2023 IT Capacity Assessment

Start of Block: INTRODUCTION

TECHNOLOGY FOR EDUCATION 2023 CAPACITY ASSESSMENT The Office of Digital Teaching and Learning at the Arizona Department of Education works in collaboration with the community of educators and solution experts to develop strategies that build capacity in IT. Areas of focus are 1) connectivity, 2) cybersecurity, 3) policies and procedures, 4) economies of scale, and 5) professional development for IT, EdTech leaders, teachers and staff.

By completing the 2023 Capacity Assessment you will inform future strategies and initiatives that ADE will bring to K12. But not only that: this assessment is **much more than a survey!!** This assessment is designed to be a tool that provides information and many resources for your immediate consumption and use. What to expect? Resources to develop your IT and EdTech departments. A tool to measure the maturity level of your Disaster Recover Plans, plus resources to improve disaster planning. Cybersecurity resources and guidance. A tool to measure the status of your Policies and Procedures in IT and templates to complete any lacking policy or procedure. Many more resources for professional development in your district.

Instructions: Please answer this assessment at the **District** level. You can pause and resume the survey at any time. To save your responses click on "Save and Next" and then close your browser. You can go back and edit your responses only within a section. Once you receive results for a section, you cannot edit to your responses. To resume the assessment simply click on the link that you received by email, making sure that you always use the same computer and same browser. This assessment works best over a laptop or computer device. Before you initiate the assessment, review this LINK with details**.**

At the end of this assessment you will receive a summary with all the links for resources provided throughout the assessment. For any questions or for support please email us at ODTL@azed.gov

Click the START button to initiate the assessment

End of Block: INTRODUCTION

Start of Block: LEA AND CONTACT INFORMATION

CONTACT INFORMATION

Let's start with the information about the district you represent and your contact information.

Please remember, your responses are at the district level. If you don't feel qualified to respond on behalf of your district, please send this assessment to an IT district representative.

LEA Name
Provide the name of the LEA (Local Education Agency) that you are representing.

_____

District or Charter
Select whether the LEA you represent is a charter school or a school district (non-charter).
1

▼ Charter ... District

County
Select the county where your LEA main offices reside.
15

▼ Apache ... Mohave

Student Count
Provide the count of total full-time students enrolled this year in your district. We will use this information for some calculations later on during this assessment.

_____

Virtual Students
If your school district is involved in distance learning, provide the count of students that are fully virtual/remote at your district. If there is no distance learning at your district, enter 0.

_____

Please enter your contact information

- First Name _____
- Last Name _____
- Email _____
- Title _____

Start of Block: COMPOSITION OF IT DEPARTMENT

IT DEPARTMENT

"Technology plays an integral part in all aspects of school life, from its use to engage students, to a vehicle to connect teachers from across the district, to streamline administrative tasks such as payroll, to conduct assessment testing, and as an efficient way to communicate with parents and the community. But who oversees the all-encompassing technology initiatives in your school district? Education technology leaders are like not other IT professionals. Not only must they know all the current and emerging technologies, they must have a deep understanding of how this technology can be used to transform education." *(*COSN Building an Effective District

Technology Team)

The next questions seek to understand how your district's IT department is structured and the services that it offers. After completing this section you will be presented with some resources to help you develop your IT team.

What is the size of your IT Department
How many staff members do you have in IT - include full time staff and contracted staff.

_____

What is the title of the leader of the IT department at your school district?

- ○ IT Director
- ○ IT Manager
- ○ Chief Technology Officer
- ○ Chief Information Officer
- ○ Other (pls specify) _____

What department does the IT leader report to?

- ○ Finance / Business Office
- ○ Operations
- ○ Academic / Education Services
- ○ Superintendent
- ○ Other (please specify) _____

Do you have a technical contact per campus to support your student and teacher needs?

- ○ Yes, one technical contact for each campus
- ○ Yes for most of them. Some sites share a technical contact
- ○ No, we do not have enough technical contacts to support each campus
- ○ I don't know

Do you outsource any part of your IT services / use Managed IT Service Providers?
A managed service provider (MSP) delivers services, such as network, application, infrastructure, and security, via ongoing and regular support to an LEA.

