



JUDICIAL COUNCIL
OF CALIFORNIA

TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

Open to the Public (Cal. Rules of Court, rule 10.75(c)(1))
THIS MEETING WILL BE CONDUCTED BY TELECONFERENCE
THIS MEETING WILL BE RECORDED

Date: January 8, 2018
Time: 12:00 noon - 1:00 p.m.
Public Call-in Number: 1-877-820-7831 Passcode: 3511860

Meeting materials will be posted on the advisory body web page on the California Courts website at least three business days before the meeting.

Agenda items are numbered for identification purposes only and will not necessarily be considered in the indicated order.

I. OPEN MEETING (CAL. RULES OF COURT, RULE 10.75(C)(1))

Call to Order and Roll Call

Approval of Minutes

Approve minutes of the December 11, 2017 meeting.

II. PUBLIC COMMENT (CAL. RULES OF COURT, RULE 10.75(K)(2))

Written Comment

In accordance with California Rules of Court, rule 10.75(k)(1), public comments about any agenda item must be submitted by January 5, 2018, 12:00 noon. Written comments should be e-mailed to jctc@jud.ca.gov or mailed or delivered to 455 Golden Gate Avenue, San Francisco, CA 94102, attention: Jessica Craven Goldstein. Only written comments received by January 5, 2018, 12:00 noon will be provided to advisory body members prior to the start of the meeting.

III. DISCUSSION AND POSSIBLE ACTION ITEMS (ITEMS 1-4)

Item 1

Chair Report

Provide update on activities of or news from the Judicial Council, advisory bodies, courts, and/or other justice partners.

Presenter: Hon. Marsha G. Slough, Chair, Judicial Council Technology Committee

Item 2

Review of Information Technology Advisory Committee's (ITAC) Annual Agenda (Action Requested)

Review of the annual agenda for ITAC. The committee will then be asked to provide feedback and consider approval of the annual agenda.

Presenter: Hon. Sheila F. Hanson, Chair, Information Technology Advisory Committee

Item 3

Disaster Recovery Framework Workstream – Final Deliverables (Action Requested)

Review the workstream's final deliverables and decide whether to approve. Also, consider whether it is appropriate to recommend the deliverables to the Judicial Council for adoption. The deliverables include a Disaster Recovery Framework, Adaptable Disaster Recovery Plan, a "How to Guide," and budget change proposal (BCP) recommendations.

Presenters: Hon. Sheila Hanson, Chair, ITAC; Hon. Alan Perkins, Workstream Executive Co-Sponsor; Mr. Brian Cotta, Workstream Executive Co-Sponsor and Project Manager; and Mr. Michael Derr, Principal Manager, Judicial Council Information Technology

Item 4


Next Generation Hosting Strategy Workstream – Final Deliverables (Action Requested)

Review the workstream's final deliverables and decide whether to approve. Also, consider whether it is appropriate to recommend the deliverables to the Judicial Council for adoption. The deliverables include a Next Generation Hosting Framework, recommendations, and budgeting/roadmapping spreadsheet tools.

Presenters: Hon. Sheila Hanson, Chair, ITAC; Hon. Jackson Lucky, Workstream Executive Co-Sponsor; Mr. Brian Cotta, Workstream Executive Co-Sponsor; and Ms. Heather Pettit, Workstream Project Manager/Court Lead

A D J O U R N M E N T

Adjourn

The background features a large, faint, circular seal of the Judicial Council of Pennsylvania. The seal contains a central figure holding a scale and a sword, surrounded by various symbols of justice and law. The text "JUDICIAL COUNCIL OF PENNSYLVANIA" is visible around the perimeter of the seal, and the year "1926" is at the bottom.

Judicial Council Technology Committee Open Meeting

January 8, 2017

Call to Order and Roll Call

- Welcome
- Open Meeting Script

*Hon. Marsha G. Slough, Chair, Judicial Council Technology
Committee*



JUDICIAL COUNCIL
OF CALIFORNIA

Chair Report

Hon. Marsha G. Slough



JUDICIAL COUNCIL
OF CALIFORNIA

Action: Review of Information Technology Advisory Committee's (ITAC) Annual Agenda

*Hon. Sheila F. Hanson, Chair, Information Technology
Advisory Committee*



JUDICIAL COUNCIL
OF CALIFORNIA

Action: Disaster Recovery Framework Workstream – Final Deliverables

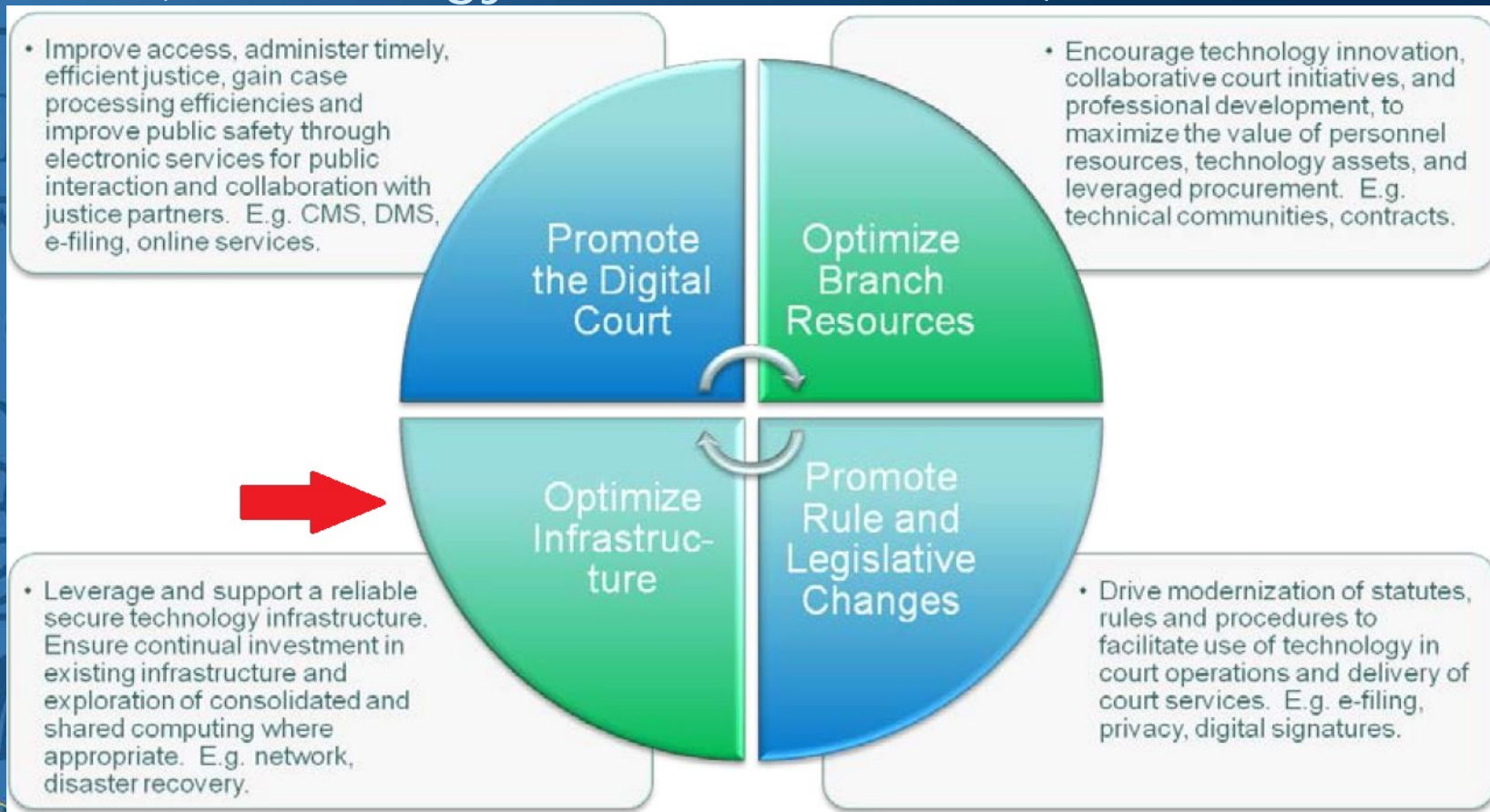
Hon. Sheila F. Hanson; Hon. Alan Perkins, Workstream Executive Co-Sponsor; Mr. Brian Cotta, Workstream Executive Co-Sponsor and Project Manager; and Mr. Michael Derr, Principal Manager, Judicial Council Information Technology



JUDICIAL COUNCIL
OF CALIFORNIA

History

Judicial Branch Technology Strategic & Tactical Plans (Technology Goals 2014-2018)



Charge & Scope

- Develop model disaster recovery guidelines, standard recovery times, and priorities for each of the major technology components of the branch.
- Develop a disaster recovery framework document that could be adapted for any trial or appellate court to serve as a court's disaster recovery plan.
- Create a plan for providing technology components that could be leveraged by all courts for disaster recovery purposes.



Workstream Partnerships

- Continuity of Operations Plan (COOP)
- ITAC: Next Generation Hosting Workstream
- ITAC: Information Systems Controls Framework



Involvement

29 participants

- Judge(s)
- Court Executive Officer(s)
- Judicial Council Information Technology Staff/Subject Matter Experts
- Court Information Officers and IT Staff



JUDICIAL COUNCIL
OF CALIFORNIA

Importance & Relevance

- Threats are at an all-time high, and rising. Constant threat of malware and cyberattacks makes it imperative that courts have back-up processes and recovery points that are isolated from their primary networks.
- Many courts are now (or will be) hosting their own case management systems.
- Courts are committed to IT for internal operational and public facing services.
- The Next Generation Hosting Workstream (ITAC-driven) is near completion and its work may change the “hosting” landscape and opportunities of what courts use and embrace today.



Comprehensive Analysis

- Detailed survey taken of Judicial Branch Entities (JBE's) on their current backup/DR solution.
- Aggressively changing landscape in regards to what courts need, what courts want and what technology is doing to change both of those!
 - The "hyper-converged" trend.....
 - The "cloud" trend....
 - Backups vs. high availability (both DR, but very different).



Feedback & Changes

- Documents were circulated for review by the Supreme Court, all appellate courts, and all superior courts.
- Few comments and suggestions were received from courts, but many courts voluntarily expressed appreciation and immediate interest in the final deliverables.
- Comments and feedback were considered and appropriate revisions were incorporated into the final documents.



Output / Documents Summary

1. "How to Use" Guide
(Completed: October 2017)
2. Disaster Recovery Framework: Recommendations and Reference Guide (Completed: October 2017)
3. Disaster Recovery Adaptable Template (Completed: October 2017)
4. Recommendation to ITAC to pursue a budget change proposal (BCP)
5. Recommendation for JC IT to review and edit the documents every (2) years.



Output 1: “How to Use” Guide

- Completion targeted for August 2017
- Provides high-level overview of the DR Recommendations and Reference Guide, as well as the DR Framework
- Assists JBE’s with establishing their own DR Framework through utilization of the documents provided as a result from this workstream
- Identifies the sections of the DR Recommendations and Reference Guide that are most applicable to JBE’s



Output 2: Recommendation & Reference Guide

- Output 2 Recommendation & Reference Guide
- Provides disaster recovery guidelines, recommendations, and general DR models relevant to JBE's
- Reviews fundamental DR concepts, technologies
 - Defines standard recovery times and definitions
 - Defines recovery priorities for each of the major technology components used in the branch
 - Details COTS* backup, site recovery, and high-availability solutions—already being used in the branch **as well as** other solutions capable of meeting the need

* *COTS = Commercial off-the-shelf*



Output 3: Adaptable DR Template

- Provides a baseline framework for JBE's to create their DR plan
- Formatted as an expandable template prompting courts to “fill in the blank”
- Planning to circulate to branch stakeholders to determine whether more or less information is desired



Output 4: BCP Recommendation

- A budget change proposal (BCP) is needed to assist courts with acquiring and implementing modern backup solutions and putting a DR plan in place
- Survey courts again prior to FY19-20 BCP cycle (Fall 2017) to determine updated needs for DR equipment and/or software
- Begin BCP development in early 2018
- Utilize existing—or establish new—leveraged purchase agreements (LPA's) depending on need(s)



Requested Action

- JCTC to provide any additional feedback at today's meeting
- If feedback received, incorporate
- Approve and recommend deliverables to the Judicial Council for adoption
- Pending Council approval, sunset Phase 1 of this workstream

Next Steps: Phase 2 Workstream

- Establish master agreements for cloud service providers (potential shared effort with DR Workstream initiative)
- Identify and implement a pilot program to test the branch Next-Generation Hosting Framework and report findings
- Establish the judicial branch support model for IT services
- Determine funding mechanism to transition courts to new hosting models
- Note: this is included in the 2018 ITAC Annual Agenda

Action: Next Generation Hosting Strategy Workstream – Final Deliverables

Hon. Sheila F. Hanson; Hon. Jackson Lucky, Workstream Executive Co-Sponsor; Mr. Brian Cotta, Workstream Executive Co-Sponsor; and Ms. Heather Pettit, Workstream Project Manager/Court Lead



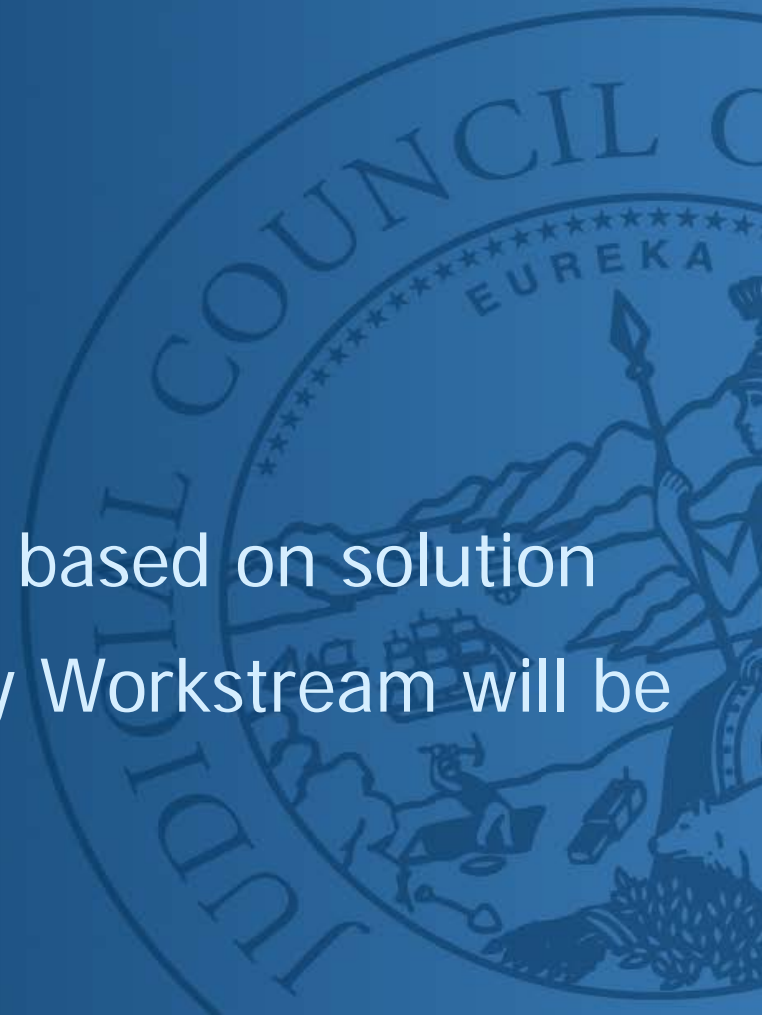
JUDICIAL COUNCIL
OF CALIFORNIA

Workstream Tasks

- Define industry best practices for hosting.
- Develop matrix of solutions with pros, cons, and example applications hosted and costs.
- Produce educational document with tool for use by courts in individual evaluation.
- Hold a one-day summit on hosting, if needed.
- Determine interest and support for possible solutions at branch level.
- Develop recommendation for branch-level hosting model.

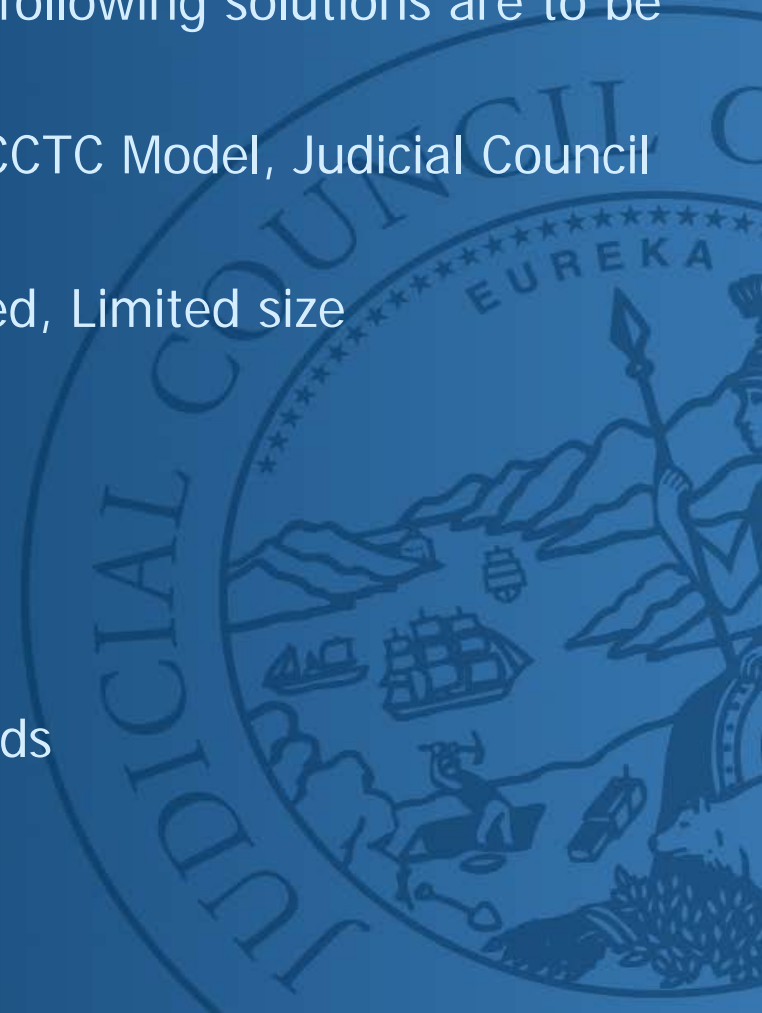
Workstream Assumptions

- All courts utilizing or moving to modern CMS within five years
- Facilities meet requirements
- Adequate internet bandwidth
- Funding is not an issue
- Resources will be determined based on solution
- Outputs for Disaster Recovery Workstream will be utilized



Data Center Options

- Based upon review of the Hosting and Disaster Recovery Assessments, as well as court ideas and strategies, the following solutions are to be investigated:
- Branch Data Center (Centrally Hosted) - CCTC Model, Judicial Council Managed, Court Managed
- Court Hosted Data Center - Court Managed, Limited size
 - Discussion of Regional Data Centers
 - Regional Applications
- Infrastructure as a Service (CLOUD)
- Software as a Service (CLOUD)
- Individual Courts – Hosting their own needs



Data Center Options Pros/Cons

Sample

Branch Data Center: Vendor Hosted (Current CCTC Model)

PROS	CONS
Full Service -Including desktop solutions	Cost Allocation - How?
Removes court pressure	Licenses are not included
Vendor does updates/anti-virus	Lack of control from the Court
Vendor controls Active Directory	Generally more costly
Vendor manages servers locally and at CCTC	No input in technology solutions being deployed at Data Center
Able to negotiate work with vendor for updates, hardware refresh, etc. - Madera, Lake and Modoc	Connectivity Costs
Hardware choices remain with Court	
No need for in-depth technical knowledge within the court	

New Framework Tools for Courts

1. Recommended Service Levels, Inventory Assets and Solutions
2. Use Inventory Checklist Template and Budget Planner
3. Use Technology Roadmap Template



Branchwide Recommended Hours & Service Level Definitions

Next Generation Hosting services should be 24/7 hours of operation.

- **Critical**: damage or disruption to a service that would stop court operations, public access or timely delivery of justice, with no viable work-around.
- **High**: damage or disruption to a service that would hinder court operations, public access or timely delivery of justice. A work-around is available, but may not be viable.
- **Medium**: damage or disruption to a specific service that would impact a group of users, but has a viable work-around.
- **Systems Support**: damage or disruption to a specific service that would not impact court operations, public access or timely delivery of justice and a viable work-around is available.

Branchwide Recommended Service Levels

SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours
Critical	Max Data Loss	1 hour	5 minutes
High	Max Time Recovery	6 hours	2 hours
High	Max Data Loss	1 hour	30 minutes
Moderate	Max Time Recovery	24 hours	24 hours
Moderate	Max Data Loss	1 Business day	1 Business day
Low	Max Time Recovery	48 hours	48 hours
Low	Max Data Loss	N/A	N/A

Branchwide Inventory Assets Sample

Requirement	Recommended Service Level
Systems	
Case Management	Critical
Jury Management	Critical
Website - Public Service Portal	Critical
E-filing	High
Communications/VoIP/Analog/Faxes	High
CCPOR/CLETS	High
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High
IVR/Call Routing	High
Electronic/Video Recording and Playback (FTR)	Moderate
Facilities Requirements- Assisted Listening (ADA)	Moderate
Building Access Controls	Moderate
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate
Court Call/Telephonic/Video appearance	Moderate
VRI - Video Remote Interpreting	Moderate
Physical Security- Video Surv.	Moderate
Video/Meeting/Conference Systems	Low

Branchwide recommended Solutions Sample

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Systems			
Case Management	✓	✓	✓
Jury Management	✓		✓
Website - Public Service Portal			✓
E-filing			✓
Communications/VoIP/Analog/Faxes	✓		
CCPOR/CLETS			✓
DMV- Justice Partners Branch and local (LAN/WAN- Connect)	✓		
IVR/Call Routing	✓		✓
Video/Meeting/Conference Systems			✓
Electronic/Video Recording and Playback (FTR)	✓		✓
Facilities Requirements- Assisted Listening (ADA)	✓		
Building Access Controls	✓		
E-Warrants_PC Dec/Ipad/Magistrate phone			✓
Court Call/Telephonic/Video appearance			✓
VRI - Video Remote Interpreting			✓
Physical Security- Video Surv.	✓		✓

Deliverables (in materials)

- Next-Generation Hosting Framework Guide
 - Data Center Options
 - Service-Level Definitions, Timeframes
 - Technology Assets and Service Levels
 - Recommended Solutions
 - Branchwide Recommendations
- Attachments
 - A. Recommended Service Levels, Inventory Assets, Solutions
 - B. Inventory Checklist Template
 - C. Technology Roadmap Template/Sample

Branch Comment

- Circulated deliverables to branch for comment October/November
- Generally supportive response
- Incorporated non-substantive revisions for clarity
- Full comment matrix provided in materials

Requested Action

- JCTC to provide any additional feedback at today's meeting
- If feedback received, incorporate
- Approve and recommend deliverables to the Judicial Council for adoption
- Pending Council approval, sunset Phase 1 of this workstream

Next Steps: Phase 2 Workstream

- Establish master agreements for cloud service providers (potential shared effort with DR Workstream initiative)
- Identify and implement a pilot program to test the branch Next-Generation Hosting Framework and report findings
- Establish the judicial branch support model for IT services
- Determine funding mechanism to transition courts to new hosting models
- Note: this is included in the 2018 ITAC Annual Agenda

Adjourn

All



JUDICIAL COUNCIL
OF CALIFORNIA



JUDICIAL COUNCIL OF CALIFORNIA

TECHNOLOGY COMMITTEE

www.courts.ca.gov/jctc.htm
jctc@jud.ca.gov

JUDICIAL COUNCIL TECHNOLOGY COMMITTEE

MINUTES OF OPEN MEETING

December 11, 2017

12:00 - 1:00 PM

Teleconference

Advisory Body Members Present: Hon. Marsha G. Slough, Chair; Hon. Gary Nadler, Vice-Chair; Hon. Kyle S. Brodie; Mr. Jake Chatters; Hon. Ming W. Chin; Ms. Audra Ibarra; Hon. Shama H. Mesiwala; and Ms. Andrea K. Rohmann

Advisory Body Members Absent: Ms. Rachel W. Hill

Liaison Members Present: Hon. Sheila F. Hanson

Others Present: Mr. Robert Oyung, Ms. Jessica Goldstein; Mr. Mark Dusman; Ms. Kathy Fink; Mr. David Koon; Ms. Jamel Jones; and Ms. Daphne Light

OPEN MEETING

Call to Order and Roll Call

The chair called the meeting to order, took roll call, and advised no public comments were received.

Approval of Minutes

The advisory body reviewed and approved the minutes of the October 16, 2017 meeting (with one abstention).

DISCUSSION AND ACTION ITEMS

Item 1

Chair Report

Update: Hon. Marsha Slough, Chair of the Judicial Council Technology Committee (JCTC), welcomed and thanked everyone for attending. Justice Slough reviewed the agenda for the meeting, as well as provided updates on recent meetings in which she and other members represented the JCTC or reported on the JCTC activities.

Item 2

Update/Report on Information Technology Advisory Committee (ITAC)

Update: Hon. Sheila F. Hanson, Chair of ITAC, provided an update and report on the activities of the advisory committee, its subcommittees, and its workstreams.

Action: The committee discussed the activities of ITAC and received the report.

Item 3

Update/Report on potential Technology Budget Change Proposals (BCPs)

Update: Mr. Robert Oyung, Chief Operating Officer for the Judicial Council, provided an update and report on the BCPs that are currently in progress of being developed and submitted, as well as an update related to developing potential BCP concepts for the next round of proposals (FY 19/20).

Action: The committee asked questions and then discussed potential technology BCP concepts for the upcoming fiscal year. The potential concepts will be added to an existing list for the committee to review and comment on at a future date.

Item 4

Update/Report on the Strategic and Tactical Plans for Technology

Update: Mr. Robert Oyung provided an update and report on the work related to the Strategic and Tactical Plans for Technology.

Action: The committee asked questions and received the report.

A D J O U R N M E N T

There being no further business, the meeting was adjourned.

Information Technology Advisory Committee (ITAC)
Annual Agenda¹—2018

Approved by Judicial Council Technology Committee: (Date Here)

I. COMMITTEE INFORMATION

Chair:	Hon. Sheila F. Hanson, Superior Court of California, County of Orange
Lead Staff:	Ms. Jamel Jones, Supervisor, Judicial Council, Information Technology
Committee's Charge/Membership: <i>Insert charge from Cal. Rules of Court, or the specific charge to the Task Force. Hyperlink rule number to courts public site. Insert total number of members and number of members by category.</i>	
<p><u>Rule 10.53. Information Technology Advisory Committee</u> of the California Rules of Court states the charge of the Information Technology Advisory Committee. The committee makes recommendations to the council for improving the administration of justice through the use of technology and for fostering cooperative endeavors to resolve common technological issues with other stakeholders in the justice system. The committee promotes, coordinates, and acts as executive sponsor for projects and initiatives that apply technology to the work of the courts.</p> <p><u>Rule 10.53. Information Technology Advisory Committee</u> sets forth additional duties of the committee.</p> <p>The ITAC currently has 23 members. The ITAC website provides the composition of the committee.</p>	

¹ The annual agenda outlines the work a committee will focus on in the coming year and identifies areas of collaboration with other advisory bodies and the Judicial Council staff resources.

All proposed projects for the year are included on the Annual Agenda, as follows:

Futures Commission Directives

- **Intelligent Chat (Phase 1) (new):** Explore and make recommendations to the Judicial Council on the potential for a pilot project using intelligent chat Technology to provide information and self-help services.
- **Voice-to-Text Language Services Outside the Courtroom (Phase 1) (new):** Explore available technologies and make recommendations to the Judicial Council on the potential for a pilot project using voice-to-text language interpretation service counters and in self-help centers. The goal of the pilot will be to determine next steps with this technology. Potential next step outcomes may be to continue to research the technology within a lab environment while it matures, to pilot at one court for a specific use case, or to pilot at multiple courts for multiple use cases.
- **Remote Video Appearances for Most Non-Criminal Hearings (Phase 1) (new):** The feasibility of and resource requirements for developing and implementing a pilot to allow remote appearances by parties, counsel, and witnesses for most noncriminal court proceedings.

Workstreams

- **Tactical Plan for Technology Update (new):** Update Tactical Plan for Technology for Effective Date 2019-2020.
- **Video Remote Interpreting Pilot (continued):** Consult As Requested and Implement Video Remote Interpreting Pilot (VRI) Program.
- **E-Filing Strategy (continued):** Establish EFM Master Agreements, Develop EFSP Certification; Report on E-Filing Implementations, Standards, and Cost-Recovery.
- **Identity and Access Management Strategy (new):** Develop a branch identity management strategy; consult on selection of a provider.
- **Self-Represented Litigants E-Services (continued):** Develop Requirements and a Request for Proposal (RFP) for Establishing Online Branchwide Self-Represented Litigants E-Services.
- **IT Community Development (new):** Expand Collaboration and Professional Development within the Branch IT Community.
- **Intelligent Forms Strategy: Research & Scope (Phase 1) (continued):** Investigate options for modernizing the electronic format and delivery of Judicial Council forms.
- **Digital Evidence: Assessment (Phase 1) (continued):** Investigate, assess, and report on statutes, rules, business practice, and technical standards related to digital evidence.
- **Data Analytics: Assessment and Report (Phase 1) (new):** Research, scope, and recommend a data analytics strategy for the branch. Investigate possible policies, technologies, and processes to help the branch utilize data analytics to improve business effectiveness. Assess priorities for data collection and present findings.

- **Disaster Recovery Framework (Phase 1):** Document and Adopt a Court Disaster Recovery Framework – *to sunset March 2018.*
- **Disaster Recovery Framework Pilot (Phase 2) (new):** Implement Branch Disaster Recovery Pilot Program, Master Agreement, Knowledge-Sharing; Develop BCP.
- **Next- Generation Hosting Strategy (Phase 1):** Assess Alternatives for Transition to a Next-Generation Branchwide Hosting Model – *to sunset March 2018.*
- **Next-Generation Hosting Strategy Pilot (Phase 2) (new):** Pilot the Branch Next-Generation Hosting Strategy Framework, Establish Master Agreements, Establish Support and Funding Models.

Subcommittees²:

- Rules & Policy Subcommittee
 - Modernize Trial Court Rules
 - Standards for E-Signatures
 - Remote Access Rules for Government Entities, Parties, Attorneys
 - Standards for Electronic Court Records as Data
 - Privacy Resource Guide (trial court)
- Joint Appellate Technology Subcommittee (JATS)
 - Modernize Appellate Court Rules
 - Rules Regarding Certification of Electronic Records, E-Signatures, and Paper Copies
 - Input on Appellate Document Management System
 - Privacy Resource Guide (appellate)
- Joint Ad Hoc Rules for Remote Access to Records Subcommittee

² California Rules of Court, rule 10.30 (c) allows an advisory body to form subgroups, composed entirely of current members of the advisory body, to carry out the body's duties, subject to available resources, with the approval of its oversight committee.

II. COMMITTEE PROJECTS

New Project (Ending 2018)	
1.1 Futures Commission Directive: Intelligent Chat (Phase 1)	Priority 1 ³
<p>Project Summary: The committee was directed by the Chief Justice to explore and make recommendations to the council on the potential for a pilot project using intelligent chat technology to provide information and self-help services.</p> <p>Key Objectives⁴: Included in the Phase 1 of this project:</p> <ul style="list-style-type: none"> (a) Identify and monitor a series of court proofs of concepts (POCs) to assess technology readiness for various use cases (e.g., Court of Appeal, E-Filing, Self-Help). (b) Identify key performance indicators and benchmark before/after success. (c) Capture learnings and report findings. (d) Update Phase 2 of workplan based on results. (e) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly. <p>Origin of Project: Chief Justice directive from the Futures Commission recommendations report.</p> <p>Status/Timeline: May 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Sponsor: Hon. Michael Groch <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager//Coordinator: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Court CIOs 	

³ For non-rules and forms projects, select priority level 1 (must be done) or 2 (should be done).

⁴ A key objective is a strategic aim, purpose, or “end of action” to be achieved for the coming year.

