TUCSON UNIFIED
SCHOOL DISTRICT

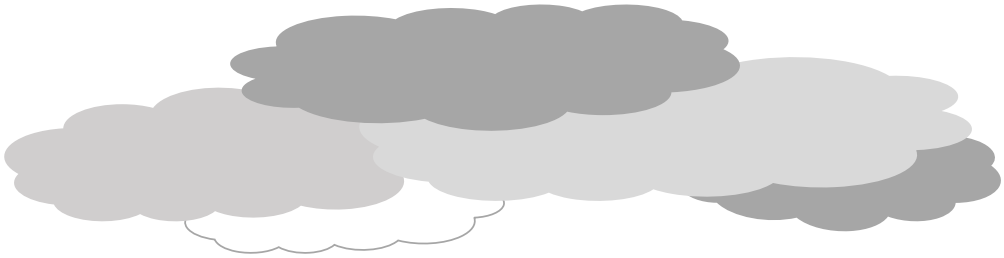
October 25, 2021

Office of Internal Audit

Risk Management

District's Business Continuity Plan / Disaster Recovery Plan (BCP/DRP)

Internal Audit Report



MARTHA SMITH

REPORT #: 001_FY2021-2022

TUCSON UNIFIED SCHOOL DISTRICT | 1010 E. Tenth Street, Tucson, AZ, 85719
Desk Phone 520-225-6073

EXECUTIVE SUMMARY

The Office of Internal Audit has performed the Business Continuity Plan and Disaster Recovery Plan (BCP/DRP) audit for the Tucson Unified School District (District).

The letter of intent from Internal Audit was addressed and sent to the Risk Management Department (RM). A copy of the letter was also sent to District Legal Counsel, and to the Superintendent and staff. The manager of the RM responded by stating duties related to the District's BCP/DRP have not been assigned to the Risk Management Department.

Most audits are risk based. This is defined by the Institute of Internal Auditors (IIA) as "…a methodology that links internal auditing to an organization's overall risk management framework. It allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite meaning they assess the likelihood of response to risk and its impact."[1]

The intended purpose of the audit was to evaluate the District's DRP/BCP for overall effectiveness and efficiencies, its internal controls, accuracy of performance tests, third-party contracts, and compliance with organizational policies, procedures, laws, regulations, and set guidelines.

The audit scope was listed as August 1, 2020, through August 1, 2021.

The internal audit objectives were to determine:

- The District's BCP/DRP processes and their reliability,
- The efficiency of their written processes,
- The response times to stabilize and restore essential District operations after a disaster.
- The District's overall coordination of standard operating procedures for key departments.
- Effectiveness of the managing department's testing documents during simulated testing.
- Compliance of the BCP/DRP procedures with the District's existing policies.

This audit was completed by reviewing the information provided by RM, randomly selected departments, and research on governing BCP and DRP regulations for schools.

RM provided a basic DRP Manual from the Technology Services (TS) department. The TS DRP Manual is specific to the TS department and is not a DRP for the District or any of its other departments. There are no written BCPs or DRPs for the District or any other District departments.

The District is a member of The School Risk Retention Trust, Inc. (the Trust). The Trust manages a pool of funds from participating districts, classified as members, to cover losses. Managing risk and mitigating losses is key to reducing potential claims and payouts by the Trust.

Excluded from this audit were activities unrelated to District BCPs and DRPs.

Observations:

1. No written BCP for the department.
2. No written DRP for the department.

OVERVIEW

BACKGROUND

The Tucson Unified School District (District) mission is "…in partnership with parents and the greater community, is to assure each pre-K through 12th grade student receives an engaging, rigorous and comprehensive education. The District is committed to inclusion and non-discrimination in all District activities. At all times, District staff should work to ensure that staff, parents, students, and members of the public are included and welcome to participate in District activities."[2]

The District is a member of The Arizona School Risk Retention Trust, Inc. (the Trust); which was established in 1986 under A.R.S. § 11-952.01(A). The Trust is a non-profit corporation that operates a risk retention pool funded and governed by its members. The Trust provides Arizona public school districts and community colleges with property and liability coverages and related services. It services 247 districts and community colleges, making it one of the largest public entity pools in the United States. Being a member of the Trust provides numerous benefits and added stewardship responsibilities.

The letter of intent was addressed to the Risk Management department (RM); it included a list of preliminary items to be provided prior to the audit. In response to the letter, RM sent the requested preliminary paperwork, and included a Disaster Recovery Plan (DRP) Manual from Technology Services (TS).

The TS DRP Manual is specific to the TS department and is not a DRP for the District or any of its other departments. There are no written BCPs or DRPs for the District or any other District departments.

To clarify, the intent of this audit was to review the BCP/DRP for the entire District; it was not to be specific to the TS department.

During the walk-through meeting, the RM manager stated that the RM department was not responsible to oversee these plans; nor knew who might be. The RM manager speculated that maybe School Safety and Security, or perhaps Technology Services, or Operations.

School Safety and Security was contacted to inquire about a BCP or DRP. The Emergency Management Supervisor for School Safety and Security stated they were not aware of the District having a BCP/DRP. The specified purpose of this department is to manage the school's Emergency Response Plan (ERP), and ensure that every school in the District has one. Internal Audit was provided a copy of the ERP. Internal Audit complements the Emergency Management Supervisor and team for creating a well-organized and comprehensive manual.