- ○ Yes
- ○ No
- ○ I don't know

What is the name of your Managed IT Service Provider(s)?

_____

What services do you outsource to the IT service provider(s)?
Select all that apply

- ☐ Technical Help Desk
- ☐ SIS administration
- ☐ LMS administration
- ☐ Network and Infrastructure
- ☐ Cybersecurity
- ☐ Technical Asset Management
- ☐ Data Management
- ☐ Application Development
- ☐ Other (Specify) _____

What services does your IT department provide in house for the district (not outsourced)?
Select all that apply

- [ ] Technical Help Desk
- [ ] SIS administration
- [ ] LMS administration
- [ ] Network and Infrastructure
- [ ] Cybersecurity
- [ ] Technical Asset Management
- [ ] Data Management
- [ ] Application Development
- [ ] Other (Specify) _____

Is there a leader of Educational Technology in your school district?

- ○ Yes, and the EdTech leader reports to IT
- ○ Yes, and the EdTech leader reports to a different department (not IT)
- ○ No, we do not have an EdTech leader in our district
- ○ I don't know

What department does the Educational Technology leader report to?

- ○ Finance / Business Office
- ○ Operations
- ○ Academic / Education Services
- ○ Superintendent
- ○ Other (please specify) _____

Would you please provide the contact information of your EdTech leader?

- ○ Name _____
- ○ Email _____

Start of Block: RESULTS: COMPOSITION OF IT DEPARTMENT

RESULTS HAVE BEEN REMOVED FROM THIS PREVIEW

Start of Block: IT POLICIES AND PROCEDURES

POLICIES AND PROCEDURES

IT policies and procedures **provide clarity for everyone in the school district** about the expected practices in the use of technology. Documentation of IT policies and procedures is a form of risk management as it allows for consistency in operations. IT leaders are expected to model responsible management of the creation, implementation, and enforcement of policies related to the social, legal, and ethical issues linked to technology use throughout the school system.

By definition, policies are formal statements issued by management to implement strategic goals, objectives, and operating principles. Procedures are approved step-by-step instructions to be applied consistently across the enterprise. Yet another term is a "Standard." Standards define the means and methods to implement the policy consistently across the enterprise. (Source: Arizona Strategic Enterprise Technology ASET)

This section assesses the IT key functional areas in your district that are covered by policies or procedures and assigns a score based on their status. Upon completion of this section you will receive a set of resources to assist the development and implementation of policies and procedures in your school district.

Please know that the development of policies and procedures is a sequential process. A developing organization may start with only the first five or six documents listed below. As an organization grows and matures, more policies and procedures are required for sustaining their operations. The order in which policies and procedures are listed below is a recommendation based on our experience in the sector. ***The list and the order are not prescriptive and not exhaustive and do not contain specific requirements from the Board of Education or any other governing entity.***

How do you categorize the status of your **Data Security and Privacy policy**?
This document defines who has access to data and access to the data is restricted.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

2. How do you categorize the status of your **Acceptable Use Policy**?
This document outlines constraints and practices that a user must agree to for access to school district technology, the internet or other resources.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

3. What is the status of your **Asset Management policy / end-of life asset management**?
This document serves to establish the rules for the control of hardware, software, applications, and information used by the school district

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

4. How do you categorize the status of your **Security Awareness and Training Policy**?
This policy sets out what security awareness training employees are expected to partake in,

what form the training will take and when it will be carried out, and what the penalties are for non-participation.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

5. How do you categorize the status of your **Backup and Recovery Policy**?
This document specifies how data will be backed up, what measures will be taken to recover from a disaster, and who has access to the backups.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

6. How do you categorize the status of your **Internet Safety Policy (CIPA Compliance)**?
The Children's Internet Protection Act (CIPA) requires certain K-12 schools and libraries to certify that they are enforcing an internet safety policy that includes technology protection measures in order to be eligible for federal funding and discounts for internet access through the E-Rate program.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