New Project (Ending 2018)	
1.2 Futures Commission Directive: Voice-to-Text Language Services Outside the Courtroom (Phase 1)	<i>Priority 1</i>
<p>Project Summary: The committee is directed to explore available technologies and make recommendations to the Judicial Council on the potential for a pilot project using voice-to-text language interpretation services at court filing and service counters and in self-help centers. The goal of the lab pilot will be to determine next steps with this technology. Potential next step outcomes may be to continue to research the technology within a lab environment while it matures, to pilot at one court for a specific use case, or to pilot at multiple courts for multiple use cases.</p> <p>Key Objectives: Included in the Phase 1 of this project:</p> <ul style="list-style-type: none"> (a) Setup a technical lab environment at the Judicial Council or a local court to test the technical recommendations of the Futures Commission for this initiative. (b) Pilot various voice-to-text language services in a lab environment. will allow for exposure to more technologies and shorter learning cycles than if a specific technology is deployed at a court for piloting. (f) Capture learnings and draft a white paper report on the lessons learned, findings, and recommendations for next steps. (g) Update Phase 2 of workplan based on results. (h) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly. <p>Origin of Project: Chief Justice directive from the Futures Commission recommendations report.</p> <p>Status/Timeline: July 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> ○ <i>ITAC:</i> Sponsors: Hon. James Mize, Ms. Heather Pettit Court Lead: TBD, Project Manager/Coordinator: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Court CIOs, pilot courts, Innovation Grant awardees 	

New Project (Ending 2018)	
1.3 Futures Commission Directive: Remote Video Appearances for Most Non-Criminal Hearings (Phase 1)	<i>Priority 1</i>
<p>Project Summary: The feasibility of and resource requirements for developing and implementing a pilot project to allow remote appearances by parties, counsel, and witnesses for most noncriminal court proceedings.</p> <p>Key Objectives: Included in the Phase 1 of this project:</p> <ul style="list-style-type: none"> (a) Identify and conduct a mock remote video hearing using a web conferencing system for a specific hearing type (e.g., Civil - Small Claims) as a Proof of Concept (POC) in a court. Include one or more mock hearings of the selected hearing type. (b) Capture learnings and report findings. (c) Update Phase 2 of workplan based on results. (d) Seek approval from ITAC and the JCTC to conclude Phase 1 and initiate Phase 2; amend the annual agenda accordingly. <p>Origin of Project: Chief Justice directive from the Futures Commission recommendations report.</p> <p>Status/Timeline: July 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Sponsor: Hon. Samantha Jessner <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager/Coordinator: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Court CIOs, pilot courts, and Innovation Award Grantees 	

New Workstream (Ending 2019)	
2. Tactical Plan for Technology Update	<i>Priority 1</i>
<p>Project Summary: Update Tactical Plan for Technology for Effective Date 2019-2020.</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Initiate workstream, including formation of membership and conduct orientation/kickoff meeting. (b) Review, gather input, and update the Tactical Plan for Technology. (c) Circulate the draft plan for branch and public comment; revise as needed. (d) Finalize, and seek approval by the JCTC and the Judicial Council; thereafter, formally sunset the workstream. <p>Origin of Project: Specific charge of ITAC per Rule 10.53 (b)(8).</p> <p>Status/Timeline: April 2019</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsor: Hon. Sheila Hanson <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Broad input from the branch and the public. 	

Existing Workstream (End 2018)

3. Video Remote Interpreting (VRI) Pilot

Priority 2

Project Summary: Consult As Requested and Implement Video Remote Interpreting Pilot (VRI) Program

Key Objectives:

In cooperation and under the direction of the Language Access Plan Implementation Task Force (LAPITF) Technological Solutions Subcommittee (TSS):

- (a) Support implementation of the Assessment Period of the VRI pilot program (including kickoff, court preparations, site visits, and deployment), as requested.
- (b) Review pilot findings; validate, refine, and amend, if necessary, the technical standards.
- (c) Identify whether new or amended rules of court are needed (and advise the Rules & Policy Subcommittee for follow up).
- (d) Consult and collaborate with LAPITF, as needed, in preparing recommendations to the Judicial Council on VRI implementations.
- (e) Coordinate and plan with JCIT regarding operational support, if appropriate.

Origin of Project: Tactical Plan for Technology 2017-2018; continuation of project from Annual Agenda 2015-2017.

Status/Timeline: September 2018

Resources:

- *Joint Workstream:*
 - *ITAC:* Sponsor: Hon. Samantha Jessner (ITAC)
 - *Language Access Plan Implementation Task Force (LAPITF):* Sponsor: Hon. Terence Bruiniers, Chair of LAPITF Technological Solutions Subcommittee (TSS)
 - *Court Lead:* n/a, *Project Manager:* Ms. Lisa Crownover
- *Judicial Council Staffing:* Court Operations Special Services Office, Information Technology
- *Collaborations:* LAPITF TSS; CEAC, TCPJAC, and their Joint Technology Subcommittee; Court CIOs

Existing Workstream (Ending 2018)	
4. E-Filing Strategy	<i>Priority 1</i>
<p>Project Summary: Establish EFM Master Agreements, Develop EFSP Certification; Report on E-Filing Implementations, Standards, and Cost-Recovery</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Finalize master agreements with the three (3) E-Filing Managers (EFMs) selected to provide services. (b) Develop the E-Filing Service Provider (EFSP) selection/certification process. (c) Monitor the progress of EFSP accessibility compliance. (d) Develop the roadmap for an e-filing deployment strategy, approach, and branch solutions/alternatives. (e) Report on the plan for implementation of the approved NIEM/ECF standards, including effective date, per direction of the Judicial Council at its June 24, 2016 meeting. (f) Consult and report on the implementation of the court cost recovery fee that will support the statewide e-filing program. (g) Coordinate and plan with JCIT regarding operational support of the ongoing e-filing program being funded through the court cost-recovery fee. (h) At the completion of these objectives and with the approval of the JCTC, formally sunset the workstream. <p>Origin of Project: Tactical Plan for Technology 2017-2018; carryover project from 2015-2017 Annual Agenda with evolving objectives; also, directive from June 2016 Judicial Council meeting.</p> <p>Status/Timeline: December 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream: Sponsor: Hon. Sheila Hanson <ul style="list-style-type: none"> ○ Court Lead: Mr. Snorri Ogata, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology, Legal Services • <i>Collaborations:</i> Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee 	

New Workstream (Ending 2019)	
5. Identity and Access Management Strategy	<i>Priority 1</i>
<p>Project Summary: Develop a Branch Identity Management Strategy; Select a Provider to Enable Single Sign-on</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Develop and issue an RFP for a statewide identity management service/provider; identify and select. (b) Develop the roadmap for a branch identity management strategy and approach. (c) Determine policies and processes for identity management (including proofing and access management). (d) Ensure linkage and alignment with other branchwide initiatives such as E-Filing, SRL Portal, Next Generation Hosting, CMS Migration and Deployment. (e) Coordinate and plan with JCIT regarding operational support, if appropriate. <p>Origin of Project: Previously, this was a sub-task of the e-filing initiative. The item was promoted to its own annual agenda initiative given its many touchpoints with other workstreams (including Self-Represented E-Services, Next-Generation Hosting, E-filing Strategy, etc.). Tactical Plan for Technology 2017-2018.</p> <p>Status/Timeline: January 2019</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream: Sponsor: Mr. Snorri Ogata <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager: Ms. Kathleen Fink • <i>Judicial Council Staffing:</i> Information Technology, Legal Services, Branch Accounting and Procurement • <i>Collaborations:</i> Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee 	

Existing Workstream (Ending 2019)

6. Self-Represented Litigants (SRL) E-Services

Priority 1

Project Summary: Develop Requirements and a Request for Proposal (RFP) for Establishing Online Branchwide Self-Represented Litigants (SRL) E-Services

Key Objectives:

- (a) Provide input for, and track, a SRL E-Services Budget Change Proposal (BCP) process for FY18-19 funding.
- (b) Develop requirements for branchwide SRL e-capabilities to facilitate interactive FAQ, triage functionality, and document assembly to guide SRLs through the process, and interoperability with the branchwide e-filing solution. The portal will be complementary to existing local court services.
- (c) Determine implementation options for a branch-branded SRL E-Services website that takes optimal advantage of existing branch, local court, and vendor resources.
- (d) Develop and issue a request for proposal (RFP) or other solicitation, as needed, to support the implementation of the branchwide e-services portal.
- (e) Coordinate and plan with JCIT regarding operational support, if appropriate.

Note: In scope for 2018 is the submission and tracking of a budget change proposal (BCP) and development of an RFP; out of scope is the actual implementation.

Origin of Project: Tactical Plan for Technology 2017-2018; next phase of project following feasibility and desirability assessment (2015-2016).

Status/Timeline: April 2019

Resources:

- **ITAC:** Workstream, Sponsors: Hon. James Mize, Hon. Michael Groch
 - Court Lead: Mr. Brett Howard, Project Manager: TBD
- **Judicial Council Staffing:** Information Technology, Center for Families, Children and the Courts (CFCC)
- **Collaborations:** Alternative Dispute Resolution (ADR) Subcommittee of the Civil and Small Claims Advisory Committee (C&SCAC) standing subcommittee; Advisory Committee Providing Access & Fairness; CEAC, TCPJAC, and their Joint Technology Subcommittee; CITMF, the Southern Regional SRL Network, and the California Tyler Users Group (CATUG)

New Workstream (Ending 2018)	
7. IT Community Development	<i>Priority 1</i>
<p>Project Summary: Expand Collaboration and Professional Development within the Branch IT Community</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Survey the courts to identify (i) their interest in exploring opportunities to share key technical resources and (ii) IT leadership and resource development needs and priorities; report findings. (b) Assess court CEO/CIO interest in an IT peer consulting program and develop recommendations. (c) Partner with CJER to develop and implement an annual plan for keeping judicial officers, CEO's, and CIO's abreast of technology trends. (d) Identify, prioritize, and report on collaboration needs and tools for use within the branch. (e) Evaluate and prioritize possible technologies to improve advisory body and workstream meeting administration; pilot recommended solutions with the committee. (f) Coordinate and plan with JCIT regarding operational support, as appropriate. <p>Origin of Project: Tactical Plan for Technology 2017-2018</p> <p>Status/Timeline: December 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsors: Hon. Alan Perkins, Ms. Jeannette Vannoy <ul style="list-style-type: none"> ○ Court Lead: Ms. Jeannette Vannoy, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee 	

Existing Workstream (Ending 2018)

8. Intelligent Forms Strategy: Research & Scope (Phase 1)

Priority 2

Project Summary: Investigate Options for Modernizing the Electronic Format and Delivery of Judicial Council Forms

Key Objectives:

Investigate, prioritize and scope a project, including:

- (a) Evaluate Judicial Council form usage (by courts, partners, litigants) and recommend a solution that better aligns with CMS operability and better ensures the courts' ability to adhere to quality standards and implement updates without reengineer.
- (b) Address form security issues that have arisen because of the recent availability and use of unlocked Judicial Council forms in place of secure forms for e-filing documents into the courts; seek solutions that will ensure the forms integrity and preserves legal content.
- (c) Investigate options for redesigning forms to take advantages of new technologies, such as document assembly technologies.
- (d) Investigate options for developing standardized forms definitions and delivery methods that would enable forms to be efficiently electronically filed into the various modern CMSs across the state.
- (e) Explore the creation and use of court generated text-based forms as an alternative to graphic forms.
- (f) Investigate whether to recommend development of a forms repository by which courts, forms publishers, and partners may readily and reliably access forms in alternate formats.
- (g) Develop recommendations for a potential BCP to support proposed solutions. (Note: Drafting a BCP would be a separate effort.)
- (h) Initiate Phase 2 of the workstream, based on the recommendations.

Origin of Project: Proposal submitted jointly by Judge Freedman and Judge Lucky, ITAC members to address concerns raised by courts and council legal/forms staff.

Status/Timeline: February 2018

Resources:

- *ITAC:* Workstream, Sponsor: Hon. Jackson Lucky
 - Court Lead: TBD, Project Manager: Ms. Camilla Kieliger
- *Judicial Council Staffing:* Information Technology, Legal Services, Center for Children, Families and the Courts
- *Collaborations:* Workstream members; CEAC, TCPJAC, and their Joint Technology Subcommittee

Existing Workstream (Ending 2018)	
9. Digital Evidence: Assessment (Phase 1)	<i>Priority 2</i>
<p>Project Summary: Investigate, Assess, and Report on Statutes, Rules, Business Practice, and Technical Standards Related to Digital Evidence</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Review existing statutes and rules of court to identify impediments to use of digital evidence and opportunities for improved processes. (b) Survey courts for existing business practices and policies regarding acceptance and retention of digital evidence. (c) Survey courts and justice system groups regarding possible technical standards and business practices for acceptance and storage of digital evidence. (d) Report findings to ITAC and provide recommendations on next steps. (e) Coordinate and plan with JCIT regarding operational support, if appropriate. <p>Origin of Project: Tactical Plan for Technology 2017-2018</p> <p>Status/Timeline: July 2018</p> <p>Resources</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsor: Hon. Kimberly Menninger <ul style="list-style-type: none"> ○ Court Leads: Ms. Mary Garcia-Whalen, Ms. Deni Butler; Project Manager: Ms. Kathleen Fink • <i>Judicial Council Staffing:</i> Information Technology, Legal Services • <i>Collaborations (Advisory Committees and External):</i> Workstream members; CEAC, TCPJAC 	

New Workstream (Ending 2018)	
10. Data Analytics: Assess and Report (Phase 1)	<i>Priority 1</i>
<p>Project Summary: Research and Recommend a Data Analytics Strategy</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Research, scope, and recommend a data analytics strategy for the branch (e.g., this may include gaining case processing and resource data). (b) Investigate possible policies, processes, and technologies to help the branch utilize data analytics to improve business effectiveness. (c) Assess priorities for data collection and present findings to ITAC. (d) Identify possible data analytical tools and templates. <p>Origin of Project: Topic resulted from a brainstorm of ideas conducted with ITAC and the court CIOs.</p> <p>Status/Timeline: January 2019</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsors: Hon. Tara Desautels, Mr. David Yamasaki <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology, Criminal Justice Services, Judicial Branch Statistical Information System (JBSIS) Program, Center for Families, Children, and the Courts • <i>Collaborations:</i> CIOs, CEAC, TCPJAC, appellate group representation 	

Existing Workstream (Ending 2018)	
11.1 Disaster Recovery (DR) Framework Phase 1	<i>Priority 1</i>
<p>Project Summary: Document and Adopt a Court Disaster Recovery Framework</p> <p>In 2017, the workstream finalized the <i>Disaster Recovery Framework Guide</i> consisting of model DR guidelines, standard recovery times, and priorities; also, a model/adaptable DR Plan for use by courts and related “how to” guide. The following objectives are intended to close out this work, and effectively transition the project to Phase 2.</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Coordinate with JCIT to define and plan the operational or ongoing support needed to maintain the <i>Disaster Recovery Framework Guide</i> and associated deliverables. (b) Seek approval of the proposed framework from the JCTC and adoption by the Judicial Council; thereafter, formally sunset this phase of the workstream. <p>Origin of Project: Tactical Plan for Technology 2017-2018; next phase of project following 2015 assessment.</p> <p>Status/Timeline: March 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsors: Hon. Alan Perkins, Mr. Brian Cotta <ul style="list-style-type: none"> ○ Court Lead/Project Manager: Mr. Brian Cotta • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Workstream members representing various court sizes; CEAC, CITMF 	

New Workstream (Ending 2019)	
11.2 Disaster Recovery (DR) Framework Phase 2	Priority 1
<p>Project Summary: Implement Branch Disaster Recovery (DR) Pilot Program, Master Agreement, Knowledge-Sharing; Develop BCP</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Leverage the innovation grant awarded to the Superior Court of Monterey County for a Cloud DR Pilot Program. (b) Recommend a list of critical technology services that make business sense for cloud-based recovery adoption. (c) Establish a cloud DR master agreement with a short list of cloud service providers for judicial branch entities/courts to leverage. (d) Publish design solution templates using technologies and solutions from vendors selected in the cloud DR master agreement. (e) Host knowledge sharing sessions for interested judicial branch entities/courts (including tools to estimate cost for deploying recovery solution using a particular cloud service provider; and Monterey solution case study). (f) Provide input to JCIT that will be used in drafting a BCP to fund a pilot group of courts interested in implementing Cloud-based DR for critical technology services (see (b)). (g) Coordinate and plan with JCIT regarding operational support, if appropriate. <p>Origin of Project: Tactical Plan for Technology 2017-2018; next phase of project following framework adoption.</p> <p>Status/Timeline: June 2019</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream: Sponsor: Mr. Paras Gupta <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Workstream members; pilot courts; CEAC, CITMF 	

Existing Workstream (Ending 2018)	
12.1 Next Generation Hosting Strategy Phase 1	Priority 1
<p>Project Summary: Assess Alternatives for Transition to a Next-Generation Branchwide Hosting Model</p> <p>In 2017, the workstream finalized the <i>Next-Generation Hosting Framework Guide</i>, recommendations, and associated templates. The following objectives are intended to close out this work, and effectively transition the project to Phase 2.</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Coordinate with JCIT to define and plan the operational or ongoing support needed to maintain the <i>Next-Generation Hosting Framework Guide</i> and associated deliverables. (b) Seek approval of the proposed framework from the JCTC and adoption by the Judicial Council; thereafter, formally sunset this phase of the workstream. <p>Origin of Project: Tactical Plan for Technology 2017-2018; assessment conducted in 2015; workstream initiated in 2016-2017 Annual Agendas.</p> <p>Status/Timeline: March 2018</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsors: Hon. Jackson Lucky, Mr. Brian Cotta <ul style="list-style-type: none"> ○ Court Lead/Project Manager: Ms. Heather Pettit • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> CEAC, TCPJAC, and their Joint Technology Subcommittee; CITMF 	

New Workstream (Ending 2019)	
12.2 Next-Generation Hosting Strategy Phase 2	Priority 1
<p>Project Summary: Pilot the Branch Next-Generation Hosting Strategy Framework, Establish Master Agreements, Establish Support and Funding Models</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Identify and implement a pilot program to test the branch Next-Generation Hosting Framework and report findings. Pilot courts to include those with available funding; also, will include collaboration with courts already in progress of transitioning to next-generation hosting. (b) Establish master agreements for cloud service providers. (Potential shared effort with DR Workstream initiative.) (c) Establish the judicial branch support model for IT services. (d) Determine funding mechanism to transition courts to new hosting models; this includes exploring a potential Budget Change Proposal (BCP). <p>Origin of Project: Tactical Plan for Technology 2017-2018</p> <p>Status/Timeline: July 2019</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Workstream, Sponsors: Ms. Heather Pettit, Mr. Brian Cotta <ul style="list-style-type: none"> ○ Court Lead: TBD, Project Manager: TBD • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> CITMF 	

Ongoing Project	
13.1 Modernize Trial Court Rules	Priority 1⁵
<p>Project Summary: Modernize Rules of Court for the Trial Courts to Support E-Business</p> <p>In collaboration with other advisory committees, continue review of rules and statutes in a systematic manner and develop recommendations for more comprehensive changes to align with modern business practices (e.g., eliminating paper dependencies).</p> <p><u>Proposals within the scope of this item include:</u></p> <ul style="list-style-type: none"> (a) Proposals to create and amend rules to conform to legislation enacted in 2017. For example, new provisions of Code of Civil Procedure section 1010.6 expressly require the Judicial Council to adopt rules of court related to disability access and electronic signatures for documents signed under penalty of perjury. The new provisions also require express consent for electronic service, which will require a rule amendment, and creation of a form for withdrawal of consent. (b) Proposals based on suggestions from the public such as revising definitions and addressing a barrier to indigent users accessing services of electronic filing service providers. (c) Proposals for technical amendments to amend rules language that is obsolete or otherwise unnecessary. <p>Origin of Project: Tactical Plan for Technology 2017-2018. Standing item on the agenda.</p> <p>Status/Timeline: Ongoing</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Rules & Policy Subcommittee, Chair, Hon. Peter Siggins • <i>Judicial Council Staffing:</i> Legal Services, Information Technology, Office of Governmental Affairs, • <i>Collaborations:</i> ITAC Joint Appellate Technology Subcommittee; Appellate Advisory Committee, Civil & Small Claims, Criminal Law, Traffic, Family and Juvenile Law, and Probate and Mental Health advisory committees; TCPJAC, CEAC and their Joint Technology, Rules, and Legislative Subcommittees 	

⁵ For rules and forms proposals, the following priority levels apply: 1(a) Urgently needed to conform to the law; 1(b) Urgently needed to respond to a recent change in the law; 1(c) Adoption or amendment of rules or forms by a specified date required by statute or council decision; 1(d) Provides significant cost savings and efficiencies, generates significant revenue, or avoids a significant loss of revenue; 1(e) Urgently needed to remedy a problem that is causing significant cost or inconvenience to the courts or the public; 1(f) Otherwise urgent and necessary, such as a proposal that would mitigate exposure to immediate or severe financial or legal risk; 2(a) Useful, but not necessary, to implement statutory changes; 2(b) Helpful in otherwise advancing Judicial Council goals and objectives.

One-Time Project (Ending 2019)	
13.2 Standards for E-Signatures	<i>Priority 2</i>
<p>Project Summary: Develop Standards for Electronic Signatures on Documents Filed by Parties and Attorneys</p> <p>Key Objective:</p> <p>(a) CEAC Records Management Subcommittee to develop standards governing electronic signatures for documents filed into the court with input from the Court Information Technology Managers Forum (CIOs). Rules & Policy Subcommittee to review.</p> <p>Origin of Project: Tactical Plan for Technology 2017-2018; continued from 2014-2017 annual agendas. Recommendation by Department of Child Support Services and attorney, Tim Perry.</p> <p>Status/Timeline: December 2018, effective January 2019 (2 years)</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Rules & Policy Subcommittee, Chair: Hon. Peter Siggins • <i>Judicial Council Staffing:</i> Legal Services, Information Technology • <i>Collaborations:</i> ITAC Joint Appellate Technology Subcommittee; CEAC Subcommittee on Records Management, CEAC, TCPJAC, and their Joint Rules and Legislative Subcommittees; Civil & Small Claims Advisory Committee, and the Court Information Technology Managers Forum (CITMF) 	

One-Time Project (Ending 2019)	
13.3 Remote Access Rules for Government Entities, Parties, Attorneys	<i>Priority 1</i>
<p>Project Summary: Develop Rule Proposal to Facilitate Remote Access to Trial Court Records By State and Local Government Entities, Parties, Parties’ Attorneys, and Court-Appointed Persons</p> <p>Key Objective:</p> <p>(a) Lead the Joint Ad Hoc Subcommittee on Remote Access to amend trial court rules to facilitate remote access to trial court records by state and local government entities, parties, parties’ attorneys, and certain court-appointed persons.</p> <p>Origin of Project: Carryover from 2016-2017 Annual Agenda. Rules and Policy Subcommittee discussion/recommendation. Currently, the trial court rules recognize remote electronic access of trial court records in criminal cases and certain civil cases by parties, their attorneys, and persons or entities authorized by statute or rule, but the rules do not make specific provisions for the access by these persons or entities. This rules proposal would facilitate remote access to trial court records by state and local government entities, parties, parties’s attorneys, and certain court-appointed persons.</p> <p>Status/Timeline: December 2018, effective January 2019 (2 years)</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Rules & Policy Subcommittee, Chair: Hon. Peter Siggins • <i>Judicial Council Staffing:</i> Legal Services, Information Technology • <i>Collaborations:</i> Appellate Advisory Committee, Criminal Law Advisory Committee, Civil and Small Claim Advisory Committee, Probate and Mental Health Advisory Committee, Advisory Committee on Providing Acces and Fairness, Trial Court-State Court Forum, CEAC, Family & Juvenile Law and Traffic Law Advisory Committee. 	

One-Time Project (Ending 2018)	
13.4 Standards for Electronic Court Records as Data	Priority 1
<p>Project Summary: Develop Standards for Electronic Court Records Maintained as Data</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) CEAC Records Management Subcommittee -- in collaboration with the Data Exchange Workstream governance body -- to develop standards and proposal to allow trial courts to maintain electronic court records as data in their case management systems to be included in the "Trial Court Records Manual" with input from the Court Information Technology Managers Forum (CITMF). Rules & Policy Subcommittee to review. (b) Determine what statutory and rule changes may be required to authorize and implement the maintenance of records in the form of data; develop proposals to satisfy these changes. <p>Origin of Project: Carryover from 2016-2017 Annual Agenda. Court Executives Advisory Committee (CEAC); Government Code section 68150 provides that court records may be maintained in electronic form so long as they satisfy standards developed by the Judicial Council. These standards are contained in the Trial Court Records Manual. However, the current version of the manual addresses maintaining electronic court records only as documents, not data.</p> <p>Status/Timeline: December 2018 (2 years)</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Rules & Policy Subcommittee, Chair: Hon. Peter Siggins • <i>Judicial Council Staffing:</i> Information Technology, Legal Services • <i>Collaborations:</i> Data Exchange governance body (TBD); CEAC, TCPJAC, and their Joint Technology Subcommittee 	

One-Time Project (Ending 2018)	
13.5 Privacy Resource Guide	Priority 2
<p>Project Summary: Develop Branch and Model Court Privacy Resource Guide on Electronic Court Records and Access in Trial and Appellate Courts</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Continue development of a comprehensive statewide privacy resource guide addressing, among other things, electronic access to court records and data, to align with both state and federal requirements. (b) Continue development of court privacy resource guide, outlining the key requirements, contents, and provisions for courts to address within its specific privacy policy. <p>Origin of Project: Tactical Plan for Technology 2017-2018; carryover from 2014-2017 Annual Agenda. Code Civ. Proc., § 1010.6 (enacted in 1999) required the Judicial Council to adopt uniform rules on access to public records; subsequently the rules have been amended in response to changes in the law and technology, requests from the courts, and suggestions from members of ITAC (formerly, CTAC), the bar, and the public.</p> <p>Status/Timeline: December 2018 (2 years)</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Joint effort between the Rules & Policy and Joint Appellate Technology Subcommittees, Lead: Hon. Julie Culver • <i>Judicial Council Staffing:</i> Legal Services, Information Technology • <i>Collaborations:</i> Identity Management Working Group; Appellate Advisory Committee, CEAC, TCPJAC, and their Joint Technology Subcommittee; Criminal Law Advisory Committee, and the Department of Justice 	

Ongoing Project	
14.1 Modernize Appellate Court Rules	<i>Priority 2(b)</i> ⁶
<p>Project Summary: Modernize Appellate Court Rules to Support E-Filing and E-Business</p> <p>Review appellate rules to ensure consistency with e-filing practice; evaluate, identify and prioritize potential rule modifications where outdated policy challenges or prevents e-business. Consider rule modifications to remove requirements for paper versions of documents (by amending individual rules or by introducing a broad exception for e-filing/e-service). Consider potential amendments to rules governing online access to court records for parties, their attorneys, local justice partners, and other government agencies. This will be the third year of work on this multi-year project.</p> <p><u>Some specific rule projects within the scope of this item:</u></p> <ul style="list-style-type: none"> (a) Formatting of electronic reporters’ transcripts: This project is ongoing . Rule 8.144 was amended in the prior rules cycle to provide format requirements for electronic court reporter transcripts consistent with amendments to Code of Civil Procedure section 271. In this rules cycle JATS will consider additional amendments to Rule 8.144. (b) Sealed & Confidential Material: Rules for the handling of sealed or confidential materials that are submitted electronically. (c) Return of lodged electronic records: The trial court rule modernization changes made in 2016 amend rules 2.551(b) and 2.577(d)(4) to give the moving party ten days after a <i>motion to seal</i> is denied, to notify the court if the party wants the record to be filed unsealed. If the clerk does not receive notification in ten days, the clerk must return the record, if lodged in paper form, or permanently delete it if lodged in electronic form. JATS will consider whether equivalent appellate rules are desirable. (d) Rule amendments regarding access: This project is underway. JATS will consider possible rule amendments to address online access to trial court records for parties, their attorneys, local justice partners, and other government agencies. The plan is for JATS to review what is ultimately proposed at the trial court level and use that as a basis for developing a companion proposal for access to appellate court records. 	

⁶ For rules and forms proposals, select one of the following priority levels: 1(a) Urgently needed to conform to the law; 1(b) Urgently needed to respond to a recent change in the law; 1(c) Adoption or amendment of rules or forms by a specified date required by statute or council decision; 1(d) Provides significant cost savings and efficiencies, generates significant revenue, or avoids a significant loss of revenue; 1(e) Urgently needed to remedy a problem that is causing significant cost or inconvenience to the courts or the public; 1(f) Otherwise urgent and necessary, such as a proposal that would mitigate exposure to immediate or severe financial or legal risk; 2(a) Useful, but not necessary, to implement statutory changes; 2(b) Helpful in otherwise advancing Judicial Council goals and objectives.

- (e) **Bookmarking:** The 2016 trial court rules modernization changes include a new requirement, added to rule 3.1110(f), that electronic exhibits be electronically bookmarked. This issue was set aside by JATS for 2016, to give those appellate courts new to e-filing (or not yet on e-filing) a chance to gain some experience with e-filing before participating in a decision as to what to require.
- (f) **Exhibits:** This project has not been started. Creating a requirement that exhibits submitted in electronic form be submitted in electronic volumes, rather than individually.
- (g) **Numbering of materials in requests for judicial notice:** Consider amending rule 8.252, which requires numbering materials to be judicially noticed consecutively, starting with page number one. But these materials are attached to a motion and declaration(s) and are electronically filed as one document, making pagination and referring to these materials in the briefs confusing for litigants and the courts.

Origin of Project: Tactical Plan for Technology 2017-2018; standing item on annual agenda.

Status/Timeline: Portions of this project are underway. Completion date of January 1, 2019. Overall modernization of rules is ongoing.

Resources/Partners:

- *ITAC:* Joint Appellate Technology Subcommittee, Chair: Hon. Louis Mauro
- *JCC Staff Resources:* Legal Services, Information Technology
- *Advisory Collaboration:* Members of the Appellate Advisory Committee who serve on the Joint Appellate Technology Subcommittee

One-Time Project (Ending 2020)

14.2 Rules Regarding Certification of Electronic Records, E-Signature, and Paper Copies

Priority 2(b)

Project Summary: Rules Regarding Certification of Electronic Records, Electronic Signature, and Paper Copies

Key Objectives:

- (a) Provide input on proposed changes to the trial court rules of court governing certification of electronic records, standards for electronic signatures, and requirements for paper copies of e-filed documents that will impact the appellate courts.
- (b) Consider whether to proceed with proposing changes to the appellate court rules on these matters.

Origin of Project: The ITAC Rules & Policy Subcommittee (RPS) is reviewing trial court rules governing certification of electronic records, standards for electronic signatures, and whether parties should have to submit paper copies of documents filed electronically. Some changes will require legislation to amend existing statutory requirements for e-filing, service, and signatures in the trial courts. (See Code Civ. Proc., § 1010.6.) As ITAC RPS moves the project forward, JATS will provide input on changes that will affect the appellate courts. The project may result in rules work for JATS. In addition, after ITAC RPS has resolved these issues for the trial courts, JATS may wish to consider proposing changes to the appellate court rules on these matters.

Status/Timeline: JATS work must wait until ITAC RPS moves forward. Completion date of January 1, 2020.

Resources/Partners:

- *ITAC:* Joint Appellate Technology Subcommittee, Chair: Hon. Louis Mauro
- *JCC Staff Resources:* Legal Services, Information Technology
- *Advisory Collaboration:* Members of the Appellate Advisory Committee who serve on the Joint Appellate Technology Subcommittee

One-Time Project (Ending 2020)	
14.3 Input on Appellate Document Management System	<i>Priority 2(b)</i>
<p>Project Summary: Monitor and Provide Input on the Appellate Courts Document Management System Implementation.</p> <p>Key Objectives:</p> <p>(a) Monitor and provide input on the implementation of a new document management system (DMS) for the appellate courts.</p> <p>Origin of Project: New item. This initiative supports JATS ongoing charge to consult on technology matters impacting appellate court business.</p> <p>Status/Timeline: January 1, 2020</p> <p>Resources/Partners:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Joint Appellate Technology Subcommittee, Chair: Hon. Louis Mauro • <i>JCC Staff Resources:</i> Legal Services, Information Technology • <i>Advisory Collaboration:</i> Members of the Appellate Advisory Committee who serve on the Joint Appellate Technology Subcommittee • <i>External Partners:</i> Appellate Administrative Presiding Justices, Appellate Court Clerks 	

Ongoing Project	
15. Liaison Collaboration	<i>Priority 1</i>
<p>Project Summary: Liaise with Advisory Bodies for Collaboration and Information Exchange</p> <p>Key Objectives:</p> <ul style="list-style-type: none"> (a) Appoint ITAC members to serve as liaisons to identified advisory bodies. (b) Share ITAC status reports with advisory body chairs and attend liaison committee meetings. (c) Identify opportunities to collaborate and share liaison feedback to ITAC, the JCTC, the Judicial Council, and the branch, as appropriate. <p>Origin of Project: Standing item on the annual agenda.</p> <p>Status/Timeline: Ongoing</p> <p>Resources:</p> <ul style="list-style-type: none"> • <i>ITAC:</i> Assigned Liaisons • <i>Judicial Council Staffing:</i> Information Technology • <i>Collaborations:</i> Liaison advisory bodies 	

III. LIST OF 2017 PROJECT ACCOMPLISHMENTS

#	Project Highlights and Achievements
1.	Tactical Plan for Technology Update – completed update of plan, effective FY2017-2018.
2.	Next-Generation Hosting Strategy (Phase 1) – completed the framework guide and associated spreadsheet tools for use by courts. These final deliverables are expected to be approved by the Judicial Council Technology Committee, adopted by the Judicial Council, and published by March 2018.
3.	Disaster Recovery Framework (Phase 1) – completed the framework guide and associated model template for use by courts. These final deliverables are expected to be approved by the Judicial Council Technology Committee, adopted by the Judicial Council, and published by March 2018.
4.	E-Filing Strategy – selected statewide e-filing managers (EFMs) to support statewide standards-based e-filing; received Budget Change Proposal (BCP) loan to support a branch e-filing program; the loan will be repaid through the implementation of a court e-filing cost recovery fee.
5.	Self-Represented Litigants (SRL) E-Services – completed a Request for Information (RFI) solicitation, which will inform its anticipated Request for Proposal (RFP).
6.	Video Remote Interpreting (VRI) Pilot – selected vendors and courts to participate in the pilot program; identified the project team and established the appropriate infrastructure at the courts to launch the program in 2018.
7.	Intelligent Forms Strategy: Research & Scope (Phase 1) – formed workstream and began development of recommendations.
8.	Digital Evidence: Assessment (Phase 1) – formed workstream and began development of surveys.
9.	Rules & Policy Subcommittee – The Judicial Council adopted e-filing and e-service rule amendments, and voted to sponsor legislation in 2018 to modernize sections of the civil code and code of civil procedure. Specifically, the committee proposed and the Judicial Council adopted rules to amend rules 2.250, 2.251, 2.252, 2.253, 2.254, 2.255, 2.256, 2.257, and 2.259; for legislation, the committee proposed and the Judicial Council voted to sponsor legislation to amend section 1719 of the Civil Code and sections 594, 659, 660, and 663a of the Code of Civil Procedure.
10.	Joint Appellate Technology Subcommittee (JATS) – provided input on the committee’s proposal to amend rule 8.144 to address the format of court reporter’s transcripts delivered in electronic form.
11.	Joint Ad Hoc Rules for Remote Access to Records Subcommittee – formed joint subcommittee and initiated project to amend the trial court rules to facilitate remote access to records by government entities, parties, parties’ attorneys, and court-appointed counsel.



JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue
San Francisco, CA 94102-3688
Tel 415-865-4200
TDD 415-865-4272
Fax 415-865-4205
www.courts.ca.gov

HON. TANI G. CANTIL-SAKAUYE
Chief Justice of California
Chair of the Judicial Council

MR. MARTIN HOSHINO
Administrative Director,
Judicial Council

INFORMATION TECHNOLOGY ADVISORY COMMITTEE

HON. SHEILA F. HANSON
Chair

HON. LOUIS R. MAURO
Vice-chair

Mr. Brian Cotta
Hon. Julie R. Culver
Ms. Alexandra Grimwade
Hon. Michael S. Groch
Hon. Sheila F. Hanson
Hon. Samantha P. Jessner
Hon. Jackson Lucky
Hon. Louis R. Mauro
Hon. Kimberly Menninger
Hon. James M. Mize
Mr. Terry McNally
Mr. Snorri Ogata
Mr. Darrel E. Parker
Hon. Alan G. Perkins
Hon. Peter J. Siggins
Hon. Mark Stone
Ms. Jeannette Vannoy
Mr. Don Willenburgh
Mr. David H. Yamasaki

COMMITTEE STAFF

Ms. Jamel Jones
Tel 415-865-4629
Fax 415-865-4503

Date
December 5, 2017

To
Members of the Judicial Council
Technology Committee

From
Information Technology
Advisory Committee (ITAC)
Hon. Sheila Hanson, Chair

ITAC Disaster Recovery
Workstream
Hon. Alan Perkins,
Executive Cosponsor

Mr. Brian Cotta,
Executive Cosponsor

Subject
*Disaster Recovery Framework
Guide*

Action Requested
Please Review and
Recommend

Deadline
January 8, 2018

Contact
Mr. Brian Cotta,
Executive Cosponsor
Brian.cotta@jud.ca.gov

Mr. Michael Derr, Principal
Manager, Information
Technology
Michael.derr@jud.ca.gov

Ms. Jamel Jones, Supervisor,
Information Technology
Jamel.jones@jud.ca.gov

Summary

The Information Technology Advisory Committee (ITAC) Disaster Recovery (DR) Framework Workstream is seeking approval and recommendation of its proposed *Disaster Recovery Framework Guide*, model template, and “how to” guide.

Background

Judicial Branch entities must be concerned about the impact of disasters of all kinds, whether resulting from extreme weather events, earthquake, or by malicious entities. A corollary to these concerns is the effect migration to new IT hosting environments will have on disaster recovery preparedness and planning. Budget constraints certainly impact the ability

of individual courts and the branch to be prepared for, and recover from, natural and unnatural disasters.

The judicial branch *Tactical Plan for Technology* identifies disaster recovery as an important issue for the courts to address. Thus, the ITAC Disaster Recovery Workstream was formed in April 2016 for the purposes of developing, documenting, and proposing model disaster recovery guidelines and an adaptable framework to serve as a disaster recovery plan for any judicial branch entity (JBE) who chooses to use it.

The workstream team was comprised of judicial officers, court executives, and technologists from 18 trial courts, 3 appellate courts, and the Judicial Council. In September 2016, the workstream team surveyed the courts to understand the current posture and preparedness of the courts in relation to recovering IT data and services in the event of a natural or unnatural disaster. With this data and additional study, the team met regularly to develop an adaptable framework document that a JBE may use in planning its IT response to disaster recovery situations.

The resulting portfolio of documents—(1) Disaster Recovery Framework: Recommendations & Reference Guide, (2) Adaptable Disaster Recovery Template (for completion by a JBE), and (3) complementary “How to Use” Guide— developed by the workstream are designed to help JBE’s with the various processes necessary to plan and implement a disaster recovery strategy at a desired pace.

Branch Comment and Approvals

In July 2017, the framework documents were circulated to the branch (including to the Supreme Court, appellate courts, and superior courts) for comment. While few suggestions were received, the response was extremely positive with many courts expressing appreciation and immediate interest in the final deliverables. As a result of this comment period, additional language was incorporated to address concerns related to corrupted backups and controlling access to backups; and, to provide an expanded discussion of cloud options. Non-substantive revisions were also made to generally improve flow.

ITAC approved the final deliverables, as revised per branch comment, at its December 4, 2017 meeting.

Requested Action

The workstream seeks approval and recommendation of the enclosed *Disaster Recovery Framework Guide*, model template, and “how to guide” at the **Monday, January 8, 2018** Judicial Council Technology Committee (JCTC) business meeting. During review of the final deliverables prior to the meeting, kindly forward any additional feedback or changes to Brian Cotta (brian.cotta@jud.ca.gov).

December 5, 2017

Page 3

Next Steps

Pending approval by the JCTC, the workstream will seek acceptance by the Judicial Council. Final documents will be published and available on the Judicial Resources Network for use by courts.

As part of its final deliverables, the workstream recommends that a next step be to prepare a budget change proposal (BCP) requesting funding to assist courts adopt the framework and help ensure successful and reliable disaster recovery software/hardware and solution(s) across the branch. At a recent meeting of the Court Information Technology Management Forum (CITMF), the group unanimously concurred that disaster recovery is the top priority for a technology BCP in FY19-20.

Thank you, in advance, for your time and attention.

Enclosures

- (1) Disaster Recovery Framework: Recommendations & Reference Guide,
- (2) Adaptable Disaster Recovery Template (for completion by a court)
- (3) "How to Use" Guide for the Disaster Recovery Framework

CALIFORNIA JUDICIAL BRANCH

Disaster Recovery Framework

A Recommendations & Reference Guide for the
California Judicial Branch

VERSION 2.3

OCTOBER 22, 2017



JUDICIAL COUNCIL
OF CALIFORNIA

INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

Table of Contents

1.0	INTRODUCTION	3
2.0	DEFINITION	3
3.0	PURPOSE OF DISASTER RECOVERY	3
4.0	DISASTER RECOVERY FRAMEWORK	4
4.1	Scope.....	4
4.2	Organizational Characteristics.....	5
4.3	Organizational History and Importance of Disaster Recovery.....	5
4.4	Supporting References and Content.....	5
4.5	Documentation Structure.....	6
5.0	SUPPORTED AND RECOMMENDED BACKUP TECHNOLOGIES	7
5.1	Disk.....	7
5.2	Cloud.....	8
6.0	CONTINGENCY STRATEGIES	9
6.1	Backup Methods.....	9
6.2	Alternate Sites.....	10
6.3	Recovery Options.....	11
6.3.1	Cold site.....	11
6.3.2	Warm site.....	11
6.3.3	Hot site.....	11
6.3.4	Mirrored site.....	11
6.3.5	Cloud.....	11
6.4	Selecting an Option.....	12
6.5	Equipment Replacement.....	14
6.5.1	Vendor agreements.....	14
6.5.2	Equipment inventory.....	15
6.5.3	Existing compatible equipment.....	15
7.0	PROVEN AND AVAILABLE TECHNOLOGIES AND PRODUCTS	15
7.1	Technologies Currently Deployed in the Branch.....	15
7.2	Potentially Useful Technologies Not Known to be Implemented in the Branch.....	16
8.0	EXAMPLE SCENARIOS AND DEPLOYMENT SOLUTIONS	16
8.1	Single-Site Small or Medium JBE.....	19
8.1.1	Scenario 1: Cloud-based DR.....	19
8.1.2	Scenario 2: Court-to-court colocation.....	21
8.2	Medium or Large JBE With Two or More Sites in Close Proximity.....	22
8.2.1	Scenario 1: Cloud-based DR.....	22

8.2.2	Scenario 2: Colocation data center	23
8.3	Medium or Large JBE with Two or More Sites NOT in Close Proximity.....	24
8.3.1	Scenario 1: Cloud-based DR.....	24
8.3.1	Scenario 2: Secondary-site data center	25
9.0	PLANNING	26
10.0	IMPLEMENTATION	27
11.0	KEY POINTS, CONCERNS, AND COMPLIANCE	28
11.1	Limited Access to & Security Controls for Backup Systems.....	28
11.2	Backup of Microsoft Office 365 & Cloud Data	28
11.3	Abandonment of Tapes.....	28
11.4	Use of Primary SAN or Array	28
11.5	Use of Virtualization Cluster.....	29
11.6	Retention of Data (Backups)	29
11.7	Data Classifications	29
11.8	Purpose-Built Backup Appliance vs. Backup Server	30
11.9	Cloud Service Subscriptions and Payments	30
11.10	Uncompromised Access to Credentials for Recovery Systems and Cloud Platforms.....	30
12.0	MONITORING, TESTING, VALIDATION, AND REVIEW	31
12.1	Regular Review of Backup and Disaster Recovery Systems	31
12.1.1	E-mail notifications.....	31
12.1.2	Backup job monitoring and auditing.....	31
12.1.3	Site recovery/cutover systems monitoring and auditing.....	31
12.1.4	Gap Analysis.....	31
12.2	Routine Testing Exercises	31
12.3	Testing Simulations	32
12.3.1	Loss of building access	32
12.3.2	Loss of access to all systems (onsite or offsite) based on catastrophic outage or disaster	32
12.3.3	Backup system failure.....	32
12.3.4	High-availability (site recovery) system failure.....	32

1.0 INTRODUCTION

The Judicial Branch Disaster Recovery Framework serves as a model and aid for implementing and maintaining a lean and robust information technology (IT) disaster recovery (DR) solution. The framework and related reference materials will assist judicial branch entities (JBEs) with establishing a disaster recovery strategy and will offer recommendations and examples of products and services that can accommodate the varying needs of small to large Supreme, appellate, and superior courts. The Supreme Court, the Courts of Appeal, and the superior courts (hereafter collectively referred to as JBEs) are not required to implement the framework in its entirety; rather, the intent is to highly encourage JBEs to use the framework as a template to develop a disaster recovery strategy and solution most appropriate to their unique local business requirements. Additionally, each court's disaster recovery implementation will differ significantly based on factors such as geographic location, natural disaster risk ratings, types of hosting solutions in use, and varying business drivers. The framework is for use as a guide and versatile benchmark of what should be in place in each JBE.

This guide is intended to provide a roadmap for JBE's and does not include all the details or steps required for implementing a trusted, fail-safe disaster recovery plan or solution. It does, however, provide tools and examples for JBEs to design disaster recovery solutions appropriate to their needs and recommend ways to ensure the integrity and usefulness of the those solutions.

2.0 DEFINITION

A disaster recovery plan includes a set of branch policies, procedures, diagrams, documentation, systems, and tools "to enable the recovery or continuation of vital technology infrastructure and systems following a *natural* or *human-induced disaster*."¹ It also includes a robust redundant and/or alternate infrastructure to facilitate quick recovery of critical systems, with regular defined intervals of testing that occur to ensure the integrity of the approach.

3.0 PURPOSE OF DISASTER RECOVERY

Data and electronic information are paramount to the operation and success of each judicial branch entity. The broad term *information system* is used to identify a human and electronic process for the collection, organization, storage, and presentation of information. Consistent with that of other industries, JBEs' use of systems and technology has increased over time. Any JBE would be challenged to continue normal operations without systems that have become integral to business process.

¹ Wikipedia contributors, "Disaster recovery," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/w/index.php?title=Disaster_recovery&oldid=772607446 (as of May 9, 2017), referencing Georgetown University, Business Continuity and Disaster Recovery, *Disaster Recovery*, <https://continuity.georgetown.edu/dr> (as of May 9, 2017).

The purpose of IT disaster recovery is to restore or maintain operations of technology systems supporting critical business functions following a natural or human-induced disaster. Although this document focuses primarily on IT disaster recovery, it is important that the disaster recovery plan support and align with the business continuity plan and/or other established plans and protocols that JBEs have in place (e.g., Continuity of Operations Plan, <https://coop.courts.ca.gov>).

Consideration should also be given to aligning the JBE disaster recovery plan to those of applicable justice partner agencies. The goal is to facilitate restoration of related or dependent services across agencies where possible.

Technologies such as backup, off-site storage, replication, and private/hybrid cloud, and metrics such as recovery point objective (RPO) and recovery time objective (RTO) are all valid discussion points and planning considerations when reviewing disaster recovery options.

A disaster recovery plan should be tailored to the individual JBE, with the goal that vital systems are preserved and made operational at performance, availability, and cost levels that meet JBE business continuity objectives.

4.0 DISASTER RECOVERY FRAMEWORK

4.1 Scope

The disaster recovery framework has been developed for the establishment of a baseline reference model for disaster recovery within the judicial branch of California. It is known that existing and future DR plans put into place by JBEs will differ from one another primarily because of varying logistics and challenges with facilities, geographic locations, funding, and/or internal requirements. To produce the framework, input was solicited from multiple courts ranging in size from small to large so that a comprehensive framework could be developed that suits all entities within the judicial branch. The framework is designed to set a direction, identify and address the growing importance of DR within the branch, and ensure that the rapid evolution and adoption of technology within the branch are complemented with a plan to ensure the integrity of electronic data and systems.

The goals of the framework are to:

- Encourage a JBE to assess their current environment and conduct a DR maturity analysis;
- Suggest and define model disaster recovery guidelines for the branch;
- Suggest and define standard recovery times and priorities for each of the major technology components of the branch;

- Be usable by all judicial branch entities as a court’s disaster recovery plan;
- Provide baseline guidance for backups and high-availability options and scenarios for JBEs to incorporate into their disaster recovery strategies;
- Provide visual reference of various disaster recovery scenarios;
- Provide guidance to all members of the judicial branch on establishing methods of applying disaster recovery and therefore ensuring the integrity, survivability, and recoverability of various systems and data; and
- For each platform, operating system, application, and security device, provide the basis for the development of implementation standards, procedures, and guidelines that can then be monitored and enforced against the recommendations defined in the framework.

4.2 Organizational Characteristics

The framework establishes how various systems and data are to be backed up and protected from data loss and will be made highly available to mitigate the chances that the disaster recovery plan would need to be relied on. Some judicial branch entities interface and share data with one another, increasing the complexities and risk factors of data ownership and protection. Additionally, because of the complex inner workings of the judicial branch and each individual JBE, each court’s Continuity of Operations Plan (COOP) overlaps. The IT DR plan and all related material should be placed into and support the COOP. It is not, however, a replacement for the COOP, and neither is the COOP a holistic solution for IT disaster recovery.

4.3 Organizational History and Importance of Disaster Recovery

Over the past decade, JBEs have increasingly deployed more and more technology to increase operational efficiencies, improve public access to justice, and to streamline interaction with various justice partners. Specifically, over the last four years, as a result of budget reductions and other hardships, some JBEs have elected and others were forced to deploy and host their own case management systems: systems that were once managed by a central entity or provider (e.g., the judicial branch, with its California Courts Technology Center [CCTC] or a respective county). Additionally, some JBEs have begun using cloud-provided services, systems, and software, drastically changing the traditional approach to disaster recovery and how data is backed up and preserved.

4.4 Supporting References and Content

Following are some sources and publications that the Judicial Council’s Information Technology Advisory Committee (ITAC) referenced in the development of this framework:

- Next Generation Hosting Strategy Workstream output(s) (ITAC deliverable pending)
- Information Systems Controls Framework (Judicial Council and ITAC deliverable)
- California Courts Technology Center
- NASCIO—*Cyber Disruption Response Planning Guide*
(www.nascio.org/Portals/0/Publications/Documents/2016/NASCIO_CyberDisruption_072016.pdf)
- National Institute of Standards and Technology—Special Publication 800-34 Rev. 1
(Contingency Planning Guide for Federal Information Systems)
(<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>)

4.5 Documentation Structure

An IT disaster recovery plan is supported by documentation that captures differing levels of detail while ensuring that the plan is flexible enough to adapt as organizational and IT priorities and dependencies change. The IT disaster recovery framework should consist of the following categories of documents:

- Organizational policy (for JBEs)—expresses management’s expectations regarding disaster recovery and importance of data, including expectations for time to recover based on categorized tiers of data types and importance.
- IT department policy—further refines management’s expectations, specifically of data protection from a technical perspective and for safeguarding electronic data from loss or destruction within specified parameters, as defined by the local entity. The department policy informs IT staff of the department’s comprehensive approach toward disaster recovery, ensuring that all subdivisions in the department are working cohesively to comply.
- List of systems/data categorized by recovery time—a complete categorized list of data assets broken into tiers of criticality, including specific hardware, systems, software, and data that support the mission of the JBE. This document includes the ITAC-recommended criticality ranking of many systems; however, local organizational policy within each JBE may necessitate changes to the list.
- List of appendixes
 - Appendix A: List of high-level technical requirements and systems and data categorized by recovery time
 - Appendix B: Recommended minimum requirements for a backup solution

- List of types of events that would trigger the declaration of a disaster or operational crisis to the JBE/region
 - Loss of data center (natural, by fire, by water, etc.)
 - Infrastructure or major equipment failure
 - Power outage or significant voltage surge
 - Cloud-hosted—circuit outage (single point of failure) or cloud data center outage (single point of failure)
 - Severing of communication cables (cut fiber, etc.)
 - Security breach
 - Data hostage situation (e.g., ransomware)
 - Malicious behavior—internal sabotage
 - Malicious behavior—vendor sabotage
- Checklists
 - Planning
 - Implementation and milestones
 - Verification and testing
- Guidelines—recommendations that can be used when other guidance has not been established. Guidelines are usually created at lower operational levels, such as by departments, to address immediate needs until consensus is reached on broader direction.

5.0 SUPPORTED AND RECOMMENDED BACKUP TECHNOLOGIES

5.1 Disk

A disk is a data storage device used for storing and retrieving digital information. It is a type of nonvolatile memory, retaining stored data even when powered off.²

- Pros
 - **Local.** Data is on the premises and therefore within your control.
 - **Speed.** Because data is local, it is typically accessed from internal networks that are capable of providing faster access times. There is also no overhead from latent internet bandwidth.
 - **Security.** Disks are not managed by a third party, which can protect your data from hacking and loss of privacy.
- Cons
 - **Management.** Controlling access to data—including virus protection and vulnerability protection—becomes the responsibility of the local agency.

² Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/wiki/Hard_disk_drive (as of May 30, 2017).

- **Cost.** Disks require upfront capital expense in addition to ongoing maintenance contracts when used in mission-critical applications.
- **Physical security.** Protection from physical threats including fire, water damage, and natural disaster are paramount and become the responsibility of the local agency.

5.2 Cloud

“Cloud computing is a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand.”³

- Pros
 - **Cost.** Onsite hardware and capital expenses are unnecessary and storage costs relatively low because you pay only for the storage you require.
 - **Expansion.** Scalable architecture allows for convenient provisioning of additional storage space as needed.
 - **Offsite location.** Data can be stored in geographically distinct locations, possibly preventing loss from disaster.
 - **Physical security.** Leading cloud providers typically take on the responsibility of keeping your data highly secure and mirrored across multiple centers within the United States. *Note: When using a cloud vendor, care should be taken to ensure all of a JBE’s data, including all replicas are housed and maintained within the United States. Additionally, it is important to clearly analyze and understand what level(s) of data protection and recovery options the cloud provider includes or offers.*
- Cons
 - **Outages.** If the Internet goes down on your side or on your cloud provider’s side, you may lose access to your information until the issue is remediated.
 - **Bandwidth.** Large amounts of bandwidth are required to conduct data/storage transfers and a lack of sufficient bandwidth can lead to performance degradations
 - **Exclusivity.** Once data has been transferred and procedures have been implemented, moving data/storage to another provider may be challenging.
 - **Privacy and security.** With private data exposure and data hostage situations becoming more commonplace, the cloud poses newer and varying security risks, some of which are still unknown. Careful analysis and IT controls should be framed around managing permissions (both internal and external), confidentiality of intellectual property, accidental and intentional deletion on individual, shared and cloud drives and clear-cut audit trails.
 - **Complexity.** Cloud technology can present newer and unknown challenges in regards to control and troubleshooting. All interaction with cloud computing is through the use of technology and the ability to remediate issues is limited to the response time of the supporting systems and hosting provider(s)’ call centers.

³ Wikipedia contributors, "Cloud computing," *Wikipedia, The Free Encyclopedia*, https://en.wikipedia.org/wiki/Cloud_computing (as of May 30, 2017).

NOTE: Tape technology is not a current or recommended backup medium for production and/or critical data. However, in certain circumstances where there may be a lack of bandwidth and options to increase bandwidth are limited or considerably expensive, tape may be an appropriate backup medium. Tape may also be a feasible choice for lab/test environments.

6.0 CONTINGENCY STRATEGIES

Recovery strategies provide a means to restore IT operations quickly and effectively following a service disruption. The strategies should address disruption impacts and allowable outage times identified in the business impact analysis. Several alternatives should be considered when developing the strategy, including cost, allowable outage time, security, and integration with larger, organization-level contingency plans.

The selected recovery strategy should address the potential impacts identified in the business impact analysis and should be integrated into the system architecture during the design and implementation phases of the system life cycle. The strategy should include a combination of methods that complement one another to provide recovery capability over the full spectrum of incidents. A wide variety of recovery approaches may be considered; the appropriate choice will depend on the incident, type of system and operational requirements. Specific recovery methods should be considered and may include commercial contracts with cold, warm, or hot backup-site vendors (see section 6.3); cloud providers; mirrored sites (see section 6.3.4); reciprocal agreements with internal or external organizations; and service-level agreements (SLAs) with the equipment vendors. In addition, technologies such as RAID (redundant array of independent disks), automatic failover, uninterruptible power supplies, and mirrored systems should be considered when developing a system recovery strategy.

6.1 Backup Methods

System data should be backed up regularly. Policies should specify the frequency of backups (e.g., daily or weekly, incremental or full) based on data criticality and the frequency that new information is introduced. Data backup policies should designate the location of stored data, file-naming conventions, media rotation frequency, and method for transporting data offsite. Data may be backed up on magnetic disks, cloud storage or other common-day and reliable mediums. The specific method for conducting backups should be chosen based on system and data availability and integrity requirements. Methods include electronic vaulting, storing to mirrored disks (using direct-access storage devices [DASDs] or RAID), and storing to cloud provided storage platforms.

Storing backed-up data offsite is *essential* business practice. Commercial data storage facilities are specially designed to archive media and protect data from threatening elements. With offsite storage, data is backed up at the organization's facility and then labeled, packed, and transported to the storage facility. If the data were required—for recovery or

testing, for example—the organization would contact the storage facility and request specific data/disks to be transported to the organization or to an alternate facility. Commercial storage facilities often offer media transportation and response and recovery services.

When selecting an offsite storage facility and vendor, the following criteria should be considered:

- Geographic area—distance from the organization and the probability of the storage site’s being affected by the same disaster that might strike the organization
- Accessibility—length of time necessary to retrieve the data from storage, and the storage facility’s operating hours
- Security—security capabilities of the storage facility and employee confidentiality, which must meet the data’s sensitivity and security requirements
- Environment—structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention, and power management controls)
- Cost—cost of shipping, operational fees, and disaster response and/or recovery services

6.2 Alternate Sites

Although major disruptions with long-term effects may be rare, they should be accounted for in the contingency plan. Thus, the plan must include a strategy to recover and perform system operations at an alternate facility for an extended period. In general, three types of alternate sites are available:

- Dedicated site owned or operated by the organization
- Reciprocal agreement or memorandum of agreement with an internal or external entity
- Commercially leased facility
- Cloud

Regardless of the type of alternate site chosen, the selection must be able to support system operations as defined in the contingency plan. The types of alternate sites may be categorized in terms of their operational readiness. Based on this factor, sites may be identified as cold, warm, hot, mobile, or mirrored sites. Progressing from basic to advanced, the sites are described below.

6.3 Recovery Options

6.3.1 Cold site

A cold site typically consists of a facility with adequate space and infrastructure (electric power, telecommunications connections, and environmental controls) to support the IT system. The space may have raised floors and other attributes suited for IT operations. The site does not contain IT equipment and usually does not contain office automation equipment, such as telephones, facsimile machines, or copiers. The organization using the cold site is responsible for providing and installing necessary equipment and telecommunications capabilities.

6.3.2 Warm site

Warm sites are partially equipped office spaces that contain some or all of the system hardware, software, telecommunications, and power sources. A warm site is maintained in an operational status ready to receive the relocated system. The site may need to be prepared before receiving the system and recovery personnel. In many cases, a warm site may serve as a normal operational facility for another system or function, and in the event of contingency plan activation, the normal activities are displaced temporarily to accommodate the disrupted system.

6.3.3 Hot site

Hot sites are office spaces appropriately sized to support system requirements and configured with the necessary system hardware, supporting infrastructure, and support personnel. Hot sites are typically staffed 24 hours a day, seven days a week. Hot-site personnel begin to prepare for the system arrival as soon as they are notified that the contingency plan has been activated.

6.3.4 Mirrored site

Mirrored sites are fully redundant facilities with full, real-time information mirroring. Mirrored sites are identical to the primary site in all technical respects. These sites provide the highest degree of availability because the data are processed and stored at the primary and alternate sites simultaneously. These sites typically are designed, built, operated, and maintained by the organization.

6.3.5 Cloud

A cloud “location” can serve as warm, hot, or mirrored site and have a number of other benefits and purposes. Cloud offerings can provide remote and virtual infrastructure and are typically rated at a high-tiered classification for uptime, reliability, and scalability. Contracted services are often available through cloud

providers to help with a JBE’s disaster recovery strategy and goals that require technical assistance by the cloud provider. For additional offerings and recommendations relative to the cloud, please reference the judicial branch Next Generation Hosting Strategy Workstream deliverables.

6.4 Selecting an Option

The cost and ready-time differences among the four options are obvious. The mirrored site is the most expensive choice, but it ensures virtually 100 percent availability. Cold sites are the least expensive to maintain; however, they may require substantial time to acquire and install necessary equipment. Partially equipped sites, such as warm sites, fall in the middle of the spectrum. The selection of fixed-site locations should account for the time and mode of transportation necessary to move personnel there. In addition, the fixed site should be in a geographic area that is unlikely to be negatively affected by the same disaster event (e.g., weather-related impacts or power grid failure) that affected the organization’s primary site. The table below summarizes the criteria that can be employed to determine which type of alternate site meets the organization’s requirements. Sites should be analyzed to ensure that the security, management, and operational and technical controls of the systems to be recovered are compatible with the prospective site. Such controls may include firewalls and physical access controls, data remanence controls, and security clearance levels of the site and staff supporting the site.

Alternate-Site Selection Criteria

Site	Cost	Hardware Equipment	Telecommunications	Setup Time	Location
Cold	Low	None	None	Long	Fixed
Warm	Medium	Partial	Partial/Full	Medium	Fixed
Hot	Medium/High	Full	Full	Short	Fixed
Mirrored	High	Full	Full	None	Fixed
Cloud	Medium/High	N/A	Mixed	Short	Agile

These alternate sites may be owned and operated by the organization (internal recovery), or commercial sites may be available under contract. Additionally, cloud providers can provide IaaS (Infrastructure as a Service) computing that mimics a colocation site and offers near-unlimited services and opportunities. If contracting for the site with a commercial vendor, adequate testing time, workspace, security requirements, hardware requirements, telecommunications requirements, support services, and recovery days (how long the organization can occupy the space during the recovery period) must be negotiated and clearly stated in the contract. Customers should be aware that multiple organizations may contract with a vendor for the same alternate site; as a result, the site may be unable to accommodate all of the customers if a disaster affects enough of those customers simultaneously. The vendor’s policy on how this situation will be addressed and how priority status is determined should be negotiated.

Two or more organizations with similar or identical IT configurations and backup technologies may enter into a formal agreement to serve as alternate sites for each other or enter into a joint contract for an alternate site. With sites that serve as alternate sites for each other, a reciprocal agreement or memorandum of understanding (MOU) should be established. A reciprocal agreement should be entered into carefully because each site must be able to support not only its own workload but the other organization's as well, in the event of a disaster. This type of agreement requires the recovery sequence for the applications from both organizations to be prioritized from a joint perspective, favorable to both parties. Testing should be conducted at the partnering sites to evaluate the extra processing thresholds, compatible system and backup configurations, sufficient telecommunications connections, compatible security measures, and sensitivity of data that might be accessible by other privileged users, in addition to functionality of the recovery strategy.

An MOU, memorandum of agreement (MOA), or a service level agreement (SLA) for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities. The legal department of each party must review and approve the agreement. In general, the agreement should address at a minimum, each of the following elements:

- Disaster declaration (i.e., circumstances constituting a disaster and notification procedures)
- Site and/or facility priority access and/or use
- Site availability
- Site guarantee
- Other clients subscribing to the same resources and site, and the total number of site subscribers, as applicable
- The contract or agreement change or modification process
- Contract or agreement termination conditions
- The process to negotiate extension of service
- Guarantee of compatibility
- IT system requirements (including data and telecommunication requirements) for hardware, software, and any special system needs (hardware and software)
- Change management and notification requirements, including hardware, software, and infrastructure

- Security requirements, including special security needs
- Whether staff support is provided
- Whether facility services are provided (use of onsite office equipment, cafeteria, etc.)
- Testing, including scheduling, availability, test time duration, and additional testing, if required
- Records management (onsite and offsite), including electronic media and hard copies
- Service-level management (performance measures and management of quality of IT services provided)
- Workspace requirements (e.g., chairs, desks, telephone, PCs)
- Supplies provided or required (e.g., office supplies)
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable

6.5 Equipment Replacement⁴

If the IT system is damaged or destroyed or the primary site is unavailable, necessary hardware and software will need to be activated or procured quickly and delivered to the alternate location. Three basic strategies exist to prepare for equipment replacement. When selecting the most appropriate strategy, note that the availability of transportation may be limited or temporarily halted in the event of a catastrophic disaster.

6.5.1 Vendor agreements

As the contingency plan is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance service. An SLA should specify how quickly the vendor must respond after being notified. The agreement should also give the organization priority status for the shipment of replacement equipment over equipment being purchased for normal operations. SLAs should further discuss what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. In such cases, organizations with health- and safety-dependent processes will often receive the highest priority for

⁴ Section 6.5 is taken from NIST Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), § 3.4.4, pp. 24–25, <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf> (as of May 10, 2017).

shipment. The details of these negotiations should be documented in the SLA, which should be maintained with the contingency plan.

6.5.2 Equipment inventory

Required equipment may be purchased in advance and stored at a secure off-site location, such as an alternate site where recovery operations will take place (warm or mobile site) or at another location where they will be stored and then shipped to the alternate site. This solution has certain drawbacks, however. An organization must commit financial resources to purchase this equipment in advance, and the equipment could become obsolete or unsuitable for use over time because system technologies and requirements change.

6.5.3 Existing compatible equipment

Equipment currently housed and used by the contracted hot site or by another organization within the agency may be used by the organization. Agreements made with hot sites and reciprocal internal sites stipulate that similar and compatible equipment will be available for contingency use by the organization.

