be the same resources that deploy code) (Tier 3)		
Security -- 1. New applications support Microsoft Active Directory credentialing for all internal users and when otherwise available (all tiers) 2. For new, externally available applications, authentication requirements must conform to judicial architecture specifications (Tier 3) 3. Maintain technical separation between internal and external applications (Tier 3) 4. Any personally identifying or sensitive information is appropriately classified and protected (Tier 2 and 3)		
Performance Monitoring / Management -- • Utilize industry standard tools for database index optimization (Tier 3)		
Future Forecasting --		

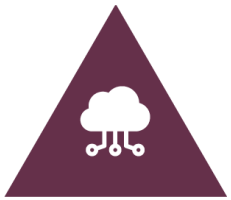
COT-Approved Changes 6/12/2025

Software Development and Support Details incl Bolt-Ons	Responsible Entity	Gap Details / Exceptions
• Estimating techniques derive future labor and licensing costs from data gathered from the ticketing system, the time management system, and the ALM application (Tier 2 and 3)		
Disaster Recovery -- See Server section • Documented manual backup processing addresses extended loss of automated functionality. (Tier 2 and 3)		
Budgeting / Staffing -- 1. Utilize a standard, uniform estimating methodology that takes into account ALL expenditures including labor, licensing fees, vendor/contractor costs, and future licensing and maintenance costs. (Tier 2 and 3) 2. Regularly audit estimate results against actuals to adjust estimating techniques accordingly (Tier 2 and 3) 3. Multiple developers are on staff (Tier 3)		
Consider Bolt-On requirements within development sphere -- 1. For enhancements to existing applications, requirements analysis and documentation must consider interfaces and other bolt-on applications that could be affected by code and database changes (Tier 3) 2. Change management is employed across all users of any bolt-on application (Tiers 2 and 3) 3. Existing bolt-ons being shared with or adopted by other entities require review and approval of the prime application beforehand (Tiers 2 and 3)		
Consider Sharable Applications requirements within development sphere • Any sharable application must comply with Tier 2 of the development standards, at a minimum.		

Software Development and Support Gap Close Strategy & Timeline

COT-Approved Changes 6/12/2025

Enter a closure plan and timeline for each gap documented in the table above.



Integration/Interface Support

Constructing, managing, and monitoring various types of connections across boundaries between distinct software applications operating in separate computing environments, enabling interoperation using an application programming interface (API) or "middleware."
When middleware breaks, communication between systems stops, so it must be monitored and provide functions for reprocessing transactions that fail.
Maintain official document storage areas for each integration/interface that contain requirements documents, deployment plans, etc., utilize active directory accounts for database access, a multi-agency change management process is documented and approved by all interface stakeholders, at least one non-production environment is kept current and utilized specifically for interface testing, plan and execute periodic release cycles that identify and remediate poor performing database queries and stored procedures.

Integration/Interface Support Details	Responsible Entity	Gap Details / Exceptions
Qualifications/Assessment -- 1. Advanced skills in XML and XML parser libraries or JSON, as applicable 2. Skills in MQ Series 3. Web and application services 4. SQL expertise, where applicable 5. Skills and experience working with XML-based data transformation		
Procuring Middleware -- 1. For new interfaces, a *Make or Buy* analysis should be conducted and communicated with governance authority for approval 2. For vendor middleware, a *fit/gap* analysis should be performed using a standard methodology for determining best functional fit, taking into		

COT-Approved Changes 6/12/2025

Integration/Interface Support Details	Responsible Entity	Gap Details / Exceptions
account compliance with AOC middleware architectural standards, specifically around transactional monitoring compliance		
Installing -- 1. Significant deployments must include the following pre-deployment documentation, at a minimum: a. Step-by-step deployment guide b. Communication plan covering staff and user base c. Rollback plan 2. For critical deployments, at least one trial deployment exercise should be performed and tested 3. Utilize, at the least, a simplistic project management methodology that clarifies specific deliverables, including a schedule, a deployment plan, a communications plan, a test plan, and specific requirements documents 4. For new interfaces, statewide data standards must be utilized, whenever applicable		
Supporting/Maintaining/Testing -- 1. Detailed architecture diagrams are maintained for each significant interface 2. For new interfaces, data dictionary/data mapping (as applicable) is maintained for each significant interface and data elements conform to applicable standards 3. Time is allotted for adherence to current tool versions 4. Data cleanup scripts are covered by a formal change control process 5. For new interfaces, regression test case libraries are created for testing and validation 6. At least one non-production environment (and ideally two) is kept current and made available to partners for interface testing		
Change Management --		