7. How do you categorize the status of your **Identity and Access Management Policy**?
Identity and access management (IAM) is a framework of business processes, policies and technologies that facilitates the management of electronic or digital identities.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

8. How do you categorize the status of your procedure for **Vetting Online Applications** for the classroom?
This is a step by step documentation of the process to follow when a staff member wants to request approval to use an online resource in the classroom, and what type of validations and authorizations are required.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

9. How do you categorize the status of your **Information Security Policy**?
This is the aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

10. How do you categorize the status of your **Network and Communications Security Policy**?
This policy helps ensure the protection of information in network and facilities to ensure confidentiality, integrity and availability of information.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

11. How do you categorize the status of your **Vulnerability Management Policy**?
This policy helps to establish the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment and the risks associated with them.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

12. How do you categorize the status of your **Endpoint Security Policy**?
The Endpoint security policies are designed to focus on the security of devices and mitigate risk.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

13. How do you categorize the status of your **Security Incident Management Policy**?
This policy establishes the necessary controls to detect security vulnerabilities and incidents, as well as the processes and procedures to resolve them.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

14. How do you categorize the status of your **Security Risk Management Policy**?
This policy provides risk assessment for security incidents.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

15. How do you categorize the status of your **Security Threat Detection Policy**?
This policy documents the ways in which the school district proactively implements ways to identify threats before they impact the business.

- ○ We do not have such policy and do not plan to create one
- ○ We do not have such policy but would like to start one
- ○ We have drafted / initiated documentation of the policy
- ○ We have finalized documentation of this policy but have not yet implemented it
- ○ This policy is fully implemented and we have reached 100% adoption
- ○ I don't know

End of Block: IT POLICIES AND PROCEDURES

Start of Block: RESULTS: IT POLICIES AND PROCEDURES

RESULTS HAVE BEEN REMOVED FROM THIS PREVIEW

End of Block: RESULTS: IT POLICIES AND PROCEDURES

Start of Block: CYBERSECURITY

CYBERSECURITY

Managing cybersecurity is all about managing risk and the identification of your district's risk tolerance and budget considerations.

The responsibility for Cybersecurity decisions does not lie only on the IT department and managing cybersecurity risk is the responsibility not only of IT but administrators, board members, students, parents, teachers and staff.

It’s not “If we get attacked”; it’s “When we get attacked.”
The next questions seek to understand cyber security readiness at your school district.

Please indicate the amount of people (staff) within your IT department that have knowledge and training in Cybersecurity operations

_____

Is your School District a current member of The Trust?

- ○ Yes
- ○ No

The following questions seek to understand whether your LEA has the minimum requirements for cyber security and identify gaps / needs for support.

Phishing Simulation

Do you have a solution for Phishing Simulations and Training?

- ○ Yes
- ○ No
- ○ I don't know

When was the last time you conducted Phishing Simulation at your district?

- ○ Within the last 6 months
- ○ Within the last year
- ○ Within the last 3 years
- ○ More than 3 years ago
- ○ We have never ran a phishing simulation
- ○ I don't know

Multifactor Authentication

Do you have a solution for Multifactor Authentication (MFA)?

- ○ Yes
- ○ No
- ○ I don't know

Vulnerability Management

Do you have a solution for Vulnerability Scanning?

- ○ Yes
- ○ No
- ○ I don't know

When was the last time you ran a Vulnerability Scan?

- ○ Within the last 6 months
- ○ Within the last year
- ○ Within the last 3 years
- ○ More than 3 years ago
- ○ We have never ran a vulnerability scan
- ○ I don’t know

Endpoint Detection and Response (EDR)

Do you have software for Endpoint Detection and Response (EDR)?

- ○ Yes
- ○ No
- ○ I don't know

Software Patching

Do you have a solution for software patching?

- ○ Yes
- ○ No
- ○ I don't know

Security Awareness Training

Do you have Security Awareness Training available for your staff, including teachers?

- ○ Yes
- ○ No
- ○ I don't know

Do you have Security Awareness Training available for your students?