When evaluating the choices, the contingency planning coordinator should consider that purchasing equipment when needed is cost-effective, but can add significant overhead time to recovery while waiting for shipment and setup; conversely, storing unused equipment is costly, but allows recovery operations to begin more quickly. Based on impacts discovered through the business impact analysis, consideration should be given to the possibility of a widespread disaster requiring mass equipment replacement and transportation delays that would extend the recovery period. Regardless of the strategy selected, detailed lists of equipment needs and specifications should be maintained within the contingency plan.

7.0 PROVEN AND AVAILABLE TECHNOLOGIES AND PRODUCTS

7.1 Technologies Currently Deployed in the Branch

The following currently deployed technologies and in use throughout the branch help JBES meet their disaster recovery plan objectives:

- [Barracuda Backup](#) with secondary Barracuda Backup appliance and/or cloud replica(s)
- [Barracuda Cloud-to-Cloud Backup](#)
- [Barracuda Essentials for Office 365](#)
- [VMware Site Recovery Manager](#)

- Various cloud providers
- Various storage area network (SAN) solutions with “snapshot” and “lagged mirror” technology

7.2 Potentially Useful Technologies Not Known to be Implemented in the Branch

Following are examples of technologies that are believed not yet to have been implemented in the branch, but that exhibit strengths in disaster recovery objectives:

- [Veeam Backup & Replication](#) with cloud replica
- [Rubrik Cloud Data Management](#) with cloud replica
- [Amazon Web Services \(AWS\) Storage Gateway](#)
- [Microsoft Azure Site Recovery](#)
- [Veeam DRaaS \(Veeam Cloud Connect\)](#)
- Hyperconverged infrastructure/solutions that can accomplish a JBE’s DR initiative(s)

NOTE: The products and/or technologies listed above are for baseline reference purposes only. JBEs do not have to choose one of these solutions, but rather can use the technologies on the list or reference the list to determine what solutions best fit within their technology environments and meet their recovery objectives.

8.0 EXAMPLE SCENARIOS AND DEPLOYMENT SOLUTIONS

Disaster recovery scenarios can be very complex and impossible to work out without specific details. Sections 8.1–8.3 offer guidelines for some general scenarios. Note that a number of caveats to implementation must be taken into account when creating a disaster recovery scenario, including the following:

- **Identify business-critical servers and data.** Identifying the business-critical servers and data will provide the information required to size the disaster recovery scenario. This information is critical to scenarios pertaining to cloud services and physical hardware.
- **Determine data circuit requirements.** Using the information from the identifying server and data needs will allow the JBE to determine the bandwidth requirements to support the replication and synchronization of the DR scenario.

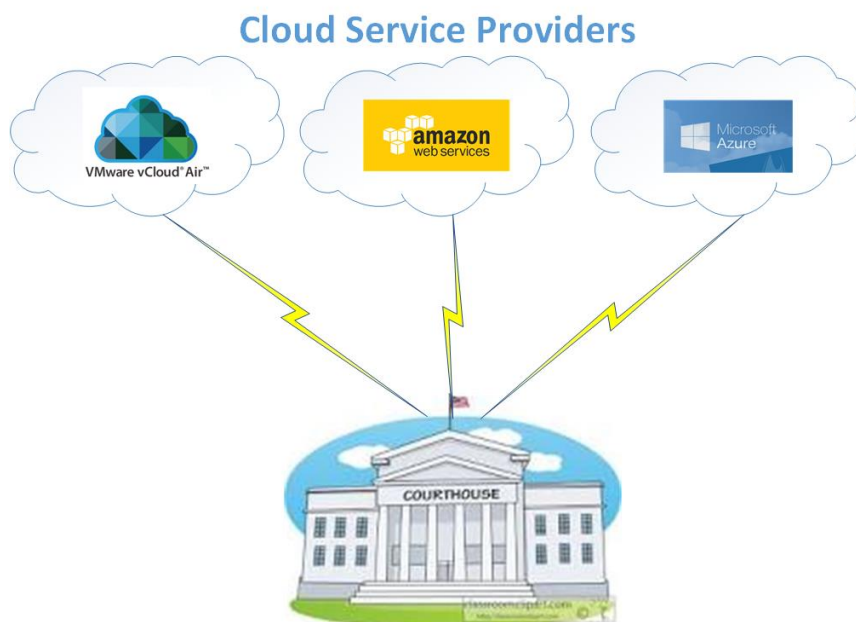
- **Identify technology to facilitate DR.** Identifying the technologies in use is important. DR scenarios are intended to assist in implementing a DR plan for IT and so focus on electronic data. However, JBEs may have critical data that are not in electronic format. Therefore, the JBE needs to identify technologies that can be used to assist in the DR plan. As an example, if a court has gone paperless, it can store the documentation for cases on the cloud, leaving the documentation accessible during an outage or disaster. However, if the court still stores paper case files, in the event of a disaster the court may lose those paper files and be unable to recover them. Another component that can support a JBE's DR strategy is through the use of virtualization technology, which allows for easy transfer of servers between data center and cloud.
- **Identify physical requirements.** Many of the scenarios in section 8.0 require physical hardware and, therefore, the related space, racks, servers, network equipment, and appliances. It is important to identify what equipment will be necessary and to ensure that power and cooling are sufficient to meet the needs of that equipment following a disaster. However unlikely it is, these scenarios may one day be running the critical court operations for a JBE, and they should be provided similar resources to the primary data center.
- **Identify public-relations impact.** Careful thought should be taken into consideration in regards to media and what the news may look like on the front page of a JBE's local newspaper.
- **Identify cost(s) or backlog impact.** A detailed business impact analysis should be conducted to determine what financial and/or labor/backlog impact may result from both short-term and long-term outages. The results of this analysis will help a JBE prioritize recovery objectives and sequencing.

To discuss DR scenarios effectively, a common starting point for the differing terminology is also essential. In many cases, different definitions for the same terminology are floating in the ether. Below are several relevant terms and their definitions:

- **Public cloud**—a network of remote servers and storage hosted by a vendor and accessible on the Internet. It allows for the storage, management, and processing of data offsite, rather than using local resources. Cloud advantages include scalability, instant provisioning, and virtualization of resources. The public cloud typically shares resources among many tenants or customers.
- **Private cloud**—similar to a public cloud, but resources are dedicated to a single tenant or customer. A private cloud can also reside on the premises, providing the benefits of local use and control while leveraging the benefits of a cloud computing platform. Examples of on-premises private cloud solutions are VMware, Nutanix, and Microsoft Hyper-V hypervisor. On-premises private cloud offers the same advantages as any other cloud, including scalability, instant provisioning, and virtualization.

- **Hybrid cloud**—a cloud computing environment using a mix of cloud services (public and private) and on-premises hardware (standard data center) to facilitate communication between a data center and cloud services.
- **Cloud service providers**—vendors who sell public and private cloud services and hybrid solutions. Top-tier cloud service providers include Amazon Web Services, Google, Microsoft, VMware and Oracle. The top-tier providers offer comprehensive solutions for virtually any cloud computing needs with multiple cloud service locations to ensure maximum survivability.

Figure 1: Cloud Service Providers



- **Disaster recovery (DR)**—a set of policies and procedures to enable recovery of critical technology infrastructure and systems following a major outage or disaster. DR’s main goal is to protect data and ensure that business can resume as quickly as possible following an event.
- **Business continuity (BC)**—the ability to continue to deliver services at a predefined level following an outage or disaster. Whereas DR allows you to protect data and rebuild, BC allows you to continue running through the outage or as soon as possible thereafter depending on the specific events.
- **Colocation data center**—a third-party data center where rack space can be rented to host physical hardware such as servers and appliances. Colocation data centers have a rating supplied by the Uptime Institute to let you know how much uptime you can expect. The ratings range from Tier I to Tier IV, with the highest tier providing the highest uptime and fault tolerance.
 - Tier I: Minimum of 99.671 percent availability, with no redundancy in power, cooling, or network
 - Tier II: Minimum of 99.741 percent availability; N+1 redundancy in power and cooling

- Tier III: Minimum of 99.982 percent availability; N+1 redundancy in power, cooling, and network, with multiple uplinks for data
- Tier IV: Minimum of 99.995 percent availability; 2N+1 redundancy in power, cooling, and network, with multiple uplinks for data

Examples of Tier III and Tier IV data centers are Recovery Point's Gaithersburg Data Center and Switch's SUPERNAP, respectively.

- **Data egress and ingress**—data traffic in and out of the cloud. Egress data traffic comes from an external source into the cloud. Think of this as uploading data to the cloud, such as when backing up data to the cloud or synchronizing on-premises servers with servers in the cloud. Ingress data traffic comes from the cloud to on-premises servers. Think of this as the download of data from the cloud, such as in a data recovery from cloud storage or when accessing running servers in the cloud. The terminology is important because vendors charge different amounts per gigabyte depending on whether the data constitutes egress or ingress traffic.
- **Load balancers**—appliances that manage redundant systems, allowing users to be directed to different servers for the same data. For example, load balancing can be used for a SharePoint intranet site to point the user to one of two redundant SharePoint servers (e.g., Sharepoint1 or Sharepoint2) to balance the number of connections and bandwidth. A load balancer can also be used to point to one application or server primarily and point to a secondary one in the event of an outage.
- **Tapeless backup appliance**—an appliance designed to replace a tape backup system. Typically, these appliances consist of a large amount of storage to hold backups. The appliance also often has data management tools built in. Various backup appliances also have native support for many top-tier cloud service providers to ensure seamless data replication.
- **Warm or hot sites**—physical locations for DR and their availability. Warm sites consist of hardware and network connectivity to support production but are not 100 percent up to date, require manual intervention, and can take hours or days to bring online. Hot sites are duplicates of production environments with real-time synchronization; they run concurrently with the main production site. Switching to a hot site can take minutes to bring online.

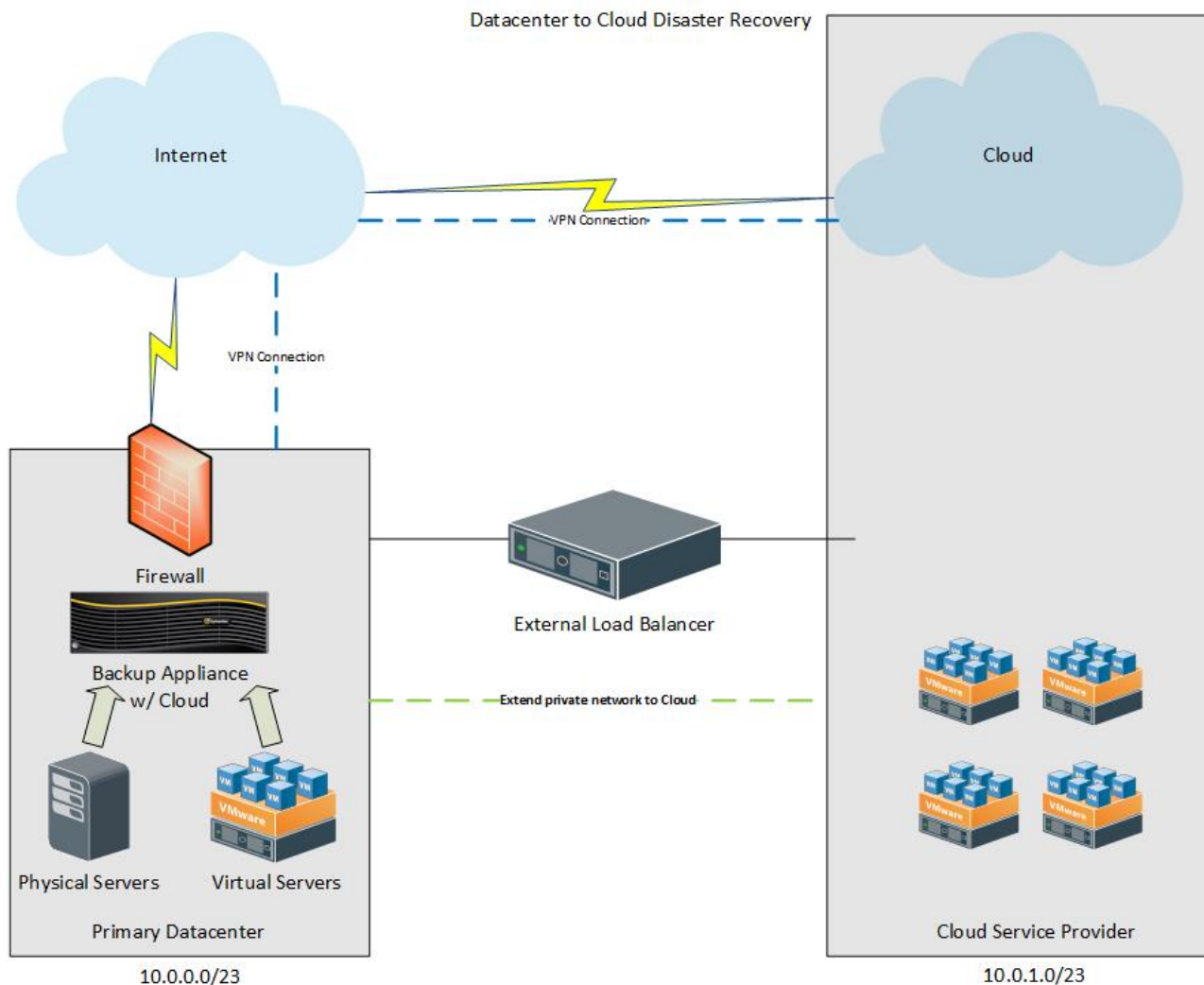
8.1 Single-Site Small or Medium JBE

8.1.1 Scenario 1: Cloud-based DR

Cloud-based **DR** is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow

JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

Figure 2. Cloud-Based DR Diagram

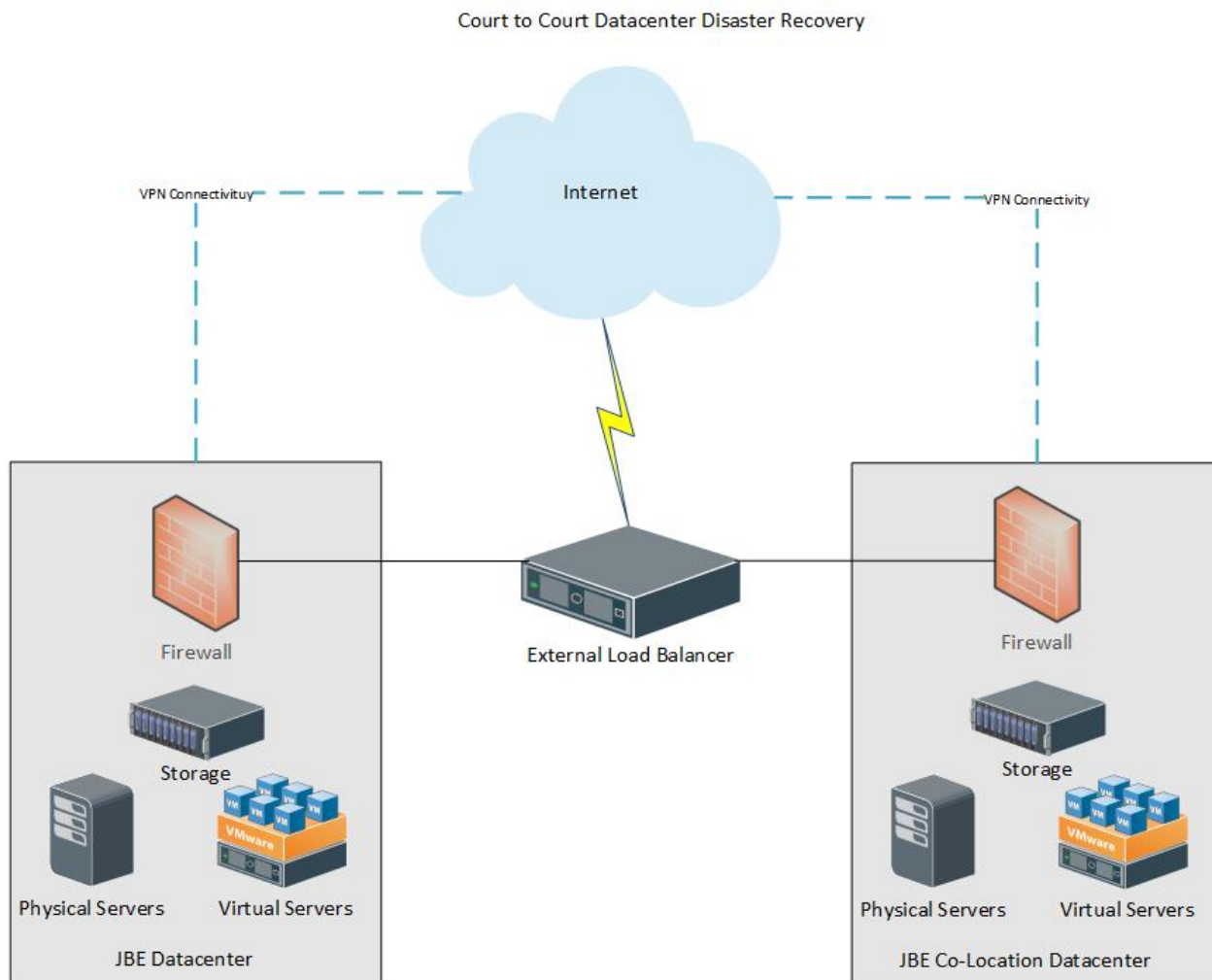


8.1.2 Scenario 2: Court-to-court colocation

Court-to-court colocation involves two similar courts in geographically diverse locations. A memorandum of understanding needs to be put into place to accommodate the complexities of this option. Implementation of this type of agreement requires a JBE to lend or borrow space in a JBE data center for racks of equipment. The JBE has to put a dedicated data circuit in the borrowed data center of an appropriate size based on requirements. In this scenario, each critical server or appliance requires a similar hardware setup, whether physical or virtual. In addition, replication has to be implemented and managed for SQL, data, and other servers. Network components also need to be in place to allow the JBE to route to the **warm or hot** redundant **sites**. Several appliances and tools can assist with running a **warm or hot site**. **Load balancers** are crucial for routing to allow the JBE to point its

server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer**. Other options such as hosted websites and tools that may be unavailable in the event of a disaster or outage can help in moving production.

Figure 3. Court-to-Court Colocation Diagram



8.2 Medium or Large JBE With Two or More Sites in Close Proximity

8.2.1 Scenario 1: Cloud-based DR

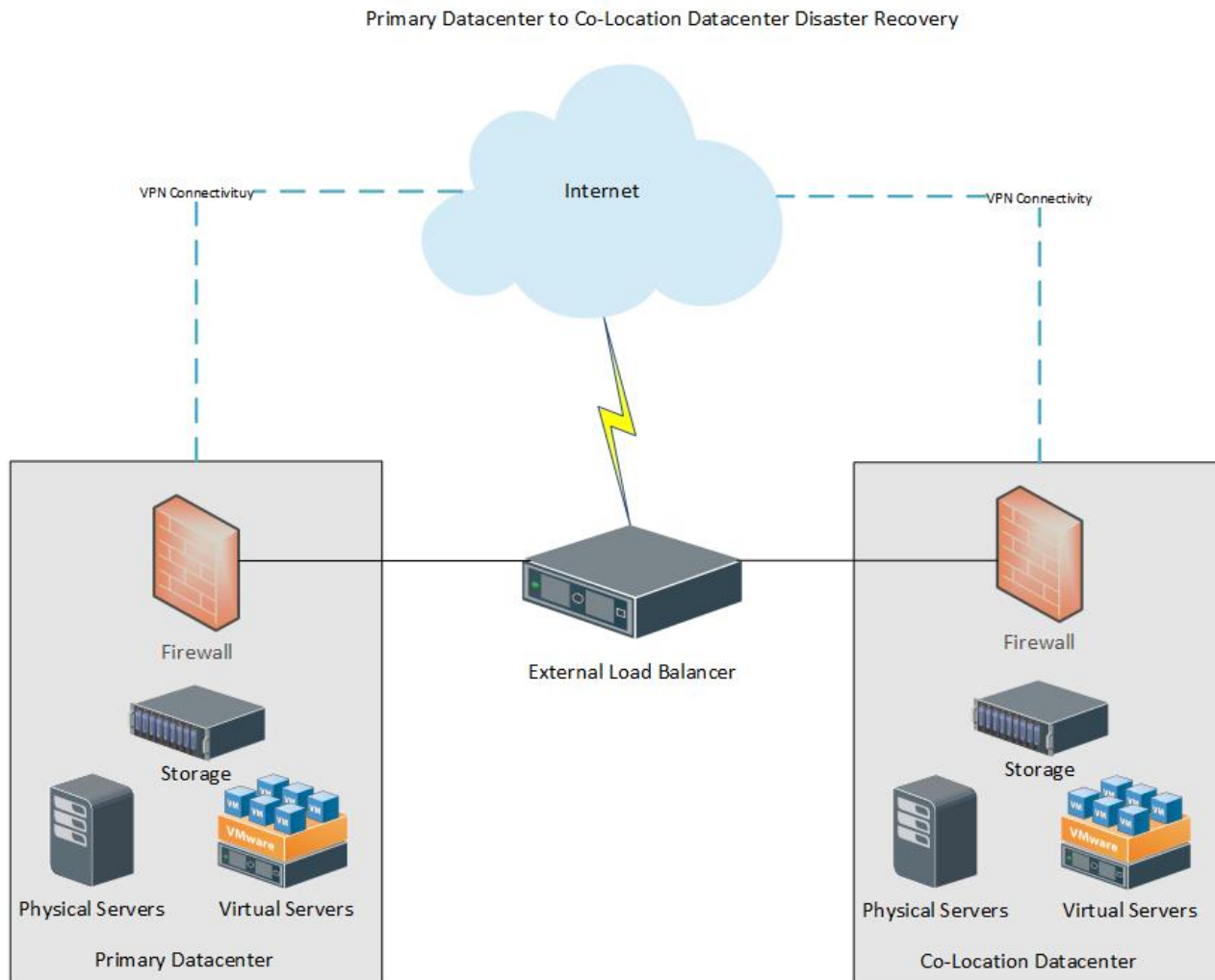
As stated in section 8.1.1, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to

allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters. Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.2.2 Scenario 2: Colocation data center

In this scenario, a JBE uses a third-party data center to host the physical and virtual servers and appliances. Using a **colocation data center** to host data requires the JBE to install a dedicated circuit (sized appropriately per requirements) at both locations to ensure full data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication and synchronization has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites**. **Load balancers** are crucial for routing to allow the JBE to point its server addresses to different IPs. These appliances can be set up so that if one of them is down, the external IP addresses can route to a standby **load balancer** hosted at the **colocation data center**. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 4. Colocation Data Center Diagram



8.3 Medium or Large JBE with Two or More Sites NOT in Close Proximity

8.3.1 Scenario 1: Cloud-based DR

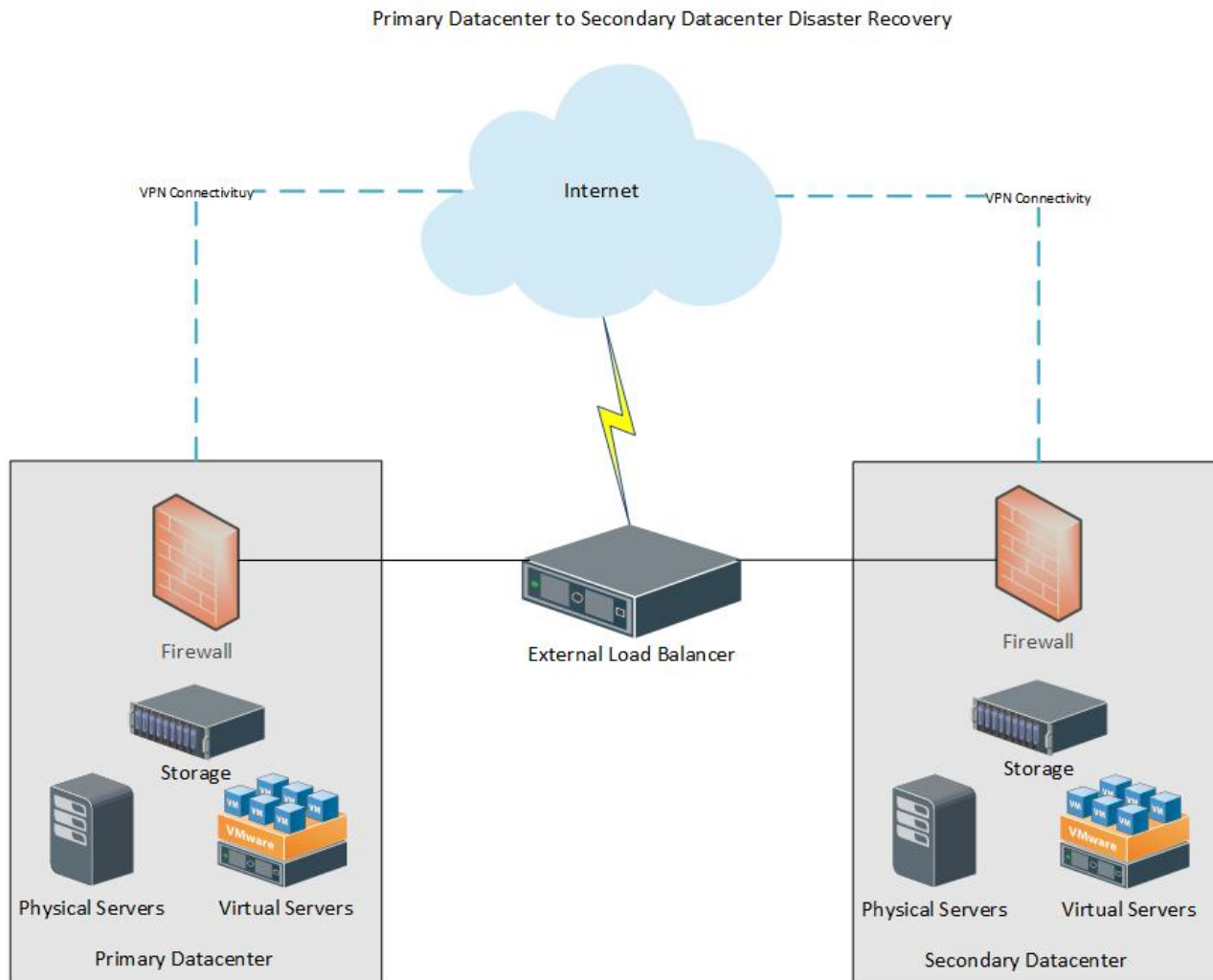
As with single-site JBEs and those with two or more sites in close proximity, cloud-based **DR** (see figure 2, above) is the preferred **DR/BC** scenario for JBEs with two or more sites *not* in close proximity. Depending on business need, the cloud can be used as offsite storage to replace tape backups; as a **public cloud** or **private cloud** for storage, replacing or supplementing the local SAN; or for **business continuity**, encompassing the **public cloud** and **private cloud** and introducing aspects of the **hybrid cloud** to allow virtual servers to be synchronized on the cloud and turned up as needed during outages or disasters. **Cloud service providers** allow JBEs to replace tape backups, store tapes offsite, and virtualize data stores and critical servers and put them up on the cloud for a monthly fee plus **data ingress and egress**. The data are accessible for daily use, for recovery, or during outages and disasters.

Additionally, servers can be switched from standby to active in minutes and reached as long as the Internet is accessible, functioning in the same manner as physical or virtual servers onsite. A dedicated Internet circuit (sized based on data requirements) is required to ensure that data and servers are replicated to cloud services regularly. To simplify management of data on the cloud and facilitate replication and synchronization, several types of **tapeless backup appliances** can be implemented to ensure data integrity in the cloud. And with top-tier **cloud service providers**, the JBE can often extend the internal network to the cloud, in concert with a **load balancer**, which can make failover significantly less painful.

8.3.1 Scenario 2: Secondary-site data center

A **secondary-site data center** is similar to a **colocation data center**. It uses a secondary court site as a redundant data center, which typically requires an increase in bandwidth at the secondary site as well as a dedicated data circuit (sized appropriately per requirements) between the two data centers to ensure data replication and synchronization. Each critical server requires a similar hardware setup, either physical or virtual. In addition, replication has to be implemented and managed for SQL, data, and other services. Network components also need to be in place to allow the JBE to route to the **warm or hot sites**. **Load balancers** are crucial in this scenario to allow the JBE to point its server addresses to different IPs. These addresses can be set up so that if one of them is down, the external IP addresses can route to the standby **load balancer** located at the secondary site as needed. Other considerations include hosted websites and tools that may be unavailable in the event of a disaster or outage.

Figure 5. Secondary-Site Data Center Diagram



9.0 PLANNING

As with any organizational undertaking, planning is an essential element in developing a solid and useful disaster recovery plan. The JBEs in California operate within a vast range of geographical, urban, and rural environments; earthquake zones and wildfire areas; and adjacencies to other JBEs. The California JBEs have varying caseloads and case types and diverse physical plants. Each possesses automation and other mission-critical support systems that differ in small or large ways from those of neighboring JBEs. For these reasons, a one-size-fits-all approach cannot work and, therefore, this document cannot specify exactly how an individual court should approach the planning effort. Each court will have its own unique set of factors to consider in developing its disaster recovery plan.

Likewise, the relative size and complexity of each court's organizational and staffing components will largely dictate the formality of the planning effort. The smallest court unit may be able to

develop a viable plan with a relatively informal and simple effort, where a large urban court may need a more elaborate and formal approach.

An important element of any DR planning effort is to first identify and thereafter coordinate as appropriate with the court's stakeholders, including internal stakeholders (judicial officers, court managers and staff, and other elements of the court family) and external stakeholders (other agencies, bar groups and law firms, vendors, and utility providers, to name a few).

In this regard, each court needs to assess the extent to which its stakeholders should be represented and involved from the outset and the level and extent of their continuing involvement throughout the planning phase. As has already been noted, what is optimal for a small rural court will likely differ significantly from what is optimal for a large urban court. Hence, stakeholder involvement should be as large and diverse as resources and practicality permit. Disaster recovery planning is most definitely an area where more stakeholder involvement is better than less.

10.0 IMPLEMENTATION

The fate of most policy and procedure manuals is to be placed on a bookshelf to gather dust. Most manuals are intended primarily for reactive reference: A discrete question comes up and a manual is pulled down from the shelf, consulted, and put back to gather more dust. Mostly, however, it stays on the shelf until a question arises.

A disaster recovery plan by its very nature, however, needs to be viewed and studied as a road map containing a cohesive set of well-thought-out procedures and steps for pre-disaster planning and preparations, continued operation during a disaster, and post-disaster response. It is intended as a tool for an organization to *prepare itself before a disaster*, as much as it is a road map for the recovery therefrom.

For this reason, it is important that the contents of the Disaster Recovery manual be widely disseminated and studied throughout the court. *All court stakeholders* who may be affected by a disaster and have a role in the recovery therefrom *should be made fully aware of the disaster recovery plan and its contents*.

As with the planning phase, described in section 9.0, the nature and extent of the dissemination and study will vary from court to court based on each court's individual environment and situation. In a small court, implementation might consist primarily of an all-hands meeting to review it and respond to questions and concerns. In the largest JBEs, such an approach is unlikely to prove practical or effective, and a more formal and involved process will be required.

11.0 KEY POINTS, CONCERNS, AND COMPLIANCE

11.1 Limited Access to & Security Controls for Backup Systems

Strict security controls and safeguards should be put into place to limit administrative access to backup systems and therefore prevent, or at a minimum – mitigate them from being compromised. Recent events, including two that have occurred in courts have further justified the importance of ensuring only one or few people (preferably executive management) maintain the master backup/recovery system(s) credentials, particularly related to access levels that allow for the backup system(s) and/or media to be wiped/deleted.

11.2 Backup of Microsoft Office 365 & Cloud Data

E-mail, hosted offsite and in Office 365, should be backed up by a trusted third-party backup service or product. Such cloud-to-cloud backups not only protect against catastrophic failure that Microsoft could experience in its data centers, but also protect the JBE against malicious or unintentional deletions of e-mail and allow for speedy recovery of e-mail. Likewise, all cloud-based OneDrive and SharePoint data including all other cloud-based critical data should be protected by a cloud-to-cloud backup solution.

11.3 Abandonment of Tapes

JBEs should be making reasonable efforts to separate from and decommission tape technologies for primary backup purposes, unless no other options are compatible with specific systems (e.g., AS/400). As budget and time permit, JBEs should also be looking to abandon tape backups *entirely*, including at secondary sites and for noncritical nonproduction data, and instead use the recommended backup media identified in this document. There are valid exceptions to this recommendation, such as if the expense and/or feasibility of increasing bandwidth to support modern backup solutions are beyond reach. JBE's can also consider cost saving approaches by repurposing production backup tape systems to be used at a secondary site or for lab/test environments. Another valid exception is to use tape as a "last resort" in case any JBE prefers to have one physical (portable) backup set on physical medium that can be securely stored.