COT-Approved Changes 6/12/2025

Integration/Interface Support Details	Responsible Entity	Gap Details / Exceptions
• A general agreement between the management of integrated entities governs changes to interfaces over time • New interfaces between courts and the AOC are documented and approved by stakeholders • See *Management and Governance* below for detailed change management information		
Triage -- • A process documented is executed for engaging a triage team consisting of multi-agency contacts, as applicable		
Training -- • Redundant expertise is in place at the development team and business analysis levels to enable appropriate support and backup		
Portfolio Management -- • For new interfaces, apply uniform interface frameworks agreed upon by the appropriate jurisdictional level, whenever possible		
Consider the Risk/Mitigation Strategies -- • Where possible, ensure that connected applications have end-to-end automated monitoring and reporting of interface status • Ensure a Business Continuity/Disaster Recovery plan is in place for all integrated data flows		
Future Forecasting -- • For business-critical interfaces, utilize estimating techniques that derive future labor and licensing costs based on real data gathered from the ticketing system, the time management system, and the application lifecycle management application		
Security --		

COT-Approved Changes 6/12/2025

Integration/Interface Support Details	Responsible Entity	Gap Details / Exceptions
1. Include infrastructure review of new requirements/design documentation to identify any security concerns 2. Utilize active directory accounts for database access (do not allow credentials to be stored in accessible files) 3. Log all transactions and store logs for sufficient time to investigate issues 4. Use levels of encryption commensurate with the sensitivity of the data being transmitted		
Performance Monitoring / Management -- 1. See database requirements in the Software Applications/Support Domain 2. Monitor and manage external partners' performance / response times		
Disaster Recovery -- • Critical integration points are identified with business partners • Communication methods are identified, planned for, and documented		
Budgeting -- 1. Utilize a standard, uniform estimating methodology that considers ALL expenditures including labor, licensing fees, vendor/contractor costs, and future licensing and maintenance costs. 2. Regularly audit estimated results against actuals to adjust estimating techniques accordingly		
Transaction Management -- • Utilize tools where possible and practical that track data movement at the transactional level and provide functions for reprocessing transactions that fail (e.g., a "backout" queue)		
Documentation / Data Dictionary -- 1. Detailed architecture diagrams are maintained for each significant interface 2. A data map is maintained for each significant interface		

COT-Approved Changes 6/12/2025

Integration/Interface Support Details	Responsible Entity	Gap Details / Exceptions
3. Detailed data flow/transaction flow diagrams are maintained for each significant interface 4. Organizations must maintain shared document storage areas for new interfaces that contain requirements documents, deployment plans, etc.		

Integration/Interface Support Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Foundational Layers Behind ALL Domains (except where noted)

Governance – IT governance uses tools, processes, and methodologies that ensure an organization's IT products, services, and infrastructure align with its business strategy and goals. For courts performing software application development and support activities and/or providing services to any other courts, a Governance Board is required to provide operational oversight that includes, at minimum, prioritization of technology projects, approval of funding, technology compliance with Judicial Branch strategic initiatives, and engagement of affected internal and external stakeholders (as appropriate).

COT-Approved Changes 6/12/2025

Change Management – Technology change management provides structure around the accomplishment of hardware, software, and infrastructure changes with an eye toward communication and the user / customer impact of any change. A documented change management process must have approvers identified, notifications made, and signoffs obtained prior to undertaking a change. High impact changes should also have a documented roll-back plan should something go wrong.

Operational Management – Operations management coordinates resources of various kinds to deliver a product or an outcome., For courts providing local support beyond user/desktop/triage technology operations management requires incident and service request procedures, resource allocation and tracking, security incident response procedures, strategic planning, and an IT staffing level commensurate with the degree of locally-supported technology dependence of the court.

Management & Governance Details (All Tiers)	Currently Exists?	Gap Details / Exceptions
Formal **Change Management** must exist including: 1. Documented change management process; 2. Identification of required approvals for each type of change; 3. Notification matrix for communicating changes including the AOC, as applicable, including owners of any applications that depend on the changing application; 4. Sign-off from all approvers before production deployment; and 5. Roll-back plan (if possible) should the change need to be reversed after deployment.		
For courts performing application development and support activities and/or providing services to other courts, a **Governance Board** provides operational		