- ○ Yes
- ○ No
- ○ I don't know

Network Penetration Testing

Do you have a service for periodic Network Penetration Testing at your district?

- ○ Yes
- ○ No
- ○ I don't know

When was the last time that you conducted a Penetration Test?

- ○ Within the last 6 months
- ○ Within the last year
- ○ Within the last 3 years
- ○ More than 3 years ago
- ○ We have never ran a penetration test
- ○ I don’t know

Do you meet The Trust's requirements for Multifactor Authentication (MFA)?

- ○ Yes
- ○ Not yet but we are working on meeting the requirements
- ○ No, and we need help to meet the requirements
- ○ I don't know

Do you meet The Trust's requirements for Endpoint Detection and Response (EDR)?

- ○ Yes
- ○ Not yet but we are working on meeting the requirements
- ○ No, and we need help to meet the requirements
- ○ I don't know

What is your **annual budget** for license and maintenance of cybersecurity solutions for your district?

_____

Is your school district participating in the Cyber-readiness Program with the State of Arizona?

- ○ Yes
- ○ No
- ○ I don't know

Please indicate the reasons why you are not choosing to join the state Cyber-readiness program

_____
_____
_____
_____
_____

Please provide feedback of your experience participating in Cyber-readiness program with the Arizona State

_____
_____
_____
_____
_____

Start of Block: RESULTS: CYBERSECURITY

RESULTS: CYBERSECURITY

RESULTS HAVE BEEN REMOVED FROM THIS PREVIEW

End of Block: RESULTS: CYBERSECURITY

DISASTER RECOVERY PLANS

A disaster recovery plan (DRP) is a formal document that details instructions on how to respond to unplanned incidents. Frequently developed together with a district-wide Business Continuity Plan, the focus of the DRP is to have an alternative course of action during interruptions in technology and a plan for how to restore data access and IT infrastructure after a disruptive event.

In the next section you will find a tool that outlines a comprehensive list of requirements for your DRP program. The goal of this tool is to help you assess the maturity of your Disaster Recovery Plans. The tool includes components for three phases of the process: 1) defining DR requirements, 2) implementing a solution, and 3) maintaining and testing your DRP.

This tool has been developed by Info-Tech Research Group and is based on the Capability Maturity Model Integration (CMMI).

At the end of the completion of this section you will receive a score and more resources to assist in your Disaster Recovery Plan.

Does your school district have board-approved Disaster Recover Plans?

- ○ Yes
- ○ No
- ○ I don't know

ASSESSMENT FOR DEFINING DRP REQUIREMENTS

ASSET MANAGEMENT: *IT asset management (ITAM) is the process of ensuring all assets are accounted for, deployed, maintained, upgraded, and disposed of when the time comes.*

How do you categorize the status of your **Hardware Asset Management and Documentation**?

- ○ No asset documentation
- ○ Ad hoc asset management tracking
- ○ Informal asset management processes
- ○ Asset management processes are standardized
- ○ Asset management processes are standardized, audited and supported by effective ITAM tools to facilitate tracking and reporting
- ○ Asset management processes have been optimized and are reviewed at least annually for further optimization as needed

How do you categorize the status of your **Software Asset Management and Documentation**?

- ○ No asset documentation
- ○ Ad hoc asset management tracking
- ○ Informal asset management processes
- ○ Asset management processes are standardized
- ○ Asset management processes are standardized, audited and supported by effective ITAM tools to facilitate tracking and reporting
- ○ Asset management processes have been optimized and are reviewed at least annually for further optimization as needed

BUSINESS IMPACT ANALYSIS: *this section evaluates the consequences of disruption of a business function and process and develops recovery strategies*

How do you categorize the status of your **Systems/Applications prioritization**?