According to industry standards, Risk Management departments are commonly responsible to oversee BCPs and DRPs of business operations for their departments and their organizations. As stated by School Business Affairs, "Some school districts are fortunate to have professional risk managers on staff who can identify and control the many risks that are unique to school systems….Whether certified or not, school risk managers are responsible for a wide range of issues, including property and casualty insurance; benefits, such as health care, workers' compensation, and unemployment; facility and environmental safety; crisis management; and the personnel training associated with these programs….To be effective, the school risk manager must have the support of the administration and a well-thought-out risk management team."[3]

Industry wide, there are several titles to describe BCPs and DRPs. Examples of the titles used are: Crisis Management, Risk Response, Recovery Mitigation, Management of Continuity, Business Recovery Management, Business Continuity and Recovery of Systems, and Continuity of Operations Planning. These titles are all synonymous. Regardless of the title used, the same standards and regulations apply.

A BCP and a DRP are considered separate but codependent plans. The National Institute of Standards and Technology (NIST) of the U.S. Department of Commerce, defines:

> BCP: "A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations." [4]
>
> DRP: "Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days." [5]

Simply stated, BCPs and DRPs are tools to assist organizations and departments of any size to get through and recover from an unexpected incident. The graph below illustrates an example of overlapping functions and a timeline of a crisis.

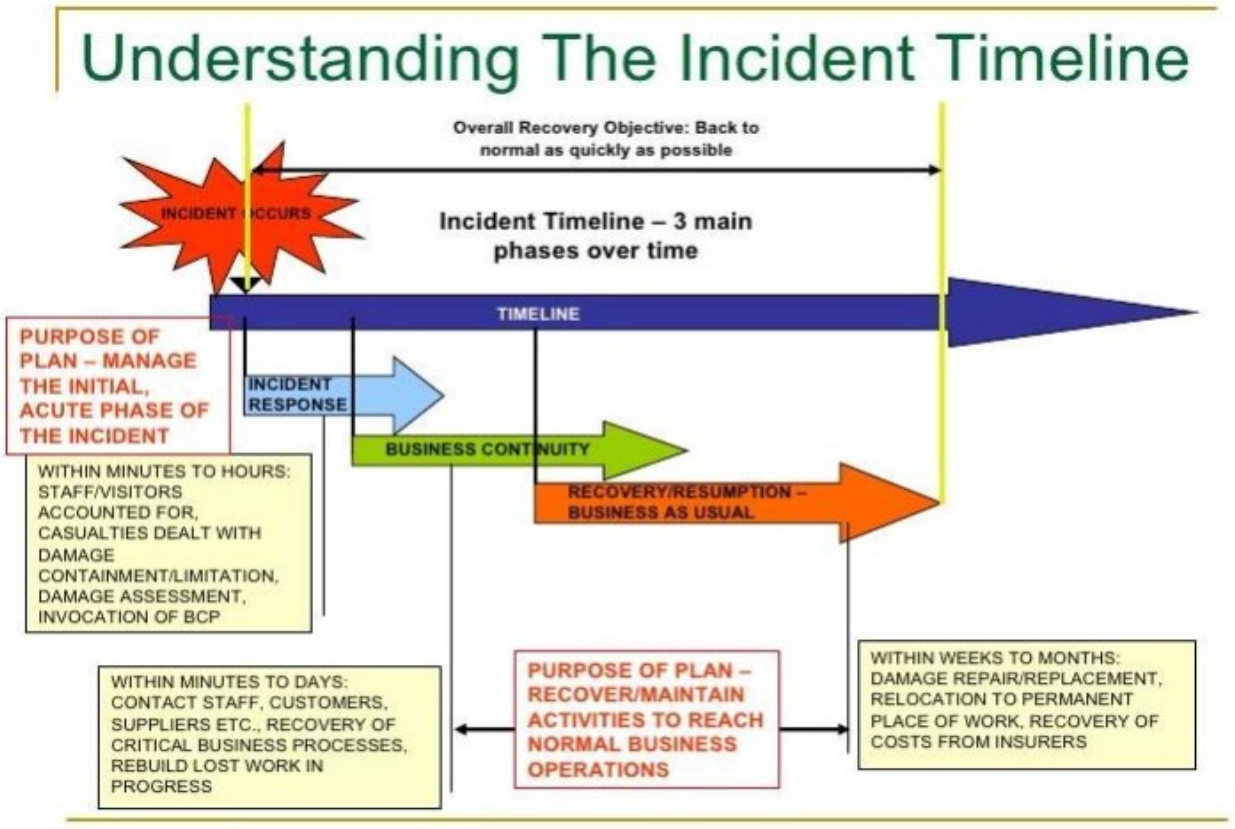


IMAGE OBTAINED FROM THE RESEARCH GATE, CRATED BY DIPANKAR GOSH [6]

The Arizona Auditor General's illustration of the BCP process below

IMAGE FROM THE ARIZONA AUDITOR GENERAL'S RISK AND BUSINESS CONTINGENCY PLANNING [7]

BCPs/DRPs are commonly work