11.4 Use of Primary SAN or Array

JBEs should never use their primary SAN and/or primary storage arrays for backup purposes. The backup environment, other than network, should be kept 100 percent separate from production storage and/or computing platforms. The only exception is for staging, test, or development systems, where a loss would not affect business operations.

11.5 Use of Virtualization Cluster

JBEs should never use their virtualization clusters, specifically a cluster served by the primary SAN or array, for backup purposes. The backup environment should be kept 100 percent separate from other resources or depend on them as little as possible.

11.6 Retention of Data (Backups)

Choosing what data to retain and how long to retain it for is a very JBE-specific decision and depends on local operating principles, local SLAs, budget for appropriate backup resources, infrastructure, and laws and rules. As with document destruction, an appropriate backup architecture should be implemented at a court that supports the JBE's retention and/or destruction requirements and aligns to the business drivers to which the JBE has committed.

****IMPORTANT NOTE**** With recent catastrophic and visible events in industry where data hostage and data corruption situations have occurred, it is of utmost importance that JBE's completely understand the architecture and working principals of their backup and DR system(s) to mitigate any chances of corruption and/or maliciously encrypted data being the only backup copy of a JBE's data. In order to avoid such a situation (e.g. sleeper code, or maliciously encrypted data), a JBE may wish to keep full copies of backups for certain periods of time and taken at different intervals (e.g. 6 months, 12 months, etc.), and 100% isolated from the production network.

11.7 Data Classifications

This framework covers the process and methods for data classification only in part, because that focus is typically a balancing act between compliance, discovery, and protection. However, larger JBEs will find that classifying data will help reduce any consumption or utilization constraints around SANs, disks, backups, and high-availability solutions. The rules for data and compliance are very specific, and so at each JBE, intake and classification of the data from various sources, such as those that follow, are important:

- **Payment Card Industry (PCI).** Reference PCI resources and/or your merchant account provider for relevant information.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** Reference HIPAA resources and/or your local county for relevant information.
- **California Law Enforcement Telecommunications System (CLETS).** Reference CLETS documents or contact your CLETS contact for relevant information.

11.8 Purpose-Built Backup Appliance vs. Backup Server

The industry allows JBEs to select any available backup solutions that meet their needs and align to the Judicial Branch *Disaster Recovery Framework*. JBEs should assess their environments to select an appropriate backup solution that presents the fewest risks and is least disruptive to ongoing management efforts. Some backup solutions are designed as purpose-built appliances (non-Microsoft) rather than traditional Microsoft Windows servers with a backup software application installed. Purpose-built appliances are recommended over traditional Microsoft Windows backup servers because they are immune to or far less affected by common-environment outages (Microsoft's Active Directory and the like) and less susceptible to malware targeted specifically for Microsoft-based servers. In a crisis, dependencies can impede recovery activities and compromise a JBE's ability to focus on restoration of data.

11.9 Cloud Service Subscriptions and Payments

Based on how the California State Controller's Office (SCO) operates, in addition to the time it takes for invoices and approvals for payment to work their way through the process, payments to contracted vendors and organizations can often be delayed. Many vendors require payment in full within 30 days of receipt of goods (Net-30), whereas the SCO pays on terms of Net-45 at best. The delay of payment can introduce complications with JBE cloud service subscriptions. When a JBE contracts with a cloud service provider, the JBE should carefully review the contract and/or agreement terms and conditions regarding what happens with a customer's data following a delayed payment. For example, when the Legislature and Governor's Office experience delays approving the California budget, delays of payments have historically resulted for many vendors. Whereas local infrastructure is a capital expenditure and is less affected by delayed payments, cloud infrastructure and services are operating expenses and rely 100 percent on timely payments.

11.10 Uncompromised Access to Credentials for Recovery Systems and Cloud Platforms

It is essential for JBEs to plan and be prepared for the worst of circumstances. JBEs should implement a credentials locker, credentials list, and so on, and store them in a documented and secured location away from and off of any IT system or facility that could be compromised and result in the activation of a JBE's recovery plan. Should a JBE's IT environment be compromised based on an IT failure, facility failure, or natural disaster, uncompromised access to credentials is mandatory to ensure that the JBE can access its backups and other DR-related systems. The JBE's credentials should be kept alongside the JBE's disaster recovery plan. JBEs should always lean on a multifaceted approach to where mission-critical documentation (e.g., credentials and DR plan) is stored and located in case

access to anything and/or everything could potentially be impeded and/or permanently inaccessible until recovery.

12.0 MONITORING, TESTING, VALIDATION, AND REVIEW

A JBE's backup strategy and DR strategy (if applicable) should be comprehensively tested *at least* once per calendar year. The sophistication or simplicity of the DR solutions in place at each JBE is irrelevant to this recommendation. Of course, a JBE may choose to test more frequently if desired, and should implement a more frequent testing exercise if any uncertainty or lack of integrity exists with the backup and/or DR solutions in place.

12.1 Regular Review of Backup and Disaster Recovery Systems

12.1.1 E-mail notifications

E-mail notifications for alerts and other information should be set up in each system that makes up a JBE's DR solution. These e-mails should be reviewed regularly (e.g., daily) and checked for errors and completeness.

12.1.2 Backup job monitoring and auditing

A responsible person, persons, or team should be assigned the task of auditing all backup jobs on a JBE's backup system on a regular interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the backup and DR plan.

12.1.3 Site recovery/cutover systems monitoring and auditing

A response person, persons, or team should be assigned the task of auditing all site recovery systems on a regular/repeat interval. Doing so will ensure that any new systems brought into the environment have a second and certain chance of being captured within the site recovery and DR plan.

12.1.4 Gap Analysis

A gap analysis should be performed regularly (e.g. quarterly or within reason) to serve as a "catch-all" mechanism in addition to the above routine checkpoints. The gap analysis will also lend to ongoing refining of a JBE's backup and DR strategy and allow for continual planning, budgeting and changing.

12.2 Routine Testing Exercises

JBEs should establish a testing plan or testing effort and execute a routine testing exercise on a regular interval, but no less frequent than once per calendar year. Testing exercises help

provide peace of mind, but more important, they prove that backup and site recovery systems are working as designed and will work should they be needed in a real scenario. Although most systems allow for out-of-band testing and data-redirect without affecting production performance or data, outages may be required for testing and should therefore be included in the test plan.

12.3 Testing Simulations

12.3.1 Loss of building access

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of building access—specifically, the building that houses the JBE’s data center. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.2 Loss of access to all systems (onsite or offsite) based on catastrophic outage or disaster

In addition to routine and general types of testing, JBEs should run simulations that reflect real-life possibilities. One simulation is to react to a full loss of all systems either at the JBE’s primary data center, the cloud, or both. In this test, ideally, an IT team would consider working offsite or from another building.

12.3.3 Backup system failure

In addition to routine and general types of testing, JBEs should run simulations on recovering data when their primary backup appliances or systems have failed but all other production systems, including secondary replicas of backups, are operational.

12.3.4 High-availability (site recovery) system failure

In addition to routing and general types of testing, JBEs should run simulations on remediating systems in the event that their primary site recovery systems have failed and cannot function as designed.

APPENDIX A

LIST OF HIGH-LEVEL TECHNICAL REQUIREMENTS AND SYSTEMS/DATA CATEGORIZED BY RECOVERY TIME

RECOVERY-TIME DISCLAIMERS

- Recovery time depends on the following:
 - The actual disaster (severity)
 - Whether the facility or physical access is affected, including safety situations (e.g., hazmat, fire, smoke)
 - Staff capacity and availability
 - Replacement equipment (if applicable)
 - Conflicting DR recovery commitments or plans (e.g., CCTC or other data centers/cloud)
 - Recovery actions, such as abrupt responses that could lead to some or significant permanent data loss based on available backups, the approach taken for data restoration, and/or disaster recovery site cutovers
- Fault tolerance is typically costly and requires additional hardware and software.
- Some functionality or components are built into other component systems (overlap of functionality).
- Time to recover (TTR) is the maximum recommended/defined outage time for purposes of implementing priorities for data recovery and outage mitigation.
- Hardware items on the end-user side of IT (e.g., printers, desktops, scanners, barcode readers, etc.) have not been included because they are considered end-user equipment and are outside the scope of the disaster recovery framework.

HIGH-LEVEL TECHNICAL REQUIREMENTS

- TTR of 12 hours maximum
- Infrastructure (network, Active Directory (AD), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP))
- Shared/combined storage (SAN, etc.)
- Virtual hypervisor/platform
- Backup solution/platform
- Wi-Fi

- Load balancers
- Reverse proxy

BUSINESS RECOVERY REQUIREMENTS (EXAMPLES OF SYSTEMS AND SERVICES)

The tiers below align with the judicial branch Next Generation Hosting Strategy Workstream's output, except in ways that clearly delineate how approaches to disaster recovery differ from hosting and uptime, given that all are interrelated and depend on one another for the reliability and protection of data.

- **TIER 1—HIGH** priority; TTR (not considering disclaimers) of 12 to 48 hours maximum; and systems and services as follows:
 - VoIP
 - Case Management Systems (CMS)
 - Document Management Systems (DMS)
 - File servers (holding judicial, executive, human resources, finance, and IT data and documentation)
 - E-mail (systems dependent on e-mail, such as alert and public communication systems), Microsoft Office 365, and others
 - Public website (hosted on-premises or offsite); important for a mechanism to broadcast information to the public and for the public to send or input data to the court; the portal at each court
 - Electronic reporting, docket, and minutes
 - Jury management system (JMS)
 - Virtual private network (VPN)
 - Electronic Probable Cause Declaration (ePCD)
 - Electronic Search Warrants (eWarrant)
 - Interfaces (interagency; some e-filing)
 - Building access control (e.g., Identiv, Schneider Electric)
 - Finance systems on-premises
 - Human resources systems on-premises, time card systems, Phoenix/SAP
 - Jury instructions
- **TIER 2—MODERATE** priority; TTR (not considering disclaimers) of 48 to 72 hours maximum; and systems and services as follows:
 - Intranets
 - File servers (holding less- or moderately important data)
 - Print servers
 - Building automation system
 - California Courts Protective Order Registry
 - CLETS
 - Department of Motor Vehicles access, controls or interface

- Other interfaces: various justice partners (e.g., Franchise Tax Board, Department of Justice, district attorney, police department, California Highway Patrol, sheriff, etc.)
- Site control (elevator controls, door controls, etc.)
- Electronic transcript assembly tools/software
- Interactive voice response (traffic, jury, etc.)
- Electronic signing product/solution
- Middleware
- Reporting systems (not built into CMS, but standalone)
- **TIER 3**—LOW priority; TTR (not considering disclaimers) of 168 hours maximum; and systems and services as follows:
 - IT tools and unique IT management systems (e.g., help desk, logging, controls, and network/system/application monitoring)
 - Video surveillance
 - Meeting systems (WebEx, Skype, etc.)
 - Digital signage
 - Queuing systems
 - Mobile device management

APPENDIX B

RECOMMENDED MINIMUM REQUIREMENTS FOR A BACKUP SOLUTION

Note: Tape should never be used as the primary backup medium.

- Disk-based
- Cloud-based
- Cloud-to-cloud backup capabilities for Microsoft Office 365 (e.g., OneDrive, SharePoint, Exchange Online) backups
- Sufficient Internet bandwidth for cloud and/or remote backups
- Scalable (can grow as court grows without large, repeated capital expenditures)
- Granular backup and restoration (e.g., exchange items in mailboxes, SQL objects, individual files)
- Ability to create multiple schedules
- Ability to notify or alert IT staff of problems
- Ability to verify backups
- Ability to restore to a different backup target
- Ability to encrypt sensitive or classified data or information
- Ability to audit all changes made to the backup system, backup jobs, schedules, etc.
- Ability to create multiple backup jobs
- Ability to create backup schedules with multiple backup targets
- Ability to replicate *offsite*:
 - To the cloud
 - To a secondary backup system
 - To a removable or portable disk
 - To tape (*as last resort*)
- Ability to initialize or mount a backed-up virtual machine in the cloud (specific for cloud backup solutions)

CALIFORNIA JUDICIAL BRANCH

Disaster Recovery Plan

Superior Court of [Insert Court Name]

VERSION 1.5

OCTOBER 12, 2017



JUDICIAL COUNCIL
OF CALIFORNIA

INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

*For internal use only. Please to do not distribute or forward
to individuals outside the judicial branch.*

Table of Contents

- 1.0 INTRODUCTION 1
 - 1.1 Definitions 1
 - 1.2 Purpose 1
 - 1.3 Applicability 2
 - 1.4 Scope..... 2
 - 1.5 Disaster Recovery Plan Phases 3
 - 1.6 Assumptions 4
- 2.0 DISASTER RECOVERY APPROACH 4
- 3.0 COMMUNICATIONS PLAN 4
 - 3.1 Status Reporting..... 5
 - 3.1.1 Pre-Declaration..... 5
 - 3.1.2 Post-Declaration and Coordination 5
 - 3.1.3 Post-Declaration and Onsite Execution..... 6
 - 3.1.4 Post-Disaster..... 6
- 4.0 DISASTER RECOVERY TEAM POSITIONS AND ASSIGNED ROLES AND RESPONSIBILITIES 6
 - 4.1 Disaster Recovery Manager..... 6
 - 4.2 Account Manager..... 6
 - 4.3 Executive Management—[Court Name] 7
 - 4.4 Executive Management—[External DR Provider Name] 7
 - 4.5 Backup Administrator..... 7
 - 4.6 Storage Administrator..... 7
 - 4.7 Network Administrator 7
 - 4.8 Network Software Support 8
 - 4.9 Unix Administrator 8
 - 4.10 Windows Administrator..... 8
 - 4.11 Applications Software Support..... 8
 - 4.12 Database Support 8
 - 4.13 Middleware Support 9
 - 4.14 Service Desk 9
 - 4.15 Emergency Operations Center 9
 - 4.16 Training, Testing, and Exercising the Disaster Recovery Team 9
- 5.0 DISASTER RECOVERY PLAN 10
 - 5.1 Site Evacuation 10
 - 5.1.1 Evacuation Procedure..... 10
 - 5.2 Notification and Activation Phase 10

5.2.1	Notification Procedures	10
5.2.2	Establish Crisis Management Center	10
5.2.3	Incoming Telephone Call Procedures	10
5.2.4	Alert External Service Provider(s)	10
5.2.5	Activate Conference Bridge	10
5.2.6	Notify Help Desk	10
5.2.7	Notify Alternate Hosting Facility(s)	10
5.2.8	Alert Offsite Data Vaulting Facility.....	10
5.2.9	[Continue as needed]	10
5.3	Assessment and Reporting Phase	10
5.3.1	Damage Assessment Phase	10
5.3.2	DR Team Report Recommendations to the DR Manager.....	10
5.4	Strategy Review and Declarations Phase	11
5.4.1	Review Recovery Strategies.....	11
5.4.2	Information Technology Strategy	11
5.4.3	Criteria.....	11
5.4.4	Declaration	11
5.5	Post-Declaration Activation and Administrative Phase	11
5.5.1	Activation Decision.....	11
5.5.2	Personnel Activation and Notification Procedures	11
5.5.3	Administrative Procedures	11
5.5.4	Tape Shipping Methodology.....	11
5.5.5	Put Vendors on Notice	11
5.6	Continuity of Services and Initial Recovery Phase	11
5.6.1	Recovery Phase	11
5.7	Return Phase	11
5.7.1	Return to Production Site	11
5.7.2	Approach for Plan Deactivation.....	12
5.7.3	Preparedness Phase	12
6.0	DISASTER RECOVERY PLAN TESTING	12
6.1	Objectives	12
6.2	Scheduling	12
6.3	Success Criteria	12
6.4	Noncontributing Factors	12
6.5	Environmental Change Coordination	12
7.0	PERSONNEL ACTIVATION AND NOTIFICATION PROCEDURES; TELEPHONE LOG...12	
8.0	CALL LISTS	12
9.0	APPLICATIONS TECHNICAL RECOVERY PLANS.....	12
10.0	APPENDIXES.....	12

10.1 Appendix B: [contact list].....12
10.2 Appendix I: [worksheet—DR Team Positions].....12

1.0 INTRODUCTION

This disaster recovery plan identifies the steps to recover the Superior Court of [court name] County technology infrastructure housed at [court location].

1.1 Definitions

This plan references the following definitions:¹

- **Business continuity plan:** The documented arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period and to return to performing its critical functions after an interruption. The business continuity plan is not a component of the disaster recovery plan. A business continuity plan is also referred to as a continuity of operations plan (COOP).
- **Disaster:**
 - A sudden, unplanned catastrophic event causing unacceptable damage or loss.
 - An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time.
 - An event where an organization's management invokes their recovery plans.
- **Disaster recovery (DR):** The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.
- **Disaster recovery plan:** The management-approved document that defines the resources, actions, tasks, and data required to manage the technology recovery effort. The disaster recovery plan is a component of the business continuity plan.
- **Disaster recovery planning:** The technical component of business continuity planning.
- **Disaster recovery team:** The main group of personnel in charge of the recovery effort.

1.2 Purpose

This disaster recovery plan mitigates the risk of system and service unavailability by providing written-response solutions for the prompt and effective continuation or resumption of mission-critical services in the event of a disaster.

¹ The definitions in this section are adapted from the glossary provided by *Disaster Recovery Journal* at www.drj.com/resources/tools/glossary-2.html (as of May 17, 2017) and used with permission.

The purpose of this plan is to establish a process to relocate critical systems on substitute hardware at a geographically dispersed site in a timely, well-orchestrated manner.

In addition, this plan has a preventive component that fulfills Presidential Decision Directive 63 on Critical Infrastructure Protection (see 63 Fed. Reg. 41804 (Aug. 5, 1998)), which requires federal agencies to identify mission-critical infrastructure components and develop a plan to protect them.

It is important to note that this disaster recovery plan is a component of business continuity.

1.3 Applicability

This disaster recovery plan applies to facility-level disruptions. A *facility-level disruption* is an event that renders a facility inoperable. This catastrophic scenario requires the availability of information technology resources to restore services at the alternate site in [location].

This plan applies to the continuity, recovery, and reconstitution of the [court name] housed at [location] and not to the specific business functions performed by the various units within the court. The business functions are the responsibility of the executive management at each division(s), which develop and execute business continuity and continuity of operations plans, as well as business recovery plans.

1.4 Scope

This disaster recovery plan focuses on the recovery and continued operation of system components that support mission-critical systems and mission-essential services in the event of a disaster.

For the purposes of this plan, a *disaster* is a major incident that seriously disrupts or is expected to disrupt operations for 24 hours or more and requires:

- the reassignment of personnel to disaster recovery activities;
- the use of additional vendor/contractor support to accomplish recovery requirements; and/or
- the acquisition of special funding to support equipment replacement and other recovery-related costs that are outside the scope of normal day-to-day operations.

If the level of effort required to accomplish these requirements falls within the scope of a disaster as defined above, then a disaster declaration should be issued, and disaster recovery plan processes and procedures should be initiated. If the level of effort required does not, then the [court IT unit] should conduct the recovery actions as part of day-to-day operations.

1.5 Disaster Recovery Plan Phases

This disaster recovery plan establishes action steps and clear lines of responsibility for recovery efforts. The plan consists of the following phases:

- **Site evacuation.** If necessary, the disaster recovery manager (DR Manager) will order the evacuation of the [court facility] data center and turn over the control of the equipment within the facility to [alternate facility].
- **Notification and activation phase.** In this phase, members of the disaster recovery team (DR Team) are notified and the DR Manager is notified to activate the team.
- **Assessment and reporting phase.** DR Team members report to the scene, evaluate conditions, and develop a formal recommendation for the DR Manager on whether to declare a disaster.
- **Strategy review and declaration phase.** This phase includes procedures for finalizing strategies and recovery actions and for declaring a disaster.
- **Post-declaration activation and administrative phase.** This phase provides procedures for notifying personnel, offsite storage retrieval, travel, and personnel scheduling. It also provides a form for documenting personnel locations and requesting travel arrangements.
- **Continuity of services and initial recovery phase.** If directed by the DR Manager, the DR Team will take action to quickly recover and continue providing the [court name] data center housed at [court facility] services to the extent allowed by conditions and, if necessary, at a degraded level until the restoration of normal operations. If conditions warrant, the DR Team will relocate and recover the [court name] data center housed at [court facility] operations at the alternate site in [location].
- **Full recovery and reconstitution of normal operations phase.** As conditions stabilize, the DR Team will take action to reestablish the [court name] data center housed at [location] operations to the [alternate location] facility. Depending on the damage that occurred, [court entity] will repair facilities, repair damaged equipment, return platforms to operation, reload applications, re-initiate network connectivity, and restore normal computer operations and associated procedures. If the site is not salvageable, an alternate site will be selected and reconstructed to a level equivalent to that of the original site.
- **Return phase.** This phase includes instructions for salvage and media reclamation activities as well as site restoration.
- **Preparedness phase.** This phase includes guidelines for updating the plan, testing the plan, and validating information within the plan (e.g., contact names, vendor names, and plan currency).

1.6 Assumptions

- The disruption disables only the [primary facility name] site; the [secondary site name] is unaffected.
- Offsite storage locations for critical backup files and information are intact and accessible.
- The recovery is performed in accordance with the procedures that have been set forth within this disaster recovery plan.
- A sufficient number of qualified personnel are available to perform recovery responsibilities.
- Backups and rotation practices are performed as scheduled.
- The backup and recovery strategies are performed as implemented and tested.
- Entities external to the company, such as customers, vendors, government agencies, and others, are reasonably cooperative during the recovery period.

2.0 DISASTER RECOVERY APPROACH

The [court name] disaster recovery approach provides a [describe model here].

3.0 COMMUNICATIONS PLAN

The key to the successful implementation of this disaster recovery plan is overcoming the technical hurdles to reestablishing production systems at the [primary court hosting facility]. However, to coordinate within any business continuity plan, proper communication throughout the execution is critical.

- **E-mail.** E-mail will be one of the primary communication methods due to the speed of transmission and the ability to disseminate information to a large audience quickly. However, because e-mail is dependent on hardware and network functionality, this medium may not be available during a declared disaster.
- **One-on-one phone call.** At times, immediate acknowledgment of the communication or interactive decision making between individuals is required. In those situations, voice calls are preferred.
- **Conference bridge.** Upon the declaration of a disaster, a conference bridge for conference calls will be set up. This is the preferred method for facilitating quick, interactive, multi-party decisions.
- **Text message.** Text messaging is an alternative method for providing status reports or for quick, two-way communications between individuals.

- **Status line.** A status line provides a listen-only, updatable, recorded status message accessible by all stakeholders. This method is effective for secondary stakeholders who do not need continuous, up-to-the-minute status reports.

During a declared disaster, all communications will require an acknowledgment to ensure receipt of the information. Each communication should provide instructions for acknowledgment.

3.1 Status Reporting

3.1.1 Pre-Declaration

Depending on the nature of the disaster, before declaration there may be an executive conference call to discuss whether the event warrants a disaster declaration. An example scenario is if a nearby chemical spill required the evacuation of the data center. Since the duration of such an evacuation would be unknown, a conference call would be appropriate to discuss options available other than a declared disaster.

3.1.2 Post-Declaration and Coordination

After a declaration, status reports will immediately commence. Within the first 24 hours, the [responsible court IT unit, e.g., service desk] will be the primary center for all communications. Immediately upon declaration, the Emergency Operations Center (see section 4.15) will open a conference bridge and it will remain open until the DR Manager requests the bridge be turned off.

The [responsible court IT unit] will begin contacting individuals as described in Appendix B.

Because of the dynamic nature of staffing, the [responsible court IT unit] will contact [appropriate court management and executive staff] within the [court name]. Anyone on the conference call can then request that other individuals be contacted to join the call.

After declaration, the DR Manager will announce a conference call for the first status meeting. This meeting should take place upon completion of notifying all key stakeholders and contacts, but no more than 3 hours after disaster declaration. The meeting will provide answers to the following questions:

- What is the extent of the disaster?
- What resources are incapacitated?
- Who is on the DR Team?
- What is the estimated arrival time of the restoration media, such as disk(s), replica appliance(s) or pulling down backup data from a remote or cloud location at [alternate facility name]?

- What are the status reporting expectations during the interval between this call and arrival onsite?

3.1.3 Post-Declaration and Onsite Execution

As soon as the DR Manager arrives onsite (where “onsite” may be in the form of establishing a conference call line), he or she will send status reports minimally every 4 hours via e-mail and text message, or as required or requested. In addition to the scheduled status reports, the disaster recovery plan requires reporting the completion of certain milestones.

The DR Manager will hold a conference call 6 hours after the recovery efforts have begun to discuss the progress made and any issues. During this call, the time of the next conference call will be determined.

Other status reporting mechanisms may be used as deemed appropriate throughout the declaration.

3.1.4 Post-Disaster

To declare the end of a disaster, the DR Manager will establish a conference call to communicate to the DR Team the end of the disaster.

4.0 DISASTER RECOVERY TEAM POSITIONS AND ASSIGNED ROLES AND RESPONSIBILITIES

Appendix I contains a worksheet listing the names of individuals in each of the roles described below. (Note that a team member may take on more than one role, just as more than one team member may be required to execute a single role.)

4.1 Disaster Recovery Manager

When a disaster or disaster drill condition is declared, the DR Manager will be the focal point for all disaster recovery activities. The primary responsibility of the DR Manager is to ensure the successful execution of the disaster recovery plan. To be successful in that task, the DR Manager will be the focal point for all communications.

Throughout the year, the DR Manager will also be responsible for maintaining the disaster recovery plan.

4.2 Account Manager

During a declaration, the Account Manager will be a primary stakeholder for all communications. This role will be an escalation point for all parties. The Account Manager will work closely with the DR Manager to ensure clear and accurate communications with

the [Court Name] Executive Management. The Account Manager will also mediate decision making between [designated entities].

4.3 Executive Management—[Court Name]

During a declaration, the [court name] Executive Management Team will be a co-primary stakeholder for all communications.

4.4 Executive Management—[External DR Provider Name]

During a declaration, the [external DR provider] Executive Management Team will be a primary stakeholder for all communications. Depending on the severity and nature of the disaster, the Executive Management Team will play an integral role in communications between [designated parties].

4.5 Backup Administrator

During a declaration, the Backup Administrator will be responsible for assisting with rebuilding the environment at the [alternate facility name] facility and executing the procedure to restore the systems from the backup media.

Throughout the year, the Backup Administrator will be responsible for maintaining backup hardware, backup applications and backup schedules and strategies, including the backup and data restore processes.

4.6 Storage Administrator

During a declaration, the Storage Administrator will be responsible for assisting with rebuilding the environment at the [alternate facility name] facility and executing the procedure to restore the systems from the production [backup data source].

Throughout the year, the Storage Administrator will be responsible for maintaining the storage area network replication and restore process.

4.7 Network Administrator

During a declaration, the Network Administrator will be responsible for ensuring connectivity to all necessary resources. This will include all tasks required to ensure network communications between the [alternate facility name] site and the end users. In the case of multiple network administrators, the primary responsibility for connectivity lies with the company designated as owning network functions.

Throughout the year, the Network Administrator will be responsible for maintaining the network restore process.

4.8 Network Software Support

When a disaster or disaster drill condition is declared, the Network Software Support Analyst will work with the Network Administrator to implement changes necessary to accommodate the recovered systems' connectivity to the [court name] environment. They will monitor and work to resolve any issues that may arise during the recovery period.

4.9 Unix Administrator

When a disaster or disaster drill condition is declared, the Unix Administrator will be responsible for the operational restoration of all Unix platform servers. The Unix Administrator will work closely with the Backup Administrator to ensure the proper restoration of data at the right time. In addition, the Unix Administrator will be responsible for the hardware verification.

Throughout the year, the Unix Administrator will be responsible for maintaining the Unix system restore process.

4.10 Windows Administrator

When a disaster or disaster drill condition is declared, the Windows Administrator will be responsible for the operational restoration of all Intel platform servers. The Windows Administrator will work closely with the Backup Administrator to ensure the proper restoration of the data at the right time. In addition, the Windows Administrator will be responsible for the hardware verification.

Throughout the year, the Windows Administrator will be responsible for maintaining the Windows system restore process.

4.11 Applications Software Support

When a disaster or disaster drill condition is declared, the Applications Software Support Analyst will work closely with the Backup Administrator to ensure the proper restoration of the data at the right time. They will monitor and work to resolve any issues that may arise during the recovery period.

4.12 Database Support

When a disaster or disaster drill condition is declared, the Database Support Analyst will work with the Applications Software Support Analyst to implement changes necessary to accommodate the recovered systems connectivity to the [court name]. They will monitor and work to resolve any issues that may arise during the recovery period.

4.13 Middleware Support

When a disaster or disaster drill condition is declared, the Middleware Support Analyst will work with the Applications Software Support Analyst to implement changes necessary to accommodate the recovered systems' connectivity to the [court name]. They will monitor and work to resolve any issues that may arise during the recovery period.

4.14 Service Desk

During a declaration, the [responsible court IT entity, e.g., service desk] will play a pivotal role in communications for the first 24 hours of the declaration. The [responsible court IT entity] will be the first point of contact by anyone working on the disaster recovery plan. The [responsible court IT entity] will then execute a communications plan to notify all parties involved and to set up the initial conference call. In addition, working with the DR Manager, the [responsible court IT entity] will be the central repository for all incoming information and will have all of the following readily available:

- Status of the declaration event
- List of incapacitated assets
- Status of team formation
- Travel plans for all traveling team members

4.15 Emergency Operations Center

The Emergency Operations Center is the location identified for the assembly of the DR Team immediately following the declaration of a disaster. The DR Team will manage and coordinate recovery and reconstitution activities from this location. It is also where the DR Team will meet, whether in person or through a communications medium, to report the status of their actions.

The Emergency Operations Center will be located in the [location name], if feasible. If an alternative location is chosen, the DR Team will clearly communicate that location to all invested parties.

4.16 Training, Testing, and Exercising the Disaster Recovery Team

New DR Team members will learn the disaster recovery processes and procedures by virtue of trainings and knowledge transfer exercises. The DR Manager will provide members with up-to-date copies of this disaster recovery plan. The DR Manager will also periodically test DR Team members on aspects of the disaster recovery plan policies, processes, and procedures that are unique to system operations and essential to recovery and reconstitution. The DR Manager will conduct annual formal tests and exercises of the team. A disaster recovery plan evaluation form will be completed by a designated DR Team member

following each test or exercise, and the DR Manager will use the information to make any necessary modifications to refine plan processes and procedures.

5.0 DISASTER RECOVERY PLAN

[Document the steps needed to complete the recovery of the primary hosting facility to an alternate location]

5.1 Site Evacuation

5.1.1 Evacuation Procedure

5.2 Notification and Activation Phase

5.2.1 Notification Procedures

5.2.2 Establish Crisis Management Center

5.2.3 Incoming Telephone Call Procedures

5.2.4 Alert External Service Provider(s)

5.2.5 Activate Conference Bridge

5.2.6 Notify Help Desk

5.2.7 Notify Alternate Hosting Facility(s)

5.2.8 Alert Offsite Data Vaulting Facility

5.2.9 [Continue as needed]

5.3 Assessment and Reporting Phase

5.3.1 Damage Assessment Phase

5.3.1.1 Facility/site damage

5.3.1.2 Office and storage areas

5.3.1.3 Network capabilities

5.3.1.4 Platform damage and operability

5.3.1.5 Application status

5.3.1.6 Database status

5.3.1.7 Forms locations

5.3.2 DR Team Report Recommendations to the DR Manager

- 5.4 Strategy Review and Declarations Phase**
 - 5.4.1 Review Recovery Strategies**
 - 5.4.2 Information Technology Strategy**
 - 5.4.3 Criteria**
 - 5.4.4 Declaration**
- 5.5 Post-Declaration Activation and Administrative Phase**
 - 5.5.1 Activation Decision**
 - 5.5.2 Personnel Activation and Notification Procedures**
 - 5.5.2.1 Brief team members
 - 5.5.2.2 Track and schedule personnel
 - 5.5.2.3 Arrange travel and transportation
 - 5.5.3 Administrative Procedures**
 - 5.5.3.1 Ensure court policy
 - 5.5.3.2 Ensure employee well-being
 - 5.5.3.3 Monitor and report recovery process
 - 5.5.3.4 Act as advisor or liaison for recovery teams
 - 5.5.3.5 Maintain recovery-related record keeping
 - 5.5.3.6 Documentation of administrative procedures
 - 5.5.4 Tape Shipping Methodology**
 - 5.5.4.1 Retrieve offsite storage tapes and bins
 - 5.5.5 Put Vendors on Notice**
- 5.6 Continuity of Services and Initial Recovery Phase**
 - 5.6.1 Recovery Phase**
- 5.7 Return Phase**
 - 5.7.1 Return to Production Site**
 - 5.7.1.1 Oversee site restoration
 - 5.7.1.2 Interim or primary site restoration activities
 - 5.7.1.3 Site restoration checklist

5.7.2 Approach for Plan Deactivation

5.7.2.1 Post-disaster DR Team brief

5.7.2.2 DR Team deactivation

5.7.3 Preparedness Phase

5.7.3.1 Maintain preparedness

5.7.3.1.1 Maintain current recovery preparedness

5.7.3.1.2 Review and validate requirements and strategies

6.0 DISASTER RECOVERY PLAN TESTING

6.1 Objectives

6.2 Scheduling

6.3 Success Criteria

6.4 Noncontributing Factors

6.5 Environmental Change Coordination

**7.0 PERSONNEL ACTIVATION AND NOTIFICATION PROCEDURES;
TELEPHONE LOG****8.0 CALL LISTS****9.0 APPLICATIONS TECHNICAL RECOVERY PLANS****10.0 APPENDIXES**

10.1 Appendix B: [contact list]

10.2 Appendix I: [worksheet—DR Team Positions]

CALIFORNIA JUDICIAL BRANCH

How to Use the Disaster Recovery Framework

A Guide for the California Judicial Branch

VERSION 1.4

OCTOBER 12, 2017



JUDICIAL COUNCIL
OF CALIFORNIA

INFORMATION TECHNOLOGY
ADVISORY COMMITTEE

Table of Contents

1.0	Introduction	1
2.0	Background	1
3.0	Disaster Recovery Framework	2
3.1	Scope.....	2
3.2	Organizational Characteristics.....	3
3.3	Documentation Structure	3
4.0	Purpose of Disaster Recovery	5
5.0	Using the Framework	7

1.0 INTRODUCTION

This “How to Use” guide acts as a reference for Judicial Branch Entities (JBE’s) to assist them with establishing local policies and procedures based upon the Disaster Recovery Framework published by the Information Technology Advisory Committee, and the Judicial Council respectively. Since the framework was developed to establish a baseline disaster recovery approach at the branch level, this guide identifies the core purposes and sections of the Disaster Recovery Framework documents that are most relevant to JBE’s. JBE’s are not required to implement the framework in its entirety, rather the intent is to encourage JBE’s to use the framework as a template to develop disaster recovery strategies and procedures appropriate to their unique local business requirements. It is intended to be used as a guide, not a benchmark, of what should be done.