- ○ No prioritization
- ○ Ad hoc prioritization
- ○ Informal assessment (e.g. subjective discussion and not formally approved)
- ○ Assessment is standardized, documented and approved by business leaders
- ○ Assessments uses quantitative (e.g. financial impact) and qualitative (e.g. strategic impact) measurements to determine criticality
- ○ The process has been optimized and reviewed and approved at least annually for further optimization as needed

How do you categorize the status of your assignment of **Recovery Time Objectives (RTO)**?
RTO is the overall length of time an information system's components can be in the recovery phase before negatively impacting the business.

- ○ No RTOs assigned
- ○ Ad hoc assignment of RTOs
- ○ Informal RTO assignment (not based on impact analysis)
- ○ RTO assignment is based on impact analysis, documented and approved by board
- ○ RTO assignment is based on a standardized, comprehensive quantitative and qualitative impact analysis
- ○ RTOs are reviewed, updated and approved as required at least annually

How do you categorize the status of your assignment of **Recovery Point Objectives**?
Recovery point objective (RPO) is the point in time to which data must be recovered after an outage.

- ○ No RPOs assigned
- ○ Ad hoc assignment of RPOs
- ○ Informal RPO assignment (not based on impact analysis)
- ○ RPO assignment is based on impact analysis, documented and approved by board
- ○ RPO assignment is based on a standardized, comprehensive quantitative and qualitative impact analysis
- ○ RPOs are reviewed, updated and approved as required at least annually

RISK MANAGEMENT: *this is the process of identifying, assessing, and controlling risks.*

Indicate the level at which risks have been assessed and mitigated as part of your Disaster Recovery Plan?

- ○ No risk assessment
- ○ Ad hoc risk assessment (no standard process or documentation)
- ○ Informal risk assessment (e.g. executed but not documented)
- ○ Risk assessment is standardized (e.g. structured risk evaluation and documentation)
- ○ Risk assessment uses quantitative and qualitative measurements, and risks are prioritized accordingly
- ○ The risk assessment process has been optimized and is reviewed and approved by the board at least annually for further optimization as needed

ASSESSMENT FOR IMPLEMENTING YOUR DRP

DISASTER RECOVERY TECHNOLOGY*: this section is about the technology solutions you have to support your DR plans.*

How do you categorize the level of your **Offsite Backups** (as part of your data protection strategy)?
Offsite backups refers to the practice of backing up data somewhere outside of your primary data center

- ○ No data protection strategy that considers disaster recovery requirements (i.e. offsite backups, replication).
- ○ Ad hoc data protection strategy to support Disaster Recovery
- ○ Informal data protection strategy (e.g. not documented)
- ○ Data protection strategy is documented and meets minimum recovery requirements like long-term backup retention to mitigate the risk that recent backups are compromised (e.g. due to a ransomware attack)
- ○ Data protection strategy meets designated RTOs and RPOs to ensure alignment with business requirements
- ○ Data protection strategy has been optimized and is reviewed at least annually for further optimization as needed

How do you categorize your status of implementation of a Disaster Recovery solution?
Examples of DR solution would be a DR site, cloud-based DR, DRaaS

- ○ No assessment of potential solutions
- ○ Limited informal assessment of specific options
- ○ Informal assessment of multiple DR solutions and potential fit
- ○ Multiple DR solution options evaluated based on specific requirements (e.g. able to execute with limited staff)
- ○ DR solution meets designated RTOs and RPOs to ensure alignment with business requirements
- ○ Solution planning includes short- and long-term outage scenarios

How have you ensured that vendors for outsourced IT services or Managed Service Providers (including cloud-based-services) meet your Disaster Recovery requirements (e.g. RTOs and RPOs)?