COT-Approved Changes 6/12/2025

Management & Governance Details (All Tiers)	Currently Exists?	Gap Details / Exceptions
oversight that includes, at minimum, prioritization of technology projects, approval of funding, technology compliance with Judicial Branch strategic initiatives, and engagement of impacted internal and external stakeholders (as appropriate). 1. Board membership includes Court Administrator, Presiding Judge, Clerk of the Court, and highest-level IT resource (Director or Manager) as an advisory member (not a voting member). Additional board members may be appropriate depending on the court size and structure. 2. The Board has authority to establish project or operational subcommittees charged with completing assigned tasks and preparing recommendations for delivery to the Board. 3. The Board is governed by a written charter that includes: ➢ Purpose ➢ Objectives ➢ Operational Subcommittees ➢ Meeting Schedule ➢ Board and Subcommittee Members Names		
Vendor Management skills are required for IT management who perform the following: 1. Review, edit, and approve any contract language that impacts or utilizes IT resources (network, systems, applications, hardware, etc.). 2. Write (or review) payment terms (ensure they are tied to milestones and payments are not made prior to service completion). 3. Write the IT language and service level / performance measurements for contracts that utilize IT resources or deliver IT services.		

Management & Governance Details (All Tiers)	Currently Exists?	Gap Details / Exceptions
4. Review all standard terms and conditions to ensure applicability to the contract. 5. Oversee IT vendor engagements and track vendor service delivery to performance measures. 6. Approve milestone payments based on service and contract deliverables.		
In courts providing support <u>beyond user/desktop/triage</u>, including performance of projects, formal **IT Operational Management** is in place. **Documented procedures are in place for handling REQUESTS and INCIDENTS.** 1. Procedures for IT response to "Requests" (non-production requests) along with a prioritization methodology for additional services or technology. ➢ The project scoping methodology includes the total hours (by resource type) with those hours costed (by resource type) estimated to complete the request plus any software/hardware costs and ongoing costs (licenses, hardware, IT hours). ➢ Perform an "impact" assessment. (e.g., what other technology or projects will be impacted if the new request is prioritized.) 2. Procedures for IT prioritization and response to production "incidents". This category includes documented service level agreements for each type of issue (critical, high, low). 3. Help Desk management tool (ticket based) in use by IT staff and customers to submit requests and incidents. Customers able to access the tool to track the status of their ticket(s).		

Management & Governance Details (All Tiers)	Currently Exists?	Gap Details / Exceptions
4. Monthly reporting of Help Desk activity to court administration that minimally reports monthly activity by category, time to close, total volume, etc. **Management has developed and maintained an IT staffing and resource allocation model that indicates resource availability schedules.** 1. IT management maintains a staffing allocation model that reflects assignment of resource priorities set by Governance Board during prioritization meetings. 2. Changes in priorities along with impact are easily and quickly discernable. **Monthly Tracking and Reporting of resource hours and costs** 1. A process for tracking IT resource hours and cost categorized by project and support area (Base Ops, Administration, etc.). 2. Hours and costs are consolidated into a monthly or quarterly management report. **Documented process for handling Cybersecurity Incident Response including** 1. Identification of a cybersecurity response team and assigned roles 2. Plan in place for identifying the area of intrusion and scope of the attack 3. Plan for isolation and remediation 4. Communication plan for notifying court management, judicial staff, and court staff 5. Post recovery / lessons learned plan documented and reviewed with Governance Board (see Security/Malware Incident Response section for details)		

COT-Approved Changes 6/12/2025

Management & Governance Details (All Tiers)	Currently Exists?	Gap Details / Exceptions
6. Test of plan not less than annually 7. Awareness training for court users includes reporting and escalation procedures		
Strategic Planning • Court leadership periodically carries out a strategic technology planning process and evaluates the current and future degrees of digital dependence for the court		
IT Staffing • Court leadership ensures sufficient IT staff exist for performing software development, testing, implementations, and ongoing maintenance, including technology management/oversight, as applicable for the degree of technology dependence in the court.		

Management & Governance Gap Closure Strategy & Timeline
Enter a closure plan and timeline for each gap documented in the table above.

Other Requirements for Reference
Arizona Judicial Branch Security Standards see https://www.azcourts.gov/cot/Enterprise-Architecture-Standards
Enterprise Architecture Standards Table see ACJA 1-505 and https://www.azcourts.gov/cot/Enterprise-Architecture-Standards
Distributed Module Development Requirements (Bolt-ons) see https://www.azcourts.gov/cot/Enterprise-Architecture-Standards
Paperless Court Operational Standards

COT-Approved Changes 6/12/2025

see ACJA 1-507 @ https://www.azcourts.gov/Portals/0/admcode/pdfcurrentcode/1-507_Amended_11-02-2016.pdf
Participation in Central Document Repository -- AO 2016-36 @ https://www.azcourts.gov/Portals/22/admorder/Orders16/2016-36.pdf