This guide is intended to provide a roadmap for JBE’s and does not include all the details required for implementing specific local backup and disaster recovery strategies and procedures. JBE’s should refer to the complete framework document for specific recommendations and best practices.

2.0 BACKGROUND

The Information Technology Advisory Committee-sponsored Disaster Recovery Workstream was charged with accomplishing the following:

- Develop model disaster recovery guidelines, standard recovery times, and priorities for each of the major technology components of the branch.
- Develop a disaster recovery framework document that could be adapted for any trial or appellate court to serve as a court’s disaster recovery plan.
- Create a plan for providing technology components that could be leveraged by all courts for disaster recovery purposes.

The formation of the workstream was based on a disaster recovery tactical initiative as identified in the Judicial Branch Technology Tactical Plan (2014-2018) aligning to the branch strategic goals, shown below in Figure #1.

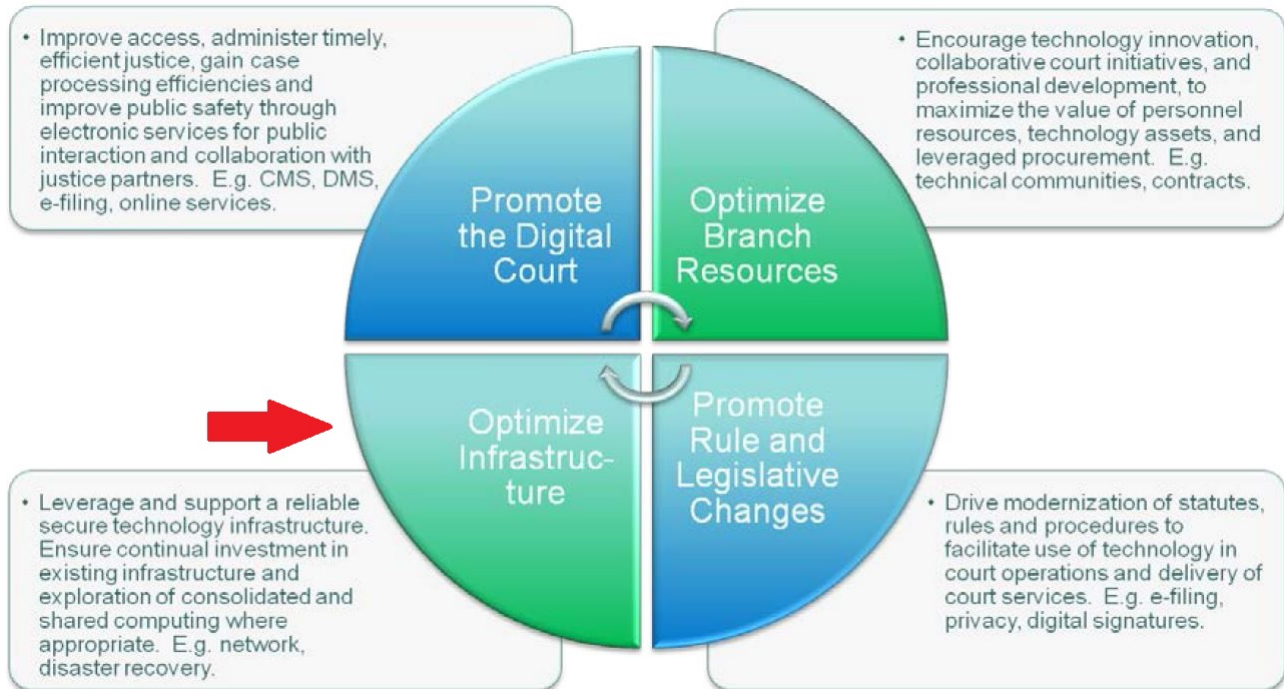


Figure 1: Judicial Branch Strategic Plan (2014-2018) Relevance

3.0 DISASTER RECOVERY FRAMEWORK

3.1 SCOPE

The disaster recovery framework has been developed for the establishment of a comprehensive and standard disaster recovery approach within the Judicial Branch of California. In order to produce the framework, input was solicited from multiple JBE’s ranging from small to large in size so that a comprehensive framework could be developed that is suitable to all entities within the judicial branch. The framework is designed to set a direction, identify and address areas of concern expressed by entities within the judicial branch, and document policies and practices that can assist JBE’s with their concerns by providing a framework for creating entity-specific disaster recovery plans and procedures, while following baseline recommendations and standards outlined accordingly.

The goals of the framework are:

- To suggest an overall direction and format for establishing and maintaining a disaster recovery plan. The plan helps JBE’s ensure that their plan is comprehensive, consistent with other JBE’s, and provides a baseline from which to work.
- To provide a holistic disaster recovery framework that the JBE’s can leverage to help streamline and expedite the completion of disaster recovery planning unique to each JBE.

- To provide general baseline recommendations on data recovery times, standards and approaches to disaster recovery.
- To provide suggestions for technology solutions (hardware/software) both in-place and not-in-place within the Judicial Branch that meet the requirements for implementing a disaster recovery plan.
- To satisfy courts' needs to establish disaster recovery plans around modern hosting services such as cloud, including software as a service, infrastructure as a service, etc. Modern hosting solutions are drastically changing the way courts manage and protect electronic data, therefore necessitating agile and proven methods on how to ensure data is backed up and to support the high availability of systems.

3.2 ORGANIZATIONAL CHARACTERISTICS

The framework establishes how disaster recovery plans should be created and maintained within individual judicial branch entities. It is imperative that a JBE's disaster recovery plan(s) and objective(s) align to—at a minimum, and satisfy the rules of court as related to data retention and privacy. Because JBE's have differing and unique relationships with how data is shared and/or divided with other justice partners, careful consideration should be exercised to ensure that both sides are taking data protection into account, ensuring that disaster recovery policies impacting each other are clearly outlined and communicated and regularly validating that all business-critical data is protected from a data backup perspective. Therefore, disaster recovery policies and procedures (administrative and technical) related to each JBE and respective justice partners are of particular importance.

3.3 DOCUMENTATION STRUCTURE

A disaster recovery plan is supported by a collection of documentation capturing differing levels of detail while maintaining consistent guidance for all participants. A JBE's disaster recovery plan documentation portfolio should consist of the following categories of documents:

- **Organizational Policy** – Expresses management's expectations with regard to tolerance to data loss for various classes of data and expectations for recovery times and retention. Generally limited to identification of base principles, including roles and responsibilities, and the disaster recovery framework. This framework provides the organizational policy for individual judicial branch entities.
- **Implementing Policy** – Further refines management's expectations; usually issued by a subordinate business or organizational unit for the purpose of interpreting the organizational policy to local entity practices. These policies will be developed as needed by the local entity.

- **Standards** – Identify specific hardware and software features and products whose use has been determined to be in support of policy and aligned to fulfilling the entities disaster recovery mission. Standards may be established by local entities as needed to support policy objectives and to streamline operations.
- **Procedures** – Support standards and policy by providing step-by-step instructions for the execution of a disaster recovery process. Judicial branch entities will develop and document procedures to ensure the quality and repeatability of disaster recovery processes.
- **Guidelines** – Provide recommendations which can be used when other guidance has not been established. Guidelines are usually created at lower operational levels such as departments to address immediate needs until consensus is reached on broader direction.

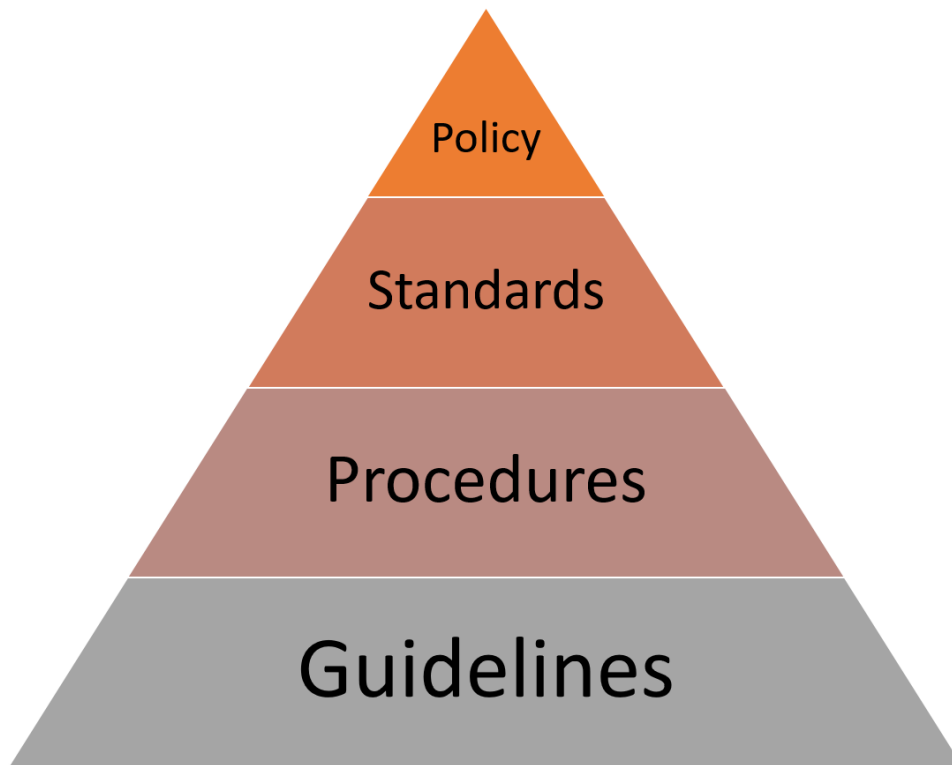


Figure 2: Documentation Structure

The following documents, published 08/1/2017 shall serve as the official Disaster Recovery Documents Package for the California Judicial Branch. This package represents “best practices” and is recommended as a disaster recovery framework to be used by all judicial branch entities.

1. Document (Reference): How to Use Guide (this document)

2. Document (Reference): Recommendations & Reference Guide
3. Document (For Completion by JBE): Adaptable Disaster Recovery Template

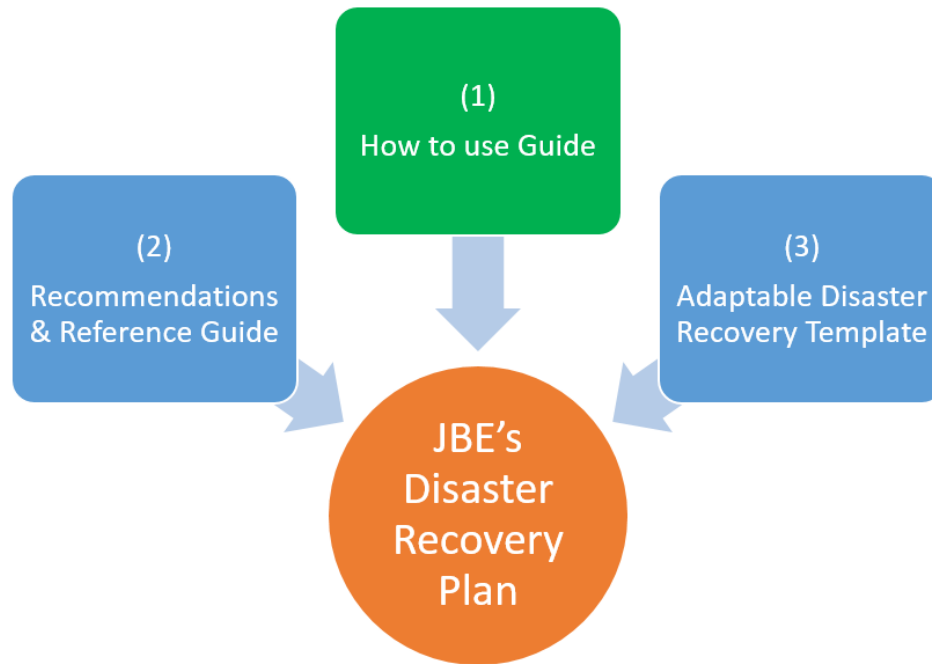


Figure 3: Document Path to Disaster Recovery Plan

4.0 PURPOSE OF DISASTER RECOVERY

Information and the supporting processes, systems, and pockets of data are important assets. Defining, achieving, maintaining, and improving disaster recovery systems, approaches and readiness may be essential to maintain legal compliance, integrity, and availability of information and systems.

JBEs and their information systems and data are faced with security threats and chances of corruption and/or loss from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage (such as malicious code, computer hacking, and denial of service attacks) have become more ubiquitous, more ambitious, and increasingly sophisticated. Ultimately, the consequences are felt the heaviest when data and systems are unreachable and/or data has been lost and/or compromised.

Many information systems have not been designed with disaster recovery in mind. While some systems do have means and methods to ensure that data is protected, the entities responsible for those systems must ensure that those means and methods are implemented and routinely tested.

Methods on protecting data that can be achieved through technical means are plentiful, and should be supported by appropriate management policies and procedures, including adequate funding and/or resource allocation. Identifying which controls should be in place requires careful planning and attention to detail. Disaster Recovery management requires, at a minimum, participation by all employees in the branch. It may also require participation from local and state justice partners, the public suppliers, third parties, contract labor, or other external parties. Disaster Recovery is a continually evolving area and courts are encouraged to stay informed and educated on current methods, products and technologies and ensure procedures are updated along the way. Although there is no requirement, it is also a best practice to establish an escalation path to ensure that incidents receive the proper attention based on severity and are processed in a timely manner.

Data is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. JBE’s, as part of their on-going program to maintain adequate and effective controls, want to ensure that the various systems and pockets of data scattered throughout the organization are accounted for and protected adequately. The benefits of keeping data as centralized as possible within various identified areas/systems/datacenters significantly outweighs scattering data across the organization especially beneath the core datacenter layer. A JBE’s disaster recovery posture and approach should emanate from the IT Department and administrative body, but never delegated to end-users. Additionally, ongoing education to end-users is essential to ensure that unseen data mines are not being created and stored in areas where IT does not have routine visibility and therefore may not get included in the respective disaster recovery plan.

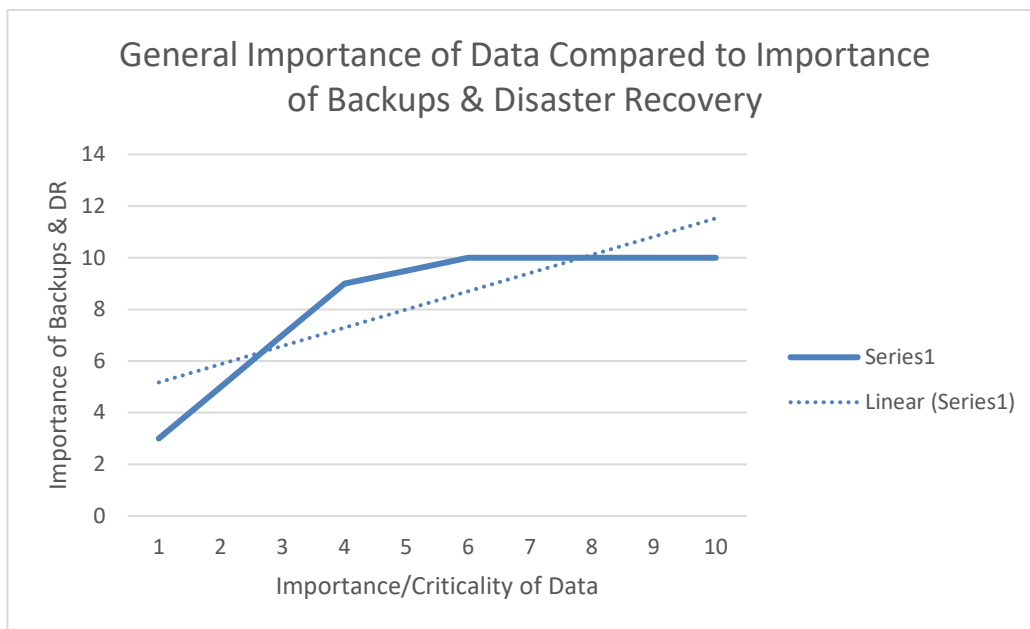


Figure 4: Importance of Data Compared to Importance of Backups & Disaster Recovery

5.0 USING THE FRAMEWORK

The Disaster Recovery Framework published by the Judicial Council provides a model that JBE's can leverage. JBE's are not required to implement the recommendations contained in the framework but they are encouraged to leverage the framework as appropriate for their unique local business requirements. The framework provides context for a court's local IT disaster recovery plan. The framework is designed to be modular and expandable so that courts can refer only to the sections that are relevant to them and expand accordingly based on varying needs. The framework references and recommends specific technologies known to be in use already within the Judicial Branch that can be implemented and shortening a JBE's effort in researching solutions.

A local court can utilize the framework and this "how to use" guide in the following manner:

1. The JBE has prioritized an initiative to improve the JBE's disaster recovery strategy and solution. Initiating such an effort will require staff time, resources and executing the initiative after solution(s) have been decided upon will ultimately require a financial commitment from the JBE for hardware/software and potential professional services.
2. Review this "how to use" guide and determine which stakeholders will be included in the development of the JBE's IT disaster recovery plan in order to create a project execution team.
3. The team then reads the "Recommendations & Reference Guide" to obtain a clear understanding of recommended standards, backup strategies, approaches to disaster recovery and various solutions being promoted that are in use today by various JBE's.
4. The JBE identifies options for implementing the plan.
5. The JBE determines what funding and resources exist to implement the local policy.
6. The JBE implements any hardware/software solution(s) needed to fulfill the disaster recovery plan and objective(s).
7. The JBE then completes the "Adaptable Disaster Recovery Template" to produce it's local Disaster Recovery Plan.



JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue
San Francisco, CA 94102-3688
Tel 415-865-4200
TDD 415-865-4272
Fax 415-865-4205
www.courts.ca.gov

HON. TANI G. CANTIL-SAKAUYE
Chief Justice of California
Chair of the Judicial Council

MR. MARTIN HOSHINO
Administrative Director,
Judicial Council

INFORMATION TECHNOLOGY ADVISORY COMMITTEE

HON. SHEILA F. HANSON
Chair

HON. LOUIS R. MAURO
Vice-chair

Hon. Marc Berman
Mr. Brian Cotta
Hon. Julie R. Culver
Hon. Tara M. Desautels
Ms. Alexandra Grimwade
Hon. Michael S. Groch
Mr. Paras Gupta
Hon. Samantha P. Jessner
Hon. Jackson Lucky
Hon. Kimberly Menninger
Hon. James M. Mize
Mr. Terry McNally
Mr. Snorri Ogata
Mr. Darrel E. Parker
Hon. Alan G. Perkins
Ms. Heather Pettit
Hon. Peter J. Siggins
Hon. Bruce Smith
Ma. Jeannette Vannoy
Mr. Don Willenburg
Mr. David H. Yamasaki

COMMITTEE STAFF
Mr. Robert Oyung
Tel 415-865-4994
Ms. Jamel Jones
Tel 415-865-4629

Date
December 5, 2017

To
**Members of the Judicial
Council Technology
Committee**

From
**Information Technology
Advisory Committee (ITAC)**

Hon. Sheila Hanson, Chair

**ITAC Next-Generation Hosting
Strategy Workstream**

**Hon. Jackson Lucky, Executive
Cosponsor**

**Mr. Brian Cotta, Executive
Cosponsor**

Subject
***Next-Generation Hosting
Framework Guide***

Action Requested
**Please Review and
Recommend**

Deadline
January 8, 2018

Contact
Brian Cotta
Brian.cotta@jud.ca.gov

**Heather L. Pettit, Project
Manager**
**Next-Generation Hosting
Strategy Workstream**
Heather.pettit@contracosta.courts.ca.gov

**Jamel Jones, Supervisor
Information Technology**
Jamel.jones@jud.ca.gov

Summary

The Information Technology Advisory Committee (ITAC) Next-Generation Hosting Strategy Workstream is seeking approval and recommendation of its proposed *Next-Generation Hosting Framework Guide* and associated documents.

Background

In 2014, the Judicial Council adopted the judicial branch *Strategic Plan for Technology*, which defines four technology goals:

- Goal 1: Promote the Digital Court
- Goal 2: Optimize Branch Resources
- Goal 3: Optimize Infrastructure
- Goal 4: Promote Rule and Legislative Changes

In accordance with this plan, the council also adopted the judicial branch *Tactical Plan for Technology: 2017-2018*, which outlines an initiative to transition to a next-generation hosting model. Although this initiative is expressed under strategic plan Goal 3, such a hosting solution would have a direct impact on the branch's ability to accomplish *three* of its strategic goals: Promote the Digital Court, Optimize Branch Resources, and Optimize Infrastructure.

To accomplish this tactical initiative, in January 2016 ITAC formed a workstream comprising judicial officers, court executive officers, and technologists from trial courts, appellate courts, and the Judicial Council staff. The task of the workstream was to assess best practices for hosting technology systems, produce a road map tool for use by courts in evaluating options, identify requirements for centralized hosting, and recommend a branch-level hosting strategy.

Before formation of the workstream, ITAC distributed a two-part survey to the Court Information Technology Management Forum, which gathered information on:

- Current court practices regarding their hosting solutions;
- The considerations and requirements of courts in selecting new hosting solutions; and
- Envisioned court strategy for next-generation hosting, including specific products, services, and providers, along with general approaches, alternatives, and benefits.

The survey findings provided the workstream with a baseline for understanding court resources, unmet needs, and objectives (both individually and collectively) and assisted with determining best solutions and recommendations.

With this information, the workstream met multiple times in 2016 and 2017. Several vendors provided branch educational presentations on possible solutions, opportunities, and pitfalls. Following those presentations, additional workstream meetings were held during which requirements, priorities, and recommendations were discussed. An initial draft of the *Next-Generation Hosting Framework Guide* and associated recommendations and templates were distributed to the workstream in April 2017, finalized in September 2017, and circulated for branch comment in October and November 2017.

The enclosed *Next-Generation Hosting Framework Guide* presents the workstreams hosting strategy recommendations based on the branch strategic and tactical plans and the best likelihood for achieving the defined goals and objectives. The recommendations are not mandatory, but

December 5, 2017

Page 3

rather a common framework that can be leveraged to help individual courts identify hosting solutions that are appropriate for their local environment. The workstream recognizes that many of the recommendations may not be feasible given today's budget and resource constraints. The intention is for the framework to provide court leadership with the foundation and guidance to inform their technology planning and decision-making as they move toward achieving their strategic goals and objectives.

Branch Comment and Approvals

The framework documents were circulated to the branch (including to the Supreme Court, appellate courts, and superior courts) for comment. While few suggestions were received, the response was generally supportive with constructive comments focused on providing clarifications. As a result of this comment period, non-substantive revisions were incorporated for clarity and general copy-editing. A comment matrix reflecting the input received is enclosed.

ITAC approved the final deliverables, as revised per branch comment, at its December 4, 2017 meeting.

Requested Action

The workstream seeks approval and recommendation of the enclosed *Next-Generation Hosting Framework Guide*, recommendations, and associated templates at the **Monday, January 8, 2018** Judicial Council Technology Committee (JCTC) business meeting.

Next Steps

Pending approval by the JCTC, the workstream will seek acceptance by the Judicial Council. Final documents will be published and available on the Judicial Resources Network for use by courts.

Thank you, in advance, for your time and attention.

Enclosures

- *Next-Generation Hosting Framework Guide*
- Attachment A- Recommended Service Levels, Inventory Assets, Solutions
- Attachment B- Inventory Checklist Template
- Attachment C- Technology Roadmap Template/Sample
- Comment Matrix from Branch Circulation

CALIFORNIA JUDICIAL BRANCH

Next-Generation Hosting Framework

A Guide for the California Judicial Branch

DRAFT

VERSION 1.0

NOVEMBER 28, 2017

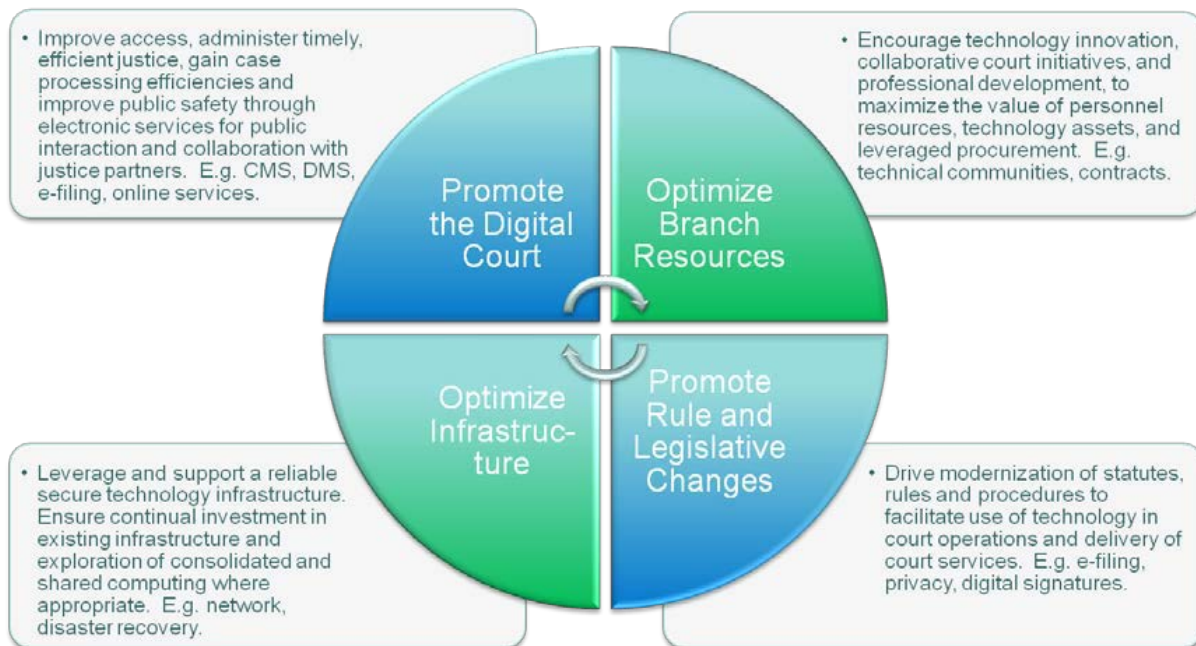
Table of Contents

1.0	INTRODUCTION	2
2.0	DEFINITIONS.....	4
3.0	NEXT-GENERATION HOSTING FRAMEWORK	5
3.1	Scope of Next-Generation Hosting Strategy.....	5
3.2	Organizational Characteristics	6
3.3	Organizational Assumptions	11
3.4	Documentation Structure	12
4.0	PURPOSE OF NEXT-GENERATION HOSTING	13
5.0	NEXT-GENERATION HOSTING OPTIONS AND BRANCH ASSETS	14
5.1	Data Center Options.....	14
5.2	Service-Level Definitions and Time Frames	17
5.3	Branchwide Assets and Service Levels.....	18
5.4	Branchwide Next-Generation Recommended Solutions	20
6.0	BRANCHWIDE RECOMMENDATIONS.....	23
7.0	USING THE NEXT-GENERATION HOSTING FRAMEWORK	24
7.1	Recommended Service Levels, Inventory Assets, and Solutions	24
7.2	Inventory Checklist Template	24
7.3	Technology Roadmap Template	24

1.0 INTRODUCTION

In October 2014, the California judicial branch adopted the *Strategic Plan for Technology 2014–2018* and the *Tactical Plan for Technology 2014–2016*. There are four technical goals defined within the strategic plan:

- Goal 1 Promote the Digital Court
- Goal 2 Optimize Branch Resources
- Goal 3 Optimize Infrastructure
- Goal 4 Promote Rule and Legislative Changes



In accordance with Goals 1, 2 and 3, the judicial branch tactical plan outlined the Next-Generation Hosting Initiative. While this initiative is expressly called out under Goal 3, the reality is this type of hosting solution has a direct impact on the branch's ability to accomplish three of its strategic goals: Promote the Digital Court, Optimize Branch Resources, and Optimize Infrastructure.

In order to truly achieve Goals 1 and 2, the hosting solution must take into account the requirements for those goals. For example, one set of objectives to Promote the Digital Court is

- Extended access and services to the public, including electronic filing and enhanced access for those with limited English proficiency;
- Enhanced judicial and administrative decision-making;
- Data and information sharing across the courts;
- Enhanced collaboration and cooperation between and among courts; and
- Enhanced collaboration and cooperation with local and statewide justice partners to promote public safety.

How each of these objectives is met is a direct result of the data center and the function within.

This framework provides recommendations based on the judicial branch's strategic and tactical plans and the best likelihood for achieving the defined goals and objectives. These are not mandatory requirements but rather a common framework that can be leveraged to help individual courts identify hosting solutions that are appropriate for their local environment. The Next-Generation Hosting Workstream recognizes many of the recommendations are not feasible in today's climate, due to budget and resource constraints. The intention is for the framework to provide court leadership with the foundation and guidance to move toward these strategic goals and objectives.

2.0 DEFINITIONS

Cloud computing—A type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources (e.g., computer networks, servers, storage, applications, and services), which can be rapidly provisioned and released with minimal managerial effort. These resources typically reside on the Internet instead of in a local data center.

Data center—A facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and various security devices.

Data loss—Any process or event that results in data being corrupted, deleted and/or made unreadable by a user and/or software or application.

Hosted solutions—For the purposes of this guide, refers to the physical servers supporting and storing court data whether provided internally, by the branch data center, or by a vendor either locally, offsite, or via cloud hosting.

Infrastructure as a service (IaaS)—The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.

Local hosting solution—A local court’s data center, managed, resourced, supported, and funded by that court.

Platform as a service (PaaS)—A category of cloud computing services that provides a platform allowing customers to develop, run, and manage web applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an application.

Service level—Measures the performance of a system. Certain goals are defined and the service level gives the percentage to which those goals should be achieved.

Software as a service (SaaS)—A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on the Internet. It is sometimes referred to as “on-demand software.” SaaS is typically accessed by users using a thin client via a web browser.

System outage; downtime—“Downtime” refers to periods when a system is unavailable. Downtime or outage duration refers to a period of time that a system fails to provide or perform its primary function. Reliability, availability, recovery, and unavailability are related concepts.

Vendor-hosted solution—Cloud computing vendors that have the capability of delivering SaaS, IaaS, and PaaS technical solutions.

3.0 NEXT-GENERATION HOSTING FRAMEWORK

3.1 SCOPE OF NEXT-GENERATION HOSTING STRATEGY

The current hosting model for information technology applications and services for the California Courts Technology Center (CCTC) was developed largely based on the strategy of centrally hosting the court case management systems and other shared applications. The branchwide strategy of hosting those systems has changed; therefore, the branch must reevaluate its hosting model to ensure resources and opportunities are utilized effectively in alignment with the new strategic direction while addressing the needs of the courts.