- ○ no vendor assessment
- ○ Ad hoc assessment
- ○ Informal assessment (not documented)
- ○ Standard documented assessment process
- ○ Vendors are evaluated using quantitative (ability to meet RTOs and RPOs) and qualitative measurements (e.g. incident response plan clarity)
- ○ Vendor assessments are reviewed, updated, and approved at least annually during annual reviews

Disaster Recovery Procedures: *this section is in regards to the steps you take, and the documentation of such steps, in preparation to incidents.*

How do you categorize the status of your documentation for Disaster Notification, Assessment and Declaration?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

How do you categorize the status of your Recovery Procedures for your critical applications and systems?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

How do you categorize the status of your Post-failover IT operations documentation (e.g. backups and maintenance processes for Disaster Recovery)?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

How do you categorize the status of your Repatriation Procedures (i.e. failing back to the primary site)?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

Disaster Recovery Awareness and Training: *this section is about communication of DRP plans and training for users.*

How do you categorize the status of your documentation for Disaster Recovery Team Roles and

Responsibilities?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

How do you categorize the status of your documentation of Vendor Roles and Responsibilities and their contact information for a Disaster Recovery Event?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

How do you categorize the status of your Disaster Recovery Summaries (summaries presented to leadership and to the board)?

- ○ No documentation
- ○ Ad hoc documentation process. Documentation is created sporadically, if at all, without a consistent approach
- ○ Informal documentation process (e.g. not using consistent templates or guidelines)
- ○ Standard documentation process (e.g. structured approach guided by templates)
- ○ Documentation is evaluated and updated using quantitative (e.g. all requirements met?) and qualitative measurements (e.g. clarity, usability)
- ○ Documentation is reviewed and optimized (if needed) at least annually. This includes reviewing and optimizing the documentation process

ASSESSMENT FOR MAINTAINING YOUR DRP

Disaster Recovery Testing: *this is the process to ensure that your organization can restore data and applications and continue operations after an interruption of its services, critical IT failure or complete disruption*

How do you categorize the status of your **Tabletop Exercises** for Disaster Recovery incident response?
Tabletop exercises are sessions where team members meet to discuss their roles during an incident and rehearse the steps to take.

- ○ No testing within the last year
- ○ Ad hoc testing process
- ○ Informal test plans (not documented)
- ○ Complete documented test plans (e.g. include scope, schedules, participants). Action items driven by testing are scheduled, tracked, and confirmed upon completion
- ○ Testing is prioritized based on risk (e.g. system criticality and the amount of system change); i.e. deeper testing where warranted
- ○ Test plans are updated at least annually to address a range of scenarios and evolving priorities (e.g. ransomware, cloud-based services, etc.)

How do you categorize the status of your **testing your Disaster Recovery technology?**
For example, the ability to failover to your DR environment), which is recommended to be executed at least annually.

- ○ No testing within the last year
- ○ Ad hoc testing process
- ○ Informal test plans (not documented)
- ○ Complete documented test plans (e.g. include scope, schedules, participants). Action items driven by testing are scheduled, tracked, and confirmed upon completion
- ○ Testing is prioritized based on risk (e.g. system criticality and the amount of system change); i.e. deeper testing where warranted
- ○ Test plans are updated at least annually to address a range of scenarios and evolving priorities (e.g. ransomware, cloud-based services, etc.)

How do you categorize the status of your **Failback testing**
Recommended to be executed at least annually, a failback test assesses the process of returning production to its original location after a disaster.

- ○ No testing within the last year
- ○ Ad hoc testing process
- ○ Informal test plans (not documented)
- ○ Complete documented test plans (e.g. include scope, schedules, participants). Action items driven by testing are scheduled, tracked, and confirmed upon completion
- ○ Testing is prioritized based on risk (e.g. system criticality and the amount of system change); i.e. deeper testing where warranted
- ○ Test plans are updated at least annually to address a range of scenarios and evolving priorities (e.g. ransomware, cloud-based services, etc.)

DRP Documentation Management: *refers to the documentation, maintenance, distribution and easy access to material pertaining disaster recovery plans.*

How do you categorize the level of documentation of your Content Management?

- ○ No content management
- ○ Ad hoc process
- ○ Informally managed (not documented)
- ○ Standardized, documented content management process
- ○ DRP documentation status is tracked and reported and includes version control and change history
- ○ DRP documentation management process and solution are reviewed and optimized (if needed) at least annually

---

How accessible are your Disaster Recovery Plans in a disaster?