As hosting models and technology evolve, the most cost-effective, branchwide strategy for application and services hosting can be enabled through a combination of selective consolidation, virtualization, and implementation of secure private and public cloud environments. The goal of this tactical initiative will be to determine an updated model for branchwide hosting that includes all judicial branch entities.

Major Tasks

- Complete a needs assessment, define branch-recommended service levels, develop implementation recommendations, and determine necessary funding changes.
- Develop a toolset for courts to utilize when determining needs and funding requirements.
- Publish findings, including a hosting implementation toolset and branch-suggested service levels.
- Finalize product, service, and maintenance contract procurement with vendor partners.
- Assist judicial branch entities with decommissioning old services and implementing new services in alignment with the needs assessment and transition plan.

Dependencies

- The needs assessment should align with the strategy and roadmap for the Digital Court initiatives.

Types of Courts Involved

All courts—Supreme Court, Courts of Appeal, and superior courts. All courts as well as the Judicial Council will benefit from an updated branchwide hosting model that is tightly aligned with current and anticipated future business requirements.

Workstream Phases

Phase 1: Develop Educational Information and Hold Summit

- Determine the top solutions in the industry.
- Define the pros and cons of each solution.
- Provide examples of court applications that could utilize each solution.
- Provide sample cost information by solution.
- Include a roadmap tool to assist courts in evaluating local needs and identifying hosting solutions for themselves.
- Produce a next-generation hosting information tool.
- Determine whether a summit on the topic is necessary and, if so, hold the summit.

Phase 2: Define Branch-Level Hosting Requirements

- Identify strategies that could be implemented or utilized across the branch.
- Survey courts (all levels) on the types of applications they envision being hosted at a more central level.
- Capture hosting requirements based on Judicial Council decisions on branchwide applications.
- Define service-level requirements for a branch-level host site.
- Produce the next-generation hosting final report and requirements.

3.2 ORGANIZATIONAL CHARACTERISTICS

As part of its 2015 annual agenda, the Projects Subcommittee of the Information Technology Advisory Committee (formerly the Court Technology Advisory Committee) surveyed courts on two related topics: disaster recovery preparedness and planning for future hosting of court data (next-generation hosting). All courts should be concerned about the impact of disasters of all kinds, whether resulting from extreme weather events, earthquakes, or by malicious entities. Budget and resource constraints impact the ability of individual courts, and the branch as a whole, to prepare for and recover from such disasters. A corollary to these concerns is the effect migration has to new hosting environments and will have on disaster recovery preparedness and planning.

A survey was disseminated on June 1, 2015, to the Court Information Technology Management Forum (CITMF). CITMF members are the IT leaders from each of the courts. Their responses were collected through June 19, 2015. Responses were obtained from 49 of the 53 members—a 92 percent response rate.

The survey sought to identify the existing resources, unmet needs, and near-future objectives of the courts, individually and collectively, and to determine how the branch might best facilitate solutions. The survey questionnaire was divided into two parts: the Disaster Recovery Framework Assessment and the Next-Generation Hosting Solutions Needs Assessment.

Next-Generation Hosting Solutions Needs Assessment

This assessment was designed to gather information on the following:

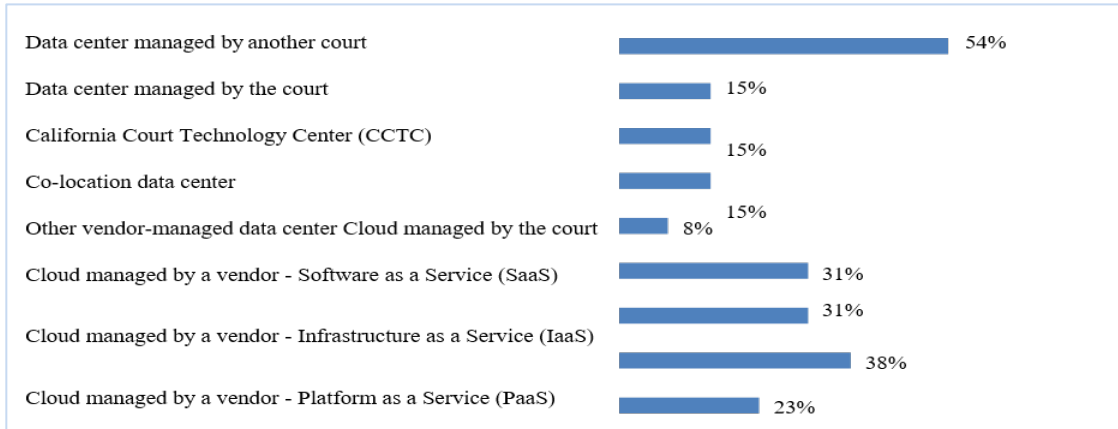
- Current practices regarding courts' hosting solutions;
- The considerations and requirements of courts in selecting new hosting solutions; and
- Envisioned court strategy for next-generation hosting, including specific products, services, and providers, along with general approaches, alternatives, and benefits.

Disaster Recovery Framework Assessment

The findings from this assessment, perhaps not surprisingly, disclose a broad range of approaches and readiness to address disaster responses, varying by court size and budget resources. The survey also shows that courts do not have only one way of hosting their systems, but use more than one hosting solution.

The following graphs outline the results of the next-generation hosting solutions section of the survey.

Figure 1. Current judicial branch hosting solutions



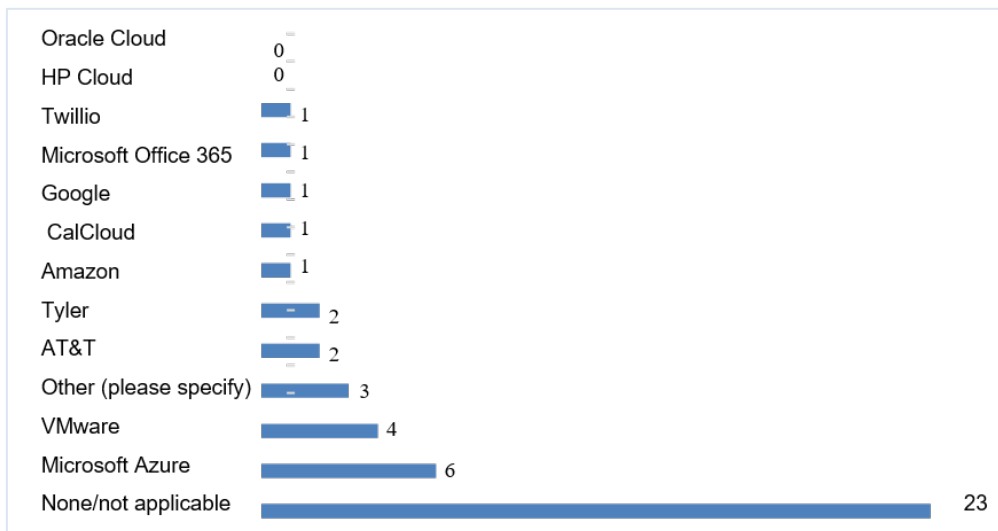
Comments

#	Other (please specify)
1	County managed data center but all court equipment is court owned and managed.
2	Moving to Office 365.
3	We do have servers onsite at this court location; however, SAIC manages those servers.
4	We do lease some VMware VM's from our county partners.

Current Cloud/Virtualization Vendor Solutions

Figure 2 lists the vendors used by those courts utilizing cloud hosting. For purposes of this survey, cloud hosting refers to services provided to customers via multiple connected servers on the Internet that comprise a cloud, as opposed to being provided by a locally hosted single server or virtual servers.

Figure 2. Cloud hosting vendors currently used by the courts (Responses: 38)

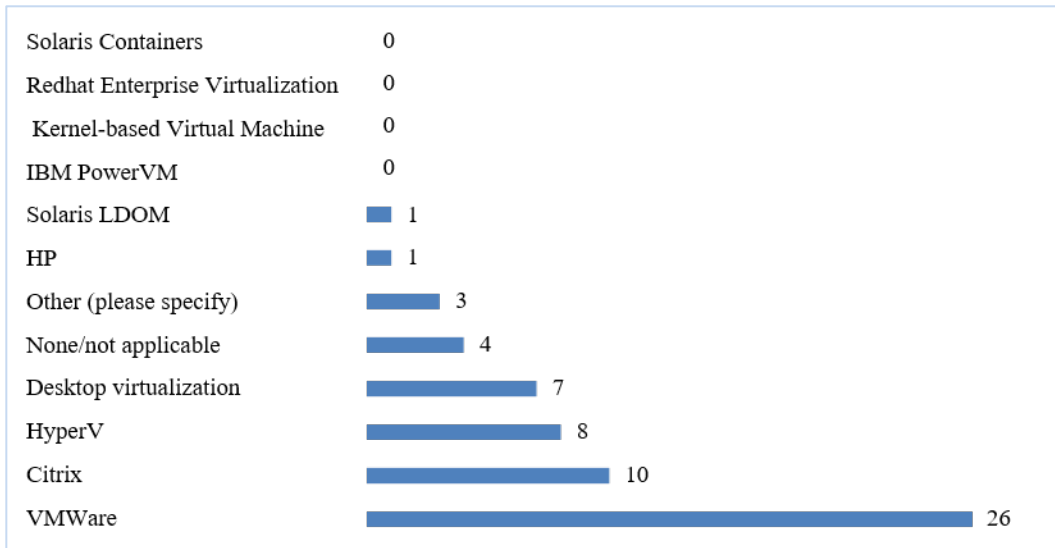


Other mentions included the following:

- “We use cloud hosting for inbound mail screening and forwarding.”
- “Barracuda Backup is based both on site and in the cloud.”
- “ADP–time and attendance, payroll, HR. Websites hosted at a web-hosting provider.”

Figure 3 lists the virtualization technologies currently deployed in the courts. Virtualization in this context refers to the act of creating a virtual (rather than physical) version of a resource, including but not limited to a virtual computer hardware platform, operating system (OS), storage device, or computer network.

Figure 3. Virtualization technologies currently deployed by the courts



Courts’ Short-Term and Long-Term Goals

Of the court representatives who answered, 34 percent are planning to move to a different hosting solution, with most indicating the move should occur in one to five years. Roughly half of those planning to move to a different hosting solution are considering moving to a data center managed by the court (with one-third considering a combination of court and outsourced staff), and almost all responses indicated they were considering cloud management. The primary reason for making the move was improved cost efficiencies (62 percent).

Figure 4. Types of hosting solutions being considered

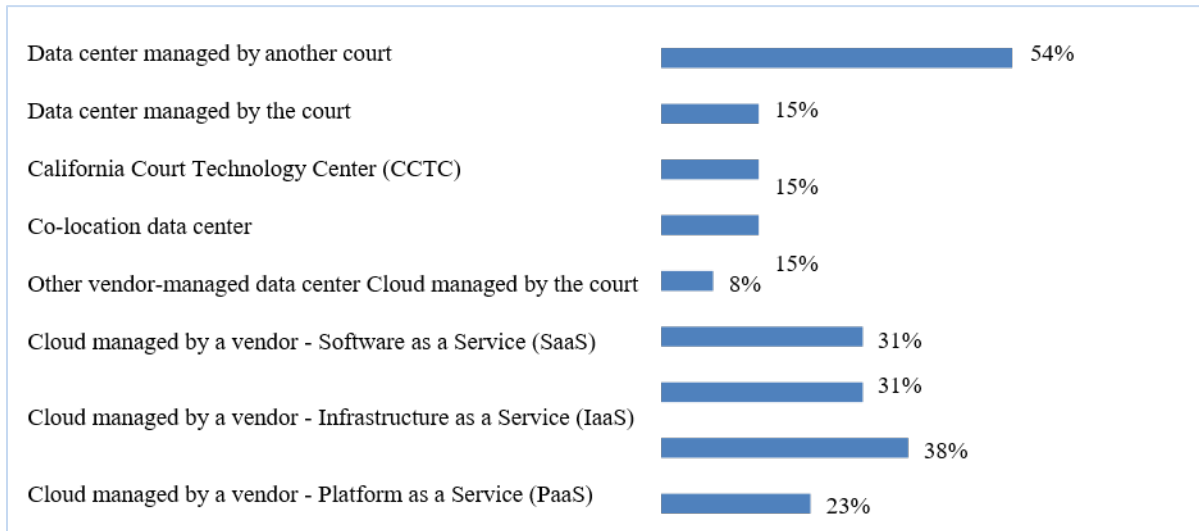


Figure 5. Time frame for courts to move to new hosting solution

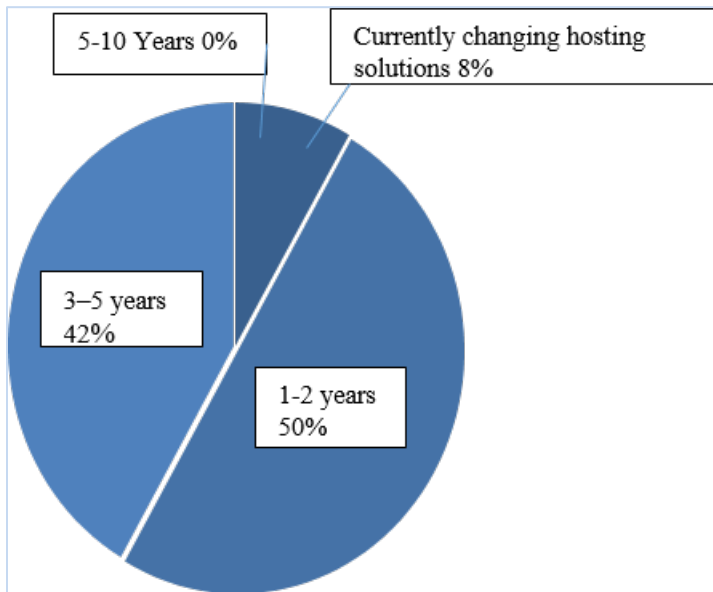
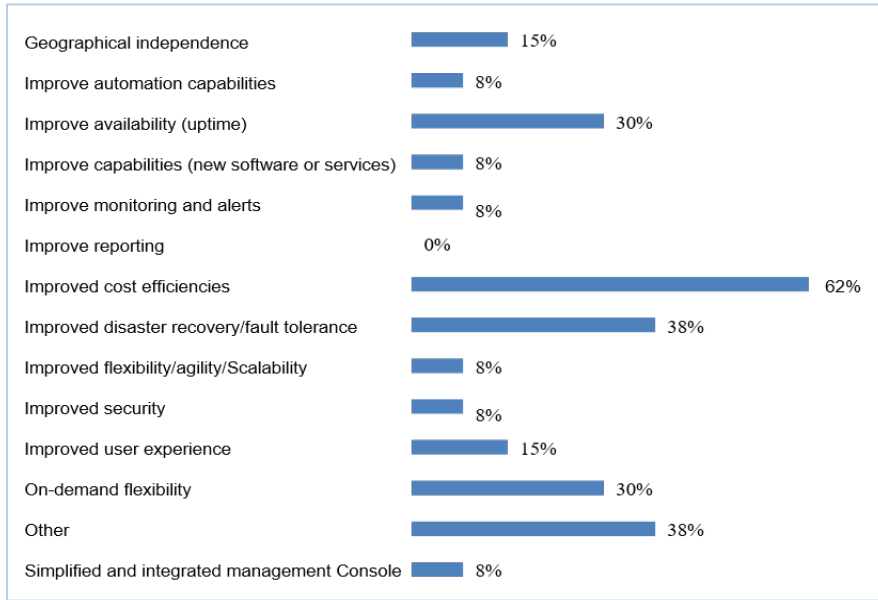
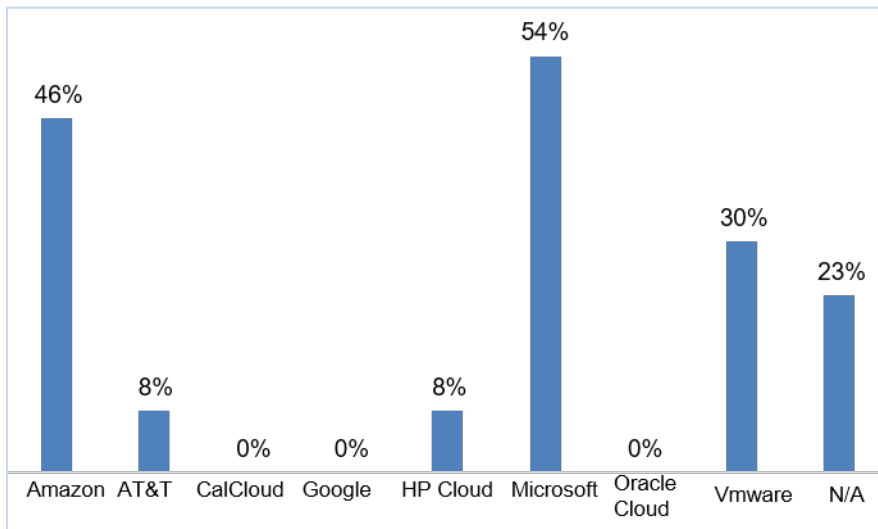


Figure 6. Reasons courts are seeking a new hosting solution

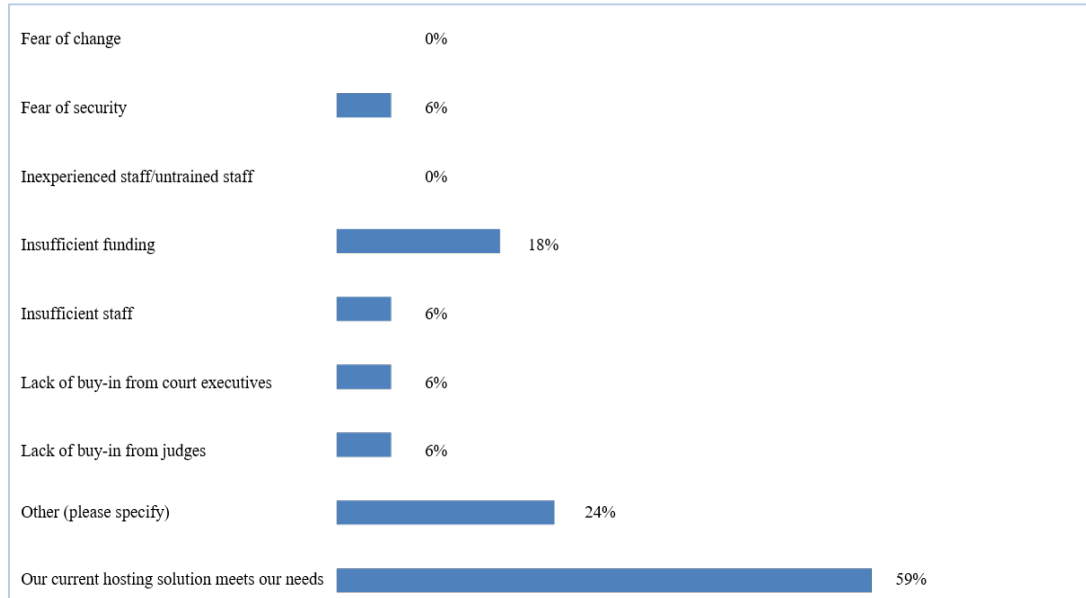


For those courts considering cloud hosting solutions, Figure 7 shows the vendors currently being considered.

Figure 7. Vendors under consideration



Lastly, it is important to analyze why some courts are not moving to new data center solutions. Figure 8 identifies some very clear reasons, such as no need, implementing a new case management system (CMS) (see “Other”), or no funding.

Figure 8. Reasons for courts not seeking a new hosting solution

Conclusion

Although the data was generated in 2015, it outlines several key elements that are still relevant:

- Of the 34 percent of the courts who are looking to move to a cloud hosting solution, 9 percent are looking to change within the next five years.
- 62 percent are looking to make a change for cost efficiencies.
- Many courts are already starting to work with vendors, such as Microsoft and Amazon, on cloud hosting solutions.
- 42 percent of courts are not seeking a new hosting solution due to insufficient funding, security fears, insufficient staff, or lack of buy-in from judges and court executives.

CITMF surveyed the courts again, in June 2016, on the use of Office 365, and 13 courts have now moved to that cloud-based solution—a significant change from 6 courts just one year prior.

3.3 ORGANIZATIONAL ASSUMPTIONS

The diversity of responses recorded in the data above demonstrate that courts have reached varying levels of technical maturity. As a result, the Next-Generation Hosting Workstream had to determine some basic assumptions to meet the goals and objectives set forth in the strategic and tactical plans. The workstream recognizes that while some of the assumptions may be broad in scope, they are necessary when determining a path to the future.

Assumptions:

- All courts are utilizing or moving to modern case management systems within the next five years.
- Current court facilities meet requirements for cloud hosting.
- Courts have adequate Internet bandwidth.
- Funding can be obtained.
- Resources will be determined based on the solution selected.

- Output from the Disaster Recovery Workstream will be utilized where appropriate.

3.4 DOCUMENTATION STRUCTURE

The Next-Generation Hosting Framework contains four key elements:

1. Recommended service-level definitions and time frames
2. A recommended court asset inventory sheet with court-defined service levels
3. A sample roadmap for long-term planning and a court roadmap template, including an estimate cost sheet for cloud-hosting solutions
4. A sample court asset inventory with service levels and a solution and budget estimate template

These documents are tools for courts use to define their data-hosting requirements and to create plans to move to a next-generation hosting data center.

4.0 PURPOSE OF NEXT-GENERATION HOSTING

As technology evolves, so do courts' needs and business practices. The courts' hosting model must partake in this evolution as well. Twenty-first century business and technology prioritizes accessibility and flexibility—a next-generation hosting solution is necessary for the courts to maintain these priorities for both its external and internal users. A new hosting solution can be accomplished through a combination of selective consolidation, virtualization, and implementation of secure private and public cloud hosting environments. The goal of this tactical initiative will be to determine an updated model for branchwide hosting, including all judicial branch entities.

The following tasks are recommended for the workstream:

- Outline industry best practices for hosting in an educational manner.
- Develop a matrix of solutions with pros, cons, and sample applications hosted, including costs.
- Produce a roadmap tool for use by courts in evaluating options.
- Consider an educational summit on hosting options and hold a summit, if appropriate.
- Identify the requirements for centralized hosting.
- Recommend a branch-level hosting strategy.

5.0 NEXT-GENERATION HOSTING OPTIONS AND BRANCH ASSETS

For each of the hosting solutions investigated by the technical team, the workstream created a list of pros and cons as well as a list of issues to be aware of in the selection of a hosting solution.

5.1 DATA CENTER OPTIONS

Based on a review of the hosting and disaster recovery assessments, as well as court ideas and strategies, the following solutions should be investigated:

- Private data center
 - A branch data center (centrally hosted)—CCTC model, Judicial Council managed, court managed
 - A court-hosted data center—court managed, limited size
 - Regional data centers
 - Regional applications
- Infrastructure as a service (cloud based)
- Software as a service (cloud based)
- Individual courts—hosting their own needs

Branch Data Center: All Solution Models

For any branch data center solution, courts would still have servers/infrastructure required at the courthouse. The following on-premises solutions include:

- Active Directory
- File/document store(s)
- Database(s)—potentially some or all
- Interactive voice response (IVR)
- VoIP
- Jury
- Networking

Branch Data Center: Vendor Hosted (Current CCTC Model)

PROS	CONS
Provides full service, including desktop solutions	Needs a cost allocation model, which would come from a negotiation between the vendor and a judicial branch entity. This cost allocation model would be included in the contract.
Removes operational pressure from court	Licenses are not included and must be budgeted above and beyond hosting vendor services. This is in contrast to cloud service providers, which often bundle licenses into the overall service cost.
Vendor manages system patches and antivirus	Less direct control for the court
Vendor manages Active Directory for centrally hosted applications (e.g., V3)	Generally more costly

For courts hosted at CCTC, vendor can also manage any server that must remain locally at the court.	Very little input in specific technology architecture being deployed at data center. This inflexibility is due in part to standardization of technology in order to maximize economies of scale. More choice can be achieved but at higher cost.
Unlike in a fully managed hosting environment, courts are able to negotiate work with the vendor for updates, hardware refresh, etc. (e.g. Madera, Lake, San Benito, and Modoc Counties) like a local data center would with court users.	Connectivity costs for reliable circuit connection to CCTC
Local hardware choices can remain with court, such as servers and desktops.	Active Directory users end up with separate AD accounts and passwords. Active Directory trusts between hosted and local forests may prove to be problematic and tough to manage at a larger scale.
No need for in-depth technical knowledge within the court.	

Branch Data Center: Judicial Council Hosted

When the workstream reviewed a Judicial Council–hosted data center, the concept generated many questions and concerns due to the level of complexity. Some of the key items that would need to be resolved include the following:

- A new governance structure would be required for security and network operations;
- Judicial Council staff would need to provide on-premises support services, contract with a vendor, or look to regional support;
- A new billing model would need to be created for courts; and
- An analysis would need to be conducted of the static costs of owning space versus another data center already in place.

PROS	CONS
Larger quantity and better pricing	Judicial Council staff would have to hire subject matter experts
Branch is in full control of its branch assets	Courts would be limited to common requirements
All branch solutions in one location	Limited flexibility for being agile; must plan forward
Better pricing on software/hardware licensing	Connectivity cost
Will have the economies of scale of other hosting solutions such as Microsoft or Amazon.	
	Forecasting becomes more important for determining future cost
	Need to build out facility to specific standards; required to meet building codes

Branch Data Center: Virtual or Cloud

Once the workstream vetted the more traditional data center models, the complexity of the issues became very apparent, so the group focused on the most likely scenario for success, which is a hybrid of both an on-premises data center and a virtual data center. Because of the various requirements and technical diversity across the branch, utilizing a hybrid approach is the most realistic, with the long-term goal of virtualizing as much of the data center as possible.

PROS	CONS
Good starting point for cloud hosting	Likely dependent on a single-vendor model
Provides agility and flexibility	Each court needs to have the expertise to work in a hybrid environment
Since two environments are available, disaster recovery can be more easily implemented	

Local Data Center

All courts today have their own local data center running most of their applications. If the court has the existing resources and expertise, the local data center may be a more cost-effective model than the cloud-hosting model.

PROS	CONS
Local control	May or may not be higher cost, depending on existing resources
Provides agility and flexibility	Requires onsite court resources
	Requires court data center
	Should adhere to building code requirements for data centers, which may be an additional expense for the courts

5.2 SERVICE-LEVEL DEFINITIONS AND TIME FRAMES

In evaluating the types of hosting solutions, it is critical to define the judicial branch's hours of operation and service requirements. After evaluation of all of the current court services, the workstream is proposing judicial branch recommendations for hours of business, service-level definitions, and service-level time frames.

Judicial branch–recommended hours of operation

Next-generation hosting services should be a 24/7 operation. While individual systems may incur planned outages for service and maintenance, the operational model for next-generation hosting should accommodate 24/7 service availability and incident-response resolution on any unscheduled outage. Advanced system monitoring and incident service-response capabilities are recommended to enable 24/7 operation.

Judicial branch–recommended service-level definitions

- *Critical*—Damage or disruption to a service that would stop court operations, public access, or timely delivery of justice, with no viable workaround.
- *High*—Damage or disruption to a service that would hinder court operations, public access, or timely delivery of justice. A workaround is available, but may not be viable.
- *Medium*—Damage or disruption to a specific service that would impact a group of users, but has a viable workaround.
- *Basic*—Damage or disruption to a specific service that would not impact court operations, public access, or timely delivery of justice and a viable workaround is available.

Judicial branch–recommended service-level agreement (SLA) time frames

SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours
Critical	Max Data Loss	1 hour	5 minutes
High	Max Time Recovery	6 hours	2 hours

High	Max Data Loss	1 hour	30 minutes
Moderate	Max Time Recovery	24 hours	24 hours
Moderate	Max Data Loss	1 business day	1 business day
Basic	Max Time Recovery	48 hours	48 hours
Basic	Max Data Loss	N/A	N/A

These recommendations provide noticeably different SLA time standards between the local and cloud environments, with the standards for cloud hosts being significantly more stringent. Industry cloud providers have been able to offer these higher best practice standards and expectations given their enhanced capabilities and resource availability.

5.3 BRANCHWIDE ASSETS AND SERVICE LEVELS

In collaboration with the Disaster Recovery Workstream and court experts, the following list provides an inventory of court technology assets and recommended service levels in a live/production environment.

Requirement	Recommended Service Level
Infrastructure	
Internet	Critical
Networking (switches/routers, firewalls), virtual, wireless, WAN, LAN, middleware)	Critical
Active Directory/DNS/DHCP	Critical
Servers (local, virtual, file, print)	Critical
Security device—ATT monitoring—internal/IDS	Critical
Virus protection	Critical
Storage	Critical
Middleware	High
Backup appliance	High
Desktops (local, virtual, thin client)	High
Load balancers	High
Proxies	High
UPS/generator/power	High
Data center cooling	High
Statewide security access parameters (all workstreams)	High
System monitoring/SolarWinds	High
Spam filter	Moderate
Public information kiosks/electronic signs	Moderate
Queueing system—Qmatic/Q-Flow	Moderate

Requirement	Recommended Service Level
Infrastructure	
Facilities automation	Moderate
Physical monitoring—temperature	Moderate
Helpdesk—IT systems	Moderate

Requirement	Recommended Service Level
Systems	
Case management	Critical
Jury management	Critical
Website—public service portal	Critical
E-filing	High
Communications/VoIP/analog/faxes	High
CCPOR/CLETS	High
DMV—justice partners, branch, and local (LAN/WAN—Connection)	High
IVR/call routing	High
Electronic/video recording and playback (FTR)	Moderate
Facilities requirements—assisted listening (ADA)	Moderate
Building access controls	Moderate
E-warrants_PC Dec/iPad/Magistrate phone	Moderate
Court Call/telephonic and video appearance	Moderate
Video remote interpreting (VRI)	Moderate
Physical security—video surveillance	Moderate
Video/meeting/conference systems	Basic

Requirement	Recommended Service Level
Applications	
E-mail/SMTP	High
Microsoft Office	High
Payroll systems—policy/union	Moderate
LexisNexis	Moderate
Westlaw	Moderate
Jury instructions	Moderate

Adobe (Acrobat)	Moderate
Xspouse	Moderate
Judicial workbench (CMS component)	Moderate
SAP/financial	Moderate
Mobile device management	Moderate
Real-time court reporting	Moderate
HR systems (non-SAP)	Moderate
Electronic evidence (policy)	Moderate
Computer-aided facilities management (CAFM)	Low
Web browser (Internet Explorer/Chrome)	Basic
Locally developed applications	Court discretion

5.4 BRANCHWIDE NEXT-GENERATION RECOMMENDED SOLUTIONS

After careful review of the various solutions available, the workstream determined the two best solutions for moving forward were either local installation or cloud services. As previously noted, courts are still required to provide many local IT solutions, such as kiosks, network equipment, and local storage. However, the majority of the court applications can run in a cloud environment. If a court has the necessary infrastructure (Internet) and the cost is equal to or less than that of a local installation, the court should move to cloud-based services.

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Infrastructure			
Internet			✓
Networking (switches/routers, firewalls), virtual, wireless, WAN, LAN, middleware)	✓		✓
Servers (local, virtual, file, print)	✓		✓
Security device—ATT monitoring—internal/IDS	✓		✓
Virus protection	✓		✓
Storage	✓		✓
Active Directory/DNS/DHCP	✓		✓
Middleware	✓		✓
Backup appliance	✓		✓
Desktops (local, virtual, thin client)	✓		✓
Load balancers	✓		✓
Proxies	✓		✓
UPS/generator/power	✓		
Data center cooling	✓		
Statewide security access parameters (all workstreams)	✓		✓
System monitoring/SolarWinds	✓		✓

Spam filter			✓
Public information kiosks/electronic signs	✓		
Queueing system—Qmatic/Q-Flow			✓
Facilities automation			✓
Physical monitoring—temperature			✓
Helpdesk—IT systems			✓

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Systems			
Case management	✓	✓	✓
Jury management	✓		✓
Website—public service portal			✓
E-filing			✓
Communications/VoIP/analog/faxes	✓		
CCPOR/CLETS			✓
DMV—justice partners, branch, and local (LAN/WAN—Connect)	✓		
IVR/call routing	✓		✓
Video/meeting/conference systems			✓
Electronic/video recording and playback (FTR)	✓		✓
Facilities requirements—assisted listening (ADA)	✓		
Building access controls	✓		
E-warrants_PC Dec/iPad/Magistrate phone			✓
Court Call/telephonic and video appearance			✓
Video remote interpreting (VRI)			✓
Physical security—video surveillance	✓		✓

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Applications			
E-mail/SMTP			✓
Microsoft Office	✓		✓
Payroll systems—policy/union			✓
LexisNexis			✓
Westlaw			✓
Jury instructions	✓		✓

Requirement	Applicable Solution		
	Local	Private Data Center	Cloud
Adobe (Acrobat)			✓
Xspouse			✓
Judicial workbench (CMS component)			✓
SAP/financial			✓
Mobile device management			✓
Real-time court reporting	✓		
HR systems (non-SAP)			✓
Electronic evidence (policy)	✓		✓
CAFM			✓
Web browser (Internet Explorer/Chrome)			✓
Locally developed applications**	✓		✓

6.0 BRANCHWIDE RECOMMENDATIONS

The Next-Generation Hosting Workstream provides its recommendations based on the business and operational needs of the courts and has created a framework within which they may make decisions on what will be best for their needs. The workstream recognizes industry standards and other initiatives that may already be in place to address key considerations such as security, performance, or disaster recovery in order to safely adopt cloud solutions.