- ○ No process for ensuring DRP can be accessed
- ○ Ad hoc process (e.g. individuals might download a copy on their own)
- ○ Informally managed (e.g. DR team maintains an offsite copy but not managed)
- ○ Standardized, documented process for ensuring required stakeholders can access the DRP
- ○ DRP availability accounts for a range of scenarios (e.g. if the internet is down)
- ○ Process for ensuring DRP availability is reviewed and optimized (if needed) at least annually

DRP Change Management: *A robust change management approach can help you avoid making unnecessary or rash changes without thorough planning and analysis.*

How do you categorize your **DRP formal reviews**?
Recommended to happen at least annually, a DRP review evaluates the accuracy of a DRP based on the most current business and system factors.

- ○ No review
- ○ Ad hoc review process
- ○ Informal review (not documented)
- ○ Complete documented review (e.g. includes review scope, schedules, participants). Action items driven by DRP review are scheduled, tracked, and confirmed upon completion
- ○ Review efforts are prioritized based on risk (e.g. system criticality and the amount of system change); i.e. deeper review where warranted
- ○ DRP review process is reviewed and optimized (if needed) at least annually

---

To what extent are your IT changes incorporated into your DRP as they occur?

- ○ No integration with IT change management
- ○ Ad hoc communication of DRP implications
- ○ Informal process (not part of the documented change management process)
- ○ Standard component of your change management process (e.g. RFC requires requestors to indicate whether the change affects your DR solution, objectives, or documentation)
- ○ Action items driven by change management are scheduled, tracked, and confirmed upon completion
- ○ Integration with the change management process is reviewed and optimized (if needed) at least annually

---

To what extent are Business changes incorporated into your DRP as they occur?

- ○ No integration with IT change management
- ○ Ad hoc communication of DRP implications
- ○ Informal process (not part of the documented change management process)
- ○ Standard component of your change management process (e.g. RFC requires requestors to indicate whether the change affects your DR solution, objectives, or documentation)
- ○ Action items driven by change management are scheduled, tracked, and confirmed upon completion
- ○ Integration with the change management process is reviewed and optimized (if needed) at least annually

---

Start of Block: RESULTS: DISASTER RECOVERY PLANS

RESULTS HAVE BEEN REMOVED FROM THIS PREVIEW

End of Block: RESULTS: DISASTER RECOVERY PLANS

Start of Block: CONNECTIVITY

CONNECTIVITY

It is estimated that over 20% of our K12 students in Arizona lack internet connectivity at home or are "under-connected." Students and families who are considered under-connected are those who have internet access and devices in their home, but not of sufficient quality for consistent use. While most of our students have returned to school, connectivity at home is still a factor that provides significant advantage to students of all ages. The ability to do homework from home, research, practice and even collaborate in groups is limited for students who are under-connected.

This section is short and aims to capture the basic elements to understand how your school district is managing internet connectivity for school and home.

To what extent does your district capture information regarding your students' level of connectivity at home?

- ○ We do not record information of student connectivity at home.
- ○ We only recorded information about connectivity during COVID / distance learning
- ○ We sometimes collect information about connectivity at home (about once a year)
- ○ We regularly capture information about students' connectivity at home

---

What are you doing with the information gathered regarding students' connectivity at home. Please describe actions taken with these data.

_____
_____
_____
_____
_____

To what extend are you using E-Rate in your school district?

- ○ Yes we use E-Rate and we believe that we are maximizing its benefit
- ○ Yes we use E-Rate but still need help to make sure we maximize the benefit
- ○ No, we know about E-Rate but choose not to use it
- ○ No, we do not know about E-Rate

Do you use an external consultant to guide you on eRate? If so, provide the company or consultant you use

- ○ No, we do not use an E-Rate external consultant
- ○ Yes (add the name on this text box)

_____

End of Block: CONNECTIVITY

Start of Block: ECONOMIES OF SCALE

ECONOMIES OF SCALE

The Office of Digital Teaching and Learning is exploring opportunities to achieve economies of scale by combining the purchasing power from multiple school districts. The following questions aim to capture your feedback on this topic. We will also be asking you to provide the current annual cost of your enterprise applications as well as the number of users. This will allow us to calculate the cost per user and find efficiencies statewide.

Please estimate the percentage of unallocated assets at your school district.
Unallocated assets are computers or devices not in use by either a student, staff or teacher.

_____

Is your school district in a 1:1 model?
A 1:1 model provides one device for each student in the district.

- ○ No, we do not do 1:1 for student devices
- ○ We have a 1:1 program for some grade levels but not for all
- ○ Yes, we have a 1:1 program for all grade levels in our district

Do you allow your students in 1:1 model to take their devices to their home?

- ○ Yes, all our 1:1 students are allowed to take their devices home
- ○ Yes, some of our 1:1 students take their devices home
- ○ No, taking devices home is not an option

Is your school district currently part of a Cooperative or group through which you can collectively negotiate better pricing for the purchase of technology? If so, select the name of the Cooperative

- ☐ No, we are not part of a Cooperative
- ☐ 1Government Procurement Alliance (1GPA)
- ☐ Arizona Cooperative Program
- ☐ Mohave Cooperative
- ☐ Western States Contracting Alliance (WSCA)
- ☐ Yavapai Consortium
- ☐ Yuma Cooperative
- ☐ Other (please specify)

_____

Please provide the cost of your annual investment for each of the following Enterprise Applications.

Student Information System

- Annual cost for your Student Information System ($) _____
- Number of students in your Student Information System _____
- Name of your Student Information System _____

Learning Management System

- Annual cost for your primary Learning Management System ($) _____
- Number of students using your primary Learning Management System _____
- What is the name of your primary Learning Management System _____

Filtering Software

- Annual cost for Filtering Software (to meet CIPA Compliance requirements) ($) _____
- Number of student devices with filtering software _____
- Name of the Software you use _____

Help Desk System

- Annual cost of your Help Desk system ($) _____
- Number of users of your Help Desk system _____
- Name of your Help Desk system _____

End of Block: ECONOMIES OF SCALE

Start of Block: EDUCATIONAL TECHNOLOGY

EDUCATIONAL TECHNOLOGY

This section focuses on Professional Development for teachers and staff in general.

As you complete this section please consider feedback from your administrators and leaders for academics and curriculum. The first three questions target the Educational Technology units from your school district.

PD in Educational Technology: In an effort to continue building capacity in Digital Teaching and Learning, ADE is working on diverse other professional learning opportunities for teachers to develop their expertise in technology for instruction.

Which of the following professional development areas are you interested in receiving support from ADE? Drag and drop your choices as you **prioritize** the type of training you desire to receive for your district *(move top priority to the top, lowest priority to the bottom)*.

_____ Digital Citizenship & Safety
_____ Student Data Privacy & Security
_____ Cybersecurity Awareness Training for Teachers
_____ Technology Basics for Users
_____ Chromebook Basics for Teachers
_____ Digital Learning Environment
_____ Instructional Planning based on Arizona's Educational Technology Standards
_____ Pedagogical Strategies for Tech Integration
_____ Others (please specify)

Programs for Technology for Instruction: the use of technology, when linked to the appropriate pedagogical standards, becomes an important enabler for instruction. Which of the following programs - if any - is your district interested in hearing about? select all that apply.

- ☐ Implementation of a Robotics program
- ☐ Implementation of a Esports program
- ☐ Gamification in the Classroom (Minecraft for Education)
- ☐ EdTech Certified Leader (ISTE Program)
- ☐ Others (please specify)

_____

Is there any additional feedback you have regarding Professional Development / Capacity Building opportunities for your teachers and staff in general?

_____
_____
_____
_____
_____

End of Block: EDUCATIONAL TECHNOLOGY

Start of Block: GENERAL FEEDBACK

The Office of Digital Teaching and Learning has been operating for over one year now. Please provide feedback of ways in which you have engaged with this office. How have we helped your district?

_____
_____
_____
_____
_____

In addition to the support available from the State around Digital Teaching and Learning, is there any additional support you will need to achieve your digital goals?

_____
_____
_____
_____
_____