After significant analysis, the workstream has determined the following recommendations for the Information Technology Advisory Committee and the Judicial Council Technology Committee:

- If the courts have the ability and the opportunity, and the cost is less than a local solution, they should move to a cloud solution;
- Adopt the recommended branch service levels and hours of operation for all data center solutions;
- Do not proceed with a VMware vendor for a branchwide agreement;
- When a technology change occurs that impacts the branch and provides an opportunity for improved support, a corresponding support model should be developed;
- Approve Phase 2 of the Next-Generation Hosting Framework, including pilot court and cloud service agreements;
- Microsoft is the office and e-mail standard across the branch, whether using Exchange or Office 365; and
- Host a webinar for courts to learn about the Next-Generation Hosting Framework.

7.0 USING THE NEXT-GENERATION HOSTING FRAMEWORK

7.1 RECOMMENDED SERVICE LEVELS, INVENTORY ASSETS, AND SOLUTIONS

See Attachment A

7.2 INVENTORY CHECKLIST TEMPLATE

See Attachment B.

7.3 TECHNOLOGY ROADMAP TEMPLATE

See Attachment C.

NEXT GENERATION HOSTING JUDICIAL BRANCH RECOMMENDATIONS

Hours of Operation

Data center operations and availability is 24 hours a day, 7 days a week.

Service level definitions

Critical: damage or disruption to a service that would stop court operations, public access or timely delivery of justice, with no viable work-around.

High: damage or disruption to a service that would hinder court operations, public access or timely delivery of justice. A work-around is available, but may not be viable.

Medium: damage or disruption to a specific service that would impact a group of users, but has a viable work-around.

Systems Support: damage or disruption to a specific service that would not impact court operations, public access or timely delivery of justice and a viable work-around is available.

Production service level agreement times

SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours
Critical	Max Data Loss	1 hour	5 minutes
High	Max Time Recovery	6 hours	2 hours
High	Max Data Loss	1 hour	30 minutes
Moderate	Max Time Recovery	24 hours	24 hours
Moderate	Max Data Loss	1 Business day	1 Business day
Basic	Max Time Recovery	48 hours	48 hours
Basic	Max Data Loss	N/A	N/A

Inventory Assets with Services Level and viable solution

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Infrastructure				
Internet	Critical			✓
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓		✓
Servers (local, virtual, File, Print)	Critical	✓		✓
Security Device- ATT Monitoring-Internal/IDS	Critical	✓		✓
Virus protection	Critical	✓		✓
Storage	Critical	✓		✓
Active Directory/DNS/DHCP	Critical	✓		✓
Middleware	High	✓		✓
Back-up Appliance	High	✓		✓
Desktops (Local, virtual, thin client)	High	✓		✓
Load Balancers	High	✓		✓
Proxy's	High	✓		✓
UPS/Generator/ Power	High	✓		
Data center Cooling	High	✓		
Statewide Security Access parameters (All workstreams)	High	✓		✓
System Monitoring/Solarwinds	High	✓		✓
Spam filter	Moderate			✓
Public Information Kiosks / Electronic signs	Moderate	✓		
Queueing system- Qmatic/Qflow	Moderate			✓
Facilities automation	Moderate			✓
Physical Monitoring-Temperature	Moderate			✓
Helpdesk- IT Systems	Moderate			✓

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Systems				
Case Management	Critical	✓	✓	✓
Jury Management	Critical	✓		✓
Website - Public Service Portal	Critical			✓
E-filing	High			✓
Communications/VoIP/Analog/Faxes	High	✓		
CCPOR/CLETS	High			✓
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High	✓		
IVR/Call Routing	High	✓		✓
Video/Meeting/Conference Systems	Basic			✓
Electronic/Video Recording and Playback (FTR)	Moderate	✓		✓
Facilities Requirements- Assisted Listening (ADA)	Moderate	✓		
Building Access Controls	Moderate	✓		
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate			✓
Court Call/Telephonic/Video appearance	Moderate			✓
VRI - Video Remote Interpreting	Moderate			✓
Physical Security- Video Surv.	Moderate	✓		✓

Requirement	Service Level	Applicable Solution		
		Local	Private Data Center	Cloud
Applications				
E-Mail/SMTP	High			✓
MS Office	High	✓		✓
Payroll Systems- Policy/Union	Moderate			✓
Lexis Nexis	Moderate			✓
West Law	Moderate			✓
Jury Instructions	Moderate	✓		✓
Adobe (Acrobat)	Moderate			✓
X-spouse	Moderate			✓
Judicial workbench (CMS Component)	Moderate			✓
SAP/Financial	Moderate			✓
Mobile device management	Moderate			✓
Real-time court reporting	Moderate	✓		
HR Systems (Non-SAP)	Moderate			✓
Electronic Evidence (Policy)	Moderate	✓		✓
CAFM	Basic			✓
Web browser (Internet Explorer/Chrome)	Basic			✓
Locally developed applications**	Court discretion	✓		✓

Roadmap Pricing Matrix (will be finalized with Phase 2):

Requirement	Service Level	Cloud Solution				
Infrastructure			X-Large /Branch	Large	Medium	Small
Internet	Critical	✓				\$\$
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓				
Servers (local, virtual, File, Print)	Critical	✓				\$
Security Device- ATT Monitoring-Internal/IDS	Critical	✓				\$\$
Virus protection	Critical	✓				
Storage	Critical	✓				
Active Directory/DNS/DHCP	Critical	✓	\$\$		\$\$	
Middleware	High	✓				
Back-up Appliance	High	✓	\$			
Desktops (Local, virtual, thin client)	High	✓				
Load Balancers	High	✓				
Proxy's	High	✓				
UPS/Generator/ Power	High					
Data center Cooling	High					
Statewide Security Access parameters (All workstreams)	High	✓				
System Monitoring/Solarwinds	High	✓	\$		\$\$	\$
Spam filter	Moderate	✓	\$			
Public Information Kiosks / Electronic signs	Moderate					
Queueing system- Qmatic/Qflow	Moderate	✓				
Facilities automation	Moderate	✓				
Physical Monitoring-Temperature	Moderate	✓				
Helpdesk- IT Systems	Moderate	✓				

Extra Large /Branch	\$\$\$	\$1,000,000-\$5,000,000
	\$\$	\$200,000-\$999,999
	\$	\$15,000-\$199,999
Large Court:	\$\$\$	\$250,000-\$500,000
	\$\$	\$xxxxxx.xx-\$xxxxx
	\$	\$xxxxxx.xx-\$xxxxx

Medium Court:	\$\$\$	\$150,000-\$250,000
	\$\$	\$50,000-\$150,000
	\$	\$5,000-\$50,000
Small Court:	\$\$\$	\$30,000-\$60,000
	\$\$	\$10,000-\$30,000
	\$	\$1,000-\$10,000

Requirement	Service Level	Cloud				
		X-Large /Branch	Large	Medium	Small	
Systems						
Case Management	Critical	✓	\$\$\$	\$\$\$	\$\$\$	\$\$\$
Jury Management	Critical	✓	\$\$		\$\$	\$
Website - Public Service Portal	Critical	✓	\$\$		\$	
E-filing	High	✓	\$\$			
Communications/VoIP/Analog/Faxes	High					
CCPOR/CLETS	High	✓				
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High					
IVR/Call Routing	High	✓				
Video/Meeting/Conference Systems	Basic	✓				\$
Electronic/Video Recording and Playback (FTR)	Moderate	✓				
Facilities Requirements- Assisted Listening (ADA)	Moderate					
Building Access Controls	Moderate					
E-Warrants/ PC Dec/Ipad/Magistrate phone	Moderate	✓				
Court Call/Telephonic/Video appearance	Moderate	✓				
VRI - Video Remote Interpreting	Moderate	✓				\$
Physical Security- Video Surveillance	Moderate	✓				

Extra Large /Branch

\$\$\$ \$1,000,000-\$5,000,000
 \$\$ \$200,000-\$999,999
 \$ \$15,000-\$199,999

Large Court:

\$\$\$ \$250,000-\$500,000
 \$\$ \$xxxxxx.xx-\$xxxxx
 \$ \$xxxxxx.xx-\$xxxxx

Medium

Court: \$\$\$ \$150,000-\$250,000
 \$\$ \$50,000-\$150,000
 \$ \$5,000-\$50,000

Small

Court: \$\$\$ \$30,000-\$60,000
 \$\$ \$10,000-\$30,000
 \$ \$1,000-\$10,000

Requirement	Service Level	Cloud				
Applications			X-Large /Branch	Large	Medium	Small
E-Mail/SMTP	High	✓	\$\$ O365	\$\$\$ O365	\$ Email	\$\$ O365
MS Office	High	✓				
Payroll Systems- Policy/Union	Moderate	✓				\$
Lexis Nexis	Moderate	✓				\$
West Law	Moderate	✓				\$
Jury Instructions	Moderate	✓				
Adobe (Acrobat)	Moderate	✓				
X-spouse	Moderate	✓				
Judicial workbench (CMS Component)	Moderate	✓				
SAP/Financial	Moderate	✓				
Mobile device management	Moderate	✓				
Real-time court reporting	Moderate					
HR Systems (Non-SAP)	Moderate	✓				
Electronic Evidence (Policy)	Moderate	✓				
CAFM	Basic	✓				
Web browser (Internet Explorer/Chrome)	Basic	✓				
Locally developed applications**	Court discretion	✓				

Extra Large /Branch	\$\$\$	\$1,000,000-\$5,000,000	Medium Court:	\$\$\$	\$150,000-\$250,000
	\$\$	\$200,000-\$999,999		\$\$	\$50,000-\$150,000
	\$	\$15,000-\$199,999		\$	\$5,000-\$50,000
Large Court:	\$\$\$	\$250,000-\$500,000	Small Court:	\$\$\$	\$30,000-\$60,000
	\$\$	\$xxxxxx.xx-\$xxxxx		\$\$	\$10,000-\$30,000
	\$	\$xxxxxx.xx-\$xxxxx		\$	\$1,000-\$10,000

Court Data Center Inventory list and Service Levels

Recommend Service Level				Court Defined Service Level			
SLA Type	SLA Criteria	Local Data Center	Cloud	SLA Type	SLA Criteria	Local Data Center	Cloud
Critical	Max Time Recovery	4 hours	1 hours	Critical	Max Time Recovery		
Critical	Max Data Loss	1 hour	5 minutes	Critical	Max Data Loss		
High	Max Time Recovery	6 hours	2 hours	High	Max Time Recovery		
High	Max Data Loss	1 hour	30 minutes	High	Max Data Loss		
Moderate	Max Time Recovery	24 hours	24 hours	Moderate	Max Time Recovery		
Moderate	Max Data Loss	1 Business day	1 Business day	Moderate	Max Data Loss		
Basic	Max Time Recovery	48 hours	48 hours	Basic	Max Time Recovery		
Basic	Max Data Loss	N/A	N/A	N/A	N/A		

Requirement	Recommend Service Level	Court Service Level	Applicable Solution		Estimated Amount \$\$ from Road Map			
			Local	Cloud	Year 1	Year 2	Year 3	Year 4
Infrastructure								
Internet	Critical							
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical							
Servers (local, virtual, File, Print)	Critical							
Security Device- ATT Monitoring-Internal/IDS	Critical							
Virus protection	Critical							
Storage	Critical							
Active Directory/DNS/DHCP	Critical							
Middleware	High							
Back-up Appliance	High							
Desktops (Local, virtual, thin client)	High							
Load Balancers	High							
Proxy's	High							
UPS/Generator/ Power	High							
Data center Cooling	High							
Statewide Security Access parameters (All workstreams)	High							
System Monitoring/Solarwinds	High							
Spam filter	Moderate							
Public Information Kiosks / Electronic signs	Moderate							
Queueing system- Qmatic/Qflow	Moderate							
Facilities automation	Moderate							
Physical Monitoring-Temperature	Moderate							
Helpdesk- IT Systems	Moderate							
					\$0.00	\$0.00	\$0.00	\$0.00
ESTIMATED STRATEGIC BUDGET								\$0.00

Requirement	Recommend Service Level	Court Service Level	Applicable Solution		Estimated Amount \$\$ from Road Map			
			Local	Cloud	Year 1	Year 2	Year 3	Year 4
Systems								
Case Management	Critical							
Jury Management	Critical							
Website - Public Service Portal	Critical							
E-filing	High							
Communications/VoIP/Analog/Faxes	High							
CCPOR/CLETS	High							
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High							
IVR/Call Routing	High							
Video/Meeting/Conference Systems	Basic							
Electronic/Video Recording and Playback (FTR)	Moderate							
Facilities Requirements- Assisted Listening (ADA)	Moderate							
Building Access Controls	Moderate							
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate							
Court Call/Telephonic/Video appearance	Moderate							
VRi - Video Remote Interpreting	Moderate							
Physical Security- Video Surv.	Moderate							
					\$0.00	\$0.00	\$0.00	\$0.00
ESTIMATED STRATEGIC BUDGET								\$0.00

Requirement	Recommend Service Level	Court Service Level	Applicable Solution		Estimated Amount \$\$ from Road Map			
			Local	Cloud	Year 1	Year 2	Year 3	Year 4
Applications								
E-Mail/SMTP	High							
MS Office	High							
Payroll Systems- Policy/Union	Moderate							
Lexis Nexis	Moderate							
West Law	Moderate							
Jury Instructions	Moderate							
Adobe (Acrobat)	Moderate							
X-spouse	Moderate							
Judicial workbench (CMS Component)	Moderate							
SAP/Financial	Moderate							
Mobile device management	Moderate							
Real-time court reporting	Moderate							
HR Systems (Non-SAP)	Moderate							
Electronic Evidence (Policy)	Moderate							
CAFM	Basic							
Web browser (Internet Explorer/Chrome)	Basic							
Locally developed applications**	Court discretion							
					\$0.00	\$0.00	\$0.00	\$0.00
					ESTIMATED STRATEGIC BUDGET			\$0.00

SAMPLE ROADMAP

*Costs are samples from existing trial courts

Budget Year 1: \$200,000 Budget Year 2: \$300,000 Budget Year 3: \$250,000 Budget Year 4: \$250,000.00

Requirement	Service Level	Cloud Solution			
Infrastructure		X-Large/Branch	Large	Medium	Small
Internet	Critical	✓			\$\$
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical	✓			
Servers (local, virtual, File, Print)	Critical	✓			\$
Security Device- ATT Monitoring-Internal/IDS	Critical	✓			\$\$
Virus protection	Critical	✓			
Storage	Critical	✓			
Active Directory/DNS/DHCP	Critical	✓	\$\$	\$\$	
Middleware	High	✓			
Back-up Appliance	High	✓	\$		
Desktops (Local, virtual, thin client)	High	✓			
Load Balancers	High	✓			
Proxy's	High	✓			
UPS/Generator/ Power	High				
Data center Cooling	High				
Statewide Security Access parameters (All workstreams)	High	✓			
System Monitoring/Solarwinds	High	✓	\$	\$\$	\$
Spam filter	Moderate	✓	\$		
Public Information Kiosks / Electronic signs	Moderate				
Queueing system- Qmatic/Qflow	Moderate	✓			
Facilities automation	Moderate	✓			
Physical Monitoring-Temperature	Moderate	✓			
Helpdesk- IT Systems	Moderate	✓			
Extra Large/Branch	\$\$\$	\$1,000,000-\$5,000,000		Medium Court: \$\$\$	\$150,000-\$250,000
	\$\$	\$200,000-\$999,999		\$\$	\$50,000-\$150,000
	\$	\$15,000-\$199,999		\$	\$5,000-\$50,000
Large Court:	\$\$\$	\$250,000-\$500,000		Small Court: \$\$\$	\$30,000-\$60,000
	\$\$	\$xxxxxx.xx-\$xxxxxx		\$\$	\$10,000-\$30,000
	\$	\$xxxxxx.xx-\$xxxxxx		\$	\$1,000-\$10,000

Requirement	Service Level	Cloud				
Systems						
Case Management	Critical	✓	\$\$\$	\$\$\$	\$\$\$	\$\$\$
Jury Management	Critical	✓	\$\$		\$\$	\$
Website - Public Service Portal	Critical	✓	\$\$		\$	
E-filing	High	✓	\$\$			
Communications/VoIP/Analog/Faxes	High					
CCPOR/CLETS	High	✓				
DMV- Justice Partners Branch and local (Lan/Wan- Connect)	High					
IVR/Call Routing	High	✓				
Video/Meeting/Conference Systems	Basic	✓				\$
Electronic/Video Recording and Playback (FTR)	Moderate	✓				
Facilities Requirements- Assisted Listening (ADA)	Moderate					
Building Access Controls	Moderate					
E-Warrants_PC Dec/Ipad/Magistrate phone	Moderate	✓				
Court Call/Telephonic/Video appearance	Moderate	✓				
VRl - Video Remote Interpreting	Moderate	✓				\$
Physical Security- Video Surv.	Moderate	✓				
Extra Large/Branch	\$\$\$	\$1,000,000-\$5,000,000		Medium Court: \$\$\$	\$150,000-\$250,000	
	\$\$	\$200,000-\$999,999		\$\$	\$50,000-\$150,000	
	\$	\$15,000-\$199,999		\$	\$5,000-\$50,000	
Large Court:	\$\$\$	\$250,000-\$500,000		Small Court: \$\$\$	\$30,000-\$60,000	
	\$\$	\$xxxxxx.xx-\$xxxxxx		\$\$	\$10,000-\$30,000	
	\$	\$xxxxxx.xx-\$xxxxxx		\$	\$1,000-\$10,000	

Requirement	Service Level	Cloud				
Applications						
E-Mail/SMTTP	High	✓	\$\$ O365	\$\$\$ O365	\$(Email Only)	\$\$ O365
MS Office	High	✓				
Payroll Systems- Policy/Union	Moderate	✓				\$
Lexis Nexis	Moderate	✓				\$
West Law	Moderate	✓				\$
Jury Instructions	Moderate	✓				
Adobe (Acrobat)	Moderate	✓				
X-spouse	Moderate	✓				

Judicial workbench (CMS Component)	Moderate	✓				
SAP/Financial	Moderate	✓				
Mobile device management	Moderate	✓				
Real-time court reporting	Moderate					
HR Systems (Non-SAP)	Moderate	✓				
Electronic Evidence (Policy)	Moderate	✓				
CAFM	Basic	✓				
Web browser (Internet Explorer/Chrome)	Basic	✓				
Locally developed applications**	Court discretion	✓				
Extra Large/Branch	\$\$\$	\$1,000,000-\$5,000,000		Medium Court:	\$\$\$	\$150,000-\$250,000
	\$\$	\$200,000-\$999,999			\$\$	\$50,000-\$150,000
	\$	\$15,000-\$199,999			\$	\$5,000-\$50,000
Large Court:	\$\$\$	\$250,000-\$500,000		Small Court:	\$\$\$	\$30,000-\$60,000
	\$\$	\$xxxxxx.xx-\$xxxxx			\$\$	\$10,000-\$30,000
	\$	\$xxxxxx.xx-\$xxxxx			\$	\$1,000-\$10,000

Requirement	Recommended Service Level
Infrastructure	
Internet	Critical
Networking (switches/routers, Firewalls), Virtual, Wireless, WAN, LAN, Middleware)	Critical
Active Directory/DNS/DHCP	Critical
Servers (local, virtual, File, Print)	Critical
Security Device- ATT Monitoring-Internal/IDS	Critical
Virus protection	Critical
Storage	Critical
Middleware	High
Back-up Appliance	High
Desktops (Local, virtual, thin client)	High
Load Balancers	High
Proxy's	High
UPS/Generator/ Power	High
Data center Cooling	High
Statewide Security Access parameters (All workstreams)	High
System Monitoring/Solarwinds	High
Spam filter	Moderate
Public Information Kiosks / Electronic signs	Moderate
Queueing system- Qmatic/Qflow	Moderate
Facilities automation	Moderate
Physical Monitoring-Temperature	Moderate
Helpdesk- IT Systems	Moderate

ITAC Next-Generation Hosting Workstream

Branch Comment on Next-Generation Hosting Framework Guide

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	Committee Response
1	Kevin Lane / Alex Lesberg 4 th District Court of Appeal	NI	Overall comment about section 5.3. Since this is a framework/standards document, should we not remove mention of specific vendors?	The framework makes recommendations based upon the strategic and tactical plan and the likelihood for achieving the defined goals and objectives. These are not mandatory requirements but rather a common framework that can be leveraged to help individual courts identify some hosting solutions, or vendors that may be appropriate for their environments. Thus, the workstream did not incorporate revisions related to this comment.
2	Kevin Lane / Alex Lesberg 4 th District Court of Appeal	NI	<i>(Re: Sec. 5.4 Table headings)</i> This is the first time that this term "private data center" appears in this doc. Terminology should be consistent and should be defined. Should these headings match the defined data center types from section 5.1?	The workstream agreed with the commenter and has updated section 5.1 to clarify private data center options, providing further definition.
3	Kevin Lane / Alex Lesberg 4 th District Court of Appeal	NI	<i>(Re: Sec. 6.0 bullet #6)</i> This bullet is confusing. Is this referring to Microsoft as the preferred vendor? Or does this mean that Microsoft Office is the standard productivity software suite?	The workstream is recommending Microsoft as the preferred vendor in order to maximize overall benefit to the branch. No further revisions were incorporated.
4	Kevin Lane / Alex Lesberg 4 th District Court of Appeal	NI	* General editing suggestion: Remove "trial" from "trial courts"	The workstream agreed with the commenter and updated the document to reflect application to all courts. "Trial" was removed, as suggested.

ITAC Next-Generation Hosting Workstream

Branch Comment on Next-Generation Hosting Framework Guide

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	Committee Response
5	Felix Castuera 1 st District Court of Appeal	A	Our court is on board with the recommendation to utilize cloud computing in the future. It makes sense for all courts to utilize other companies that offer cloud computing to minimize costs and at the same time improve services. The First District had implemented a light version of the proposed hybrid solution with Microsoft OneDrive. Our court still uses local servers, and at the same time, offers our staff the capability to save, access, and edit documents remotely through OneDrive.	The workstream supports this comment. No revisions were required related to this comment.
6	Jim Lin Information Technology Inyo Superior Court	NI	The major roadblock to implementing the aforementioned solutions is cost. We have 10 / 100 GB fiber running in our server closets, speed is not a hindrance. Cost also includes on prem storage of the 'e' initiatives. In one of our locations, we have abundant storage, but in another we have virtually 0 storage in case one location is lost, we will be dead in the water. Our court have 19 / 20 employees and moving to Office365 have been on my agenda for this court for past 9 months. The total cost to implement and yearly support is negligible compared to larger court's budget for an hour.	The workstream recognizes that many of the recommendations are not feasible in today's climate, due to budget and resource constraints. There will be impediments, but the intention is for the framework to provide court leadership with the foundation and guidance to move towards these strategic goals and objectives. No action required; therefore, the workstream did not incorporate revisions related to this comment.

ITAC Next-Generation Hosting Workstream

Branch Comment on Next-Generation Hosting Framework Guide

All comments are verbatim unless indicated by an asterisk (*).

	Commentator	Position	Comment	Committee Response
7	Jim Lin Information Technology Inyo Superior Court	NI	The end game of becoming an all-digital court is clear and I share those same sentiment as I stood in awe at Riverside's, Alameda's, and Yolo's courtrooms and how they have moved from dealing with paper to virtually paperless. Their move was precipitated in a large part with a new courtroom with newer equipment than the 7 – 8-year-old servers I am managing right now.	The goal is to have all courts and the branch to work toward implementing a Next Generation Hosting strategy as funding, budget and resources permit. No action required; therefore, the workstream did not incorporate revisions related to this comment.
8	Chris Stewart Chief Technology Officer Sacramento Superior Court	NI	Two additional 'cons' for the table: Branch Data Center: Vendor Hosted (Current CCTC Model) (pg. 13 or 14): 1. AD: Users end up with separate AD accounts and passwords. AD trusts between hosted and local forests may prove to be problematic and tough to manage at a larger scale. 2. Local courts are limited to hosted environment limitations (e.g. lack of interior dynamic routing protocol and automated backup VPN solution)	The workstream agreed with comment #1. There is also an Identity Management Initiative that may help address some of these issues in the long term. The workstream incorporated the suggested addition into the document. Comment #2 is a limitation of the current implementation not inherent in a vendor hosted solution. The workstream did not incorporate revisions related to this comment.

Status Reports



- Civil Case Management System (V3) Replacement Projects
- Sustain Justice Edition (SJE) Case Management System Replacement Projects
- Placer Court Hosting Consortium



JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue • San Francisco, California 94102-3688
Telephone 415-865-4200 • Fax 415-865-4205 • TDD 415-865-4272

MEMORANDUM

Date	Action Requested
December 13, 2017, 2017	Please Review
To	Deadline
Hon. Marsha G. Slough, Chair Hon. Gary Nadler, Vice-Chair Judicial Council Technology Committee	N/A
From	Contact
Kathleen Fink, Manager, Judicial Council Information Technology	Kathleen Fink, Manager 415-865-4094 kathleen.fink@jud.ca.gov
Subject	
Civil Case Management System (V3) Replacement Projects: Status November 17 – December 11, 2017	

Project: Civil Case Management System (CMS) (V3) Replacement projects for the Superior Courts of Orange, Sacramento, San Diego, and Ventura Counties

Status: The monthly Project Status meeting was held on December 11, 2017.

The Intra-Branch Agreement (IBA) for fiscal year 2017/2018 for Ventura has been executed. The IBA for Sacramento has been transmitted for court signature and the San Diego IBA is in process. Orange is validating the amounts needed for fiscal years 2016/17, 2017/18, and 2018/19.

Ventura (Journal Technologies eCourt): Configuration and testing on small claims case type is well underway and there are no new updates.

December 13, 2017

Page 2

San Diego (Tyler Odyssey): Traffic implementation successfully completed. The Statement of Work (SOW) with Tyler for civil, small claims, and probate case types has been signed. A kickoff meeting is planned for January 22, 2018.

Sacramento (Thomson Reuters C-Track): The court is working with Thomson Reuters to finalize the participation agreement for the design and discovery phase. The court is also working on an SOW with Independent Verification and Validation services.

Orange (Update CMS V3 for supportability and reliability): Development and test environments are set up. Technical staff are working with Judicial Council Information Technology V3 staff to validate the code build environment. Planning to deploy the JCC V3 release package for R13.11 in production (January 1), then rebuild the release from the source and redeploy the version through development, test, and production. Targeting to complete by the end of January 2018.



JUDICIAL COUNCIL OF CALIFORNIA

455 Golden Gate Avenue
San Francisco, CA 94102-3688
Tel 415-865-4200
TDD 415-865-4272
Fax 415-865-4205
www.courts.ca.gov

HON. TANIG. CANTIL-SAKAUYE
*Chief Justice of California
Chair of the Judicial Council*

MR. MARTIN HOSHINO
*Administrative Director,
Judicial Council*

TECHNOLOGY COMMITTEE

HON. MARSHA G. SLOUGH
Chair

HON. DANIEL J. BUCKLEY
Vice-chair

*Hon. Kyle S. Brodie
Mr. Jake Chatters
Hon. Ming W. Chin
Mr. Richard D. Feldstein
Hon. David E. Gunn
Ms. Audra Ibarra
Hon. Gary Nadler
Ms. Debra Elaine Pole*

Date

December 15, 2017

To

Hon. Marsha G. Slough, Chair
Hon. Gary Nadler, Vice-Chair
Judicial Council Technology Committee

From

David Koon
Manager, Judicial Council Information
Technology

Subject

Sustain Justice Edition (SJE) Replacement
Projects - Status September 27 –
December 15, 2017

Action Requested

Please Review

Deadline

N/A

Contact

David Koon
David.koon@jud.ca.gov

Members of the Judicial Council Technology Committee:

As requested, this communication provides a written update regarding the progress of the nine Sustain Courts which received \$4.1 million in funding for FY 17/18 as a result of submitting a BCP to replace the Sustain Justice Edition case management system with a modern CMS platform.

Project: Sustain Justice Edition (SJE) Replacement projects for the Superior Courts of Humboldt, Lake, Madera, Modoc, Plumas, San Benito, Sierra, Trinity, and Tuolumne counties.

Status: The SJE Courts and Judicial Council IT staff are continuing to work on identifying the installment payments and high-level project milestones to be included in each court's Intra-Branch Agreement (IBA).

Next Steps: Finalize each court's IBA based upon the installment payments and high-level milestones identified so that work can begin to implement a new CMS. There is a meeting scheduled on January 12th between the nine courts and the vendor to discuss various items including project schedule.

Further updates will be provided in upcoming meetings. Thank you.

Monthly Project Monitoring Report

Report Period: 11/01/2017-12/4/2017
Report Date: 12/5/2017
Court Name: Placer
Prepared By: Greg Harding



JUDICIAL COUNCIL
OF CALIFORNIA
ADMINISTRATIVE DIVISION
INFORMATION TECHNOLOGY

Project Name	Placer County Hosting Center
Court Project Manager	Greg Harding
IBA Number	1033111
IBA Effective Date	11/1/2016
IBA End Date	4/30/2019
Project Start Date	October 2015
Estimated Finish Date	January 2018
Estimated % Complete	90%

1. Accomplishments / Plans

Accomplishments during *this Reporting Period*:

- Lake Superior Court migration to PCHC complete
- CDI/CDR configured for Lake, Modoc
- San Benito's Interfaces ready for testing

Plans during the *next Reporting Period*:

- Modoc Superior Court Go-live Dec 16th

2. Risks and Issues

Issue Status (Issues requiring resolution or others that may affect the proposed approach baseline):

-

Change Status (Considerations or new course of actions that change the proposed approach):

-

Risk Status (Report risks to the current approach, any risks discovered, and proposed risk responses):

- San Benito Interface Sustain SJE DII issues

3. Scheduled Milestones / Deliverables

List any Milestones that are late as well as Milestones due in the next 4 to 6 weeks (as applicable).

Milestone	Due Date (Actual)	Status
WBS 15.1 – Plumas/Sierra go-live plan created	9/16/2017	Complete
WBS 15.2 – Plumas/Sierra CMS hosting transition complete	9/16/2017	Complete
WBS 15.3 – Plumas/Sierra Managed Court services transition complete	9/16/2017	Complete
WBS 16.1 Lake go live plan created	9/20/2017	Complete

4. Payment Schedule and Milestones

List IBA payment milestones that have been completed, are yet to be completed, total IBA amount and payments remaining to be made.

IBA Installment Payments	IBA Installment Amount	IBA Payment Date	IBA Actual Payment
Court signs executed contracts with vendors	\$265,599.00		
Court develops all hardware and software specifications	\$470,901.00		
Total IBA Amount	\$736,500.00		
Remaining IBA Amount To Be Paid	\$736,500.00		
Project Tracking Milestones	Project Milestone Target Date	Project Milestone Actual Date	N/A For Project Milestone Tracking
WBS 1 – CCTC Requirements Document Completed	NOV 16	DEC 16	
WBS2 – Server Design	MAR17	FEB 17	
WBS3 – Server Build	APR17	APR17	
WBS4 – Network and Connectivity Design	JAN 17	JAN 17	
WBS5 – Network and Connectivity Implemented with connectivity to CCTC	MAY 17	JUNE 17	
WBS6 – Information Systems Framework and Security Policies Developed and Implemented	JUL17	AUG 17	
WBS7 – DMV Service Transition	JUL 17	AUG 17	
WBS7.1 – DMV DISA Approval	MAR 17	FEB 17	
WBS7.2 – DMV Connectivity Configured and implemented	JUN 17	APR17	
WBS9 – Interface rework completed	JUL 17	SEPT 17	
WBS10 – SJE Core Environments Created	MAY 17	MAY 17	
WBS11 – Initial SJE Data Copy	MAY 17	MAY 17	
WBS12 – Non-CMS Applications Installed	JUN 17	MAY 17	
WBS 13 – UAT of CCTC connectivity	SEPT 17	SEPT 17	
WBS14 –UAT of SJE and interfaces including DMV	AUG 17	AUG 17	
WBS15 – UAT of “managed court” services	SEPT 17	SEPT 17	
WBS 15.1 – Plumas/Sierra go-live plan created	AUG 17	AUG 17	
WBS 15.2 – Plumas/Sierra CMS hosting transition complete	OCT 17	SEPT 17	
WBS 15.3 – Plumas/Sierra Managed Court services transition complete	OCT 17	SEPT 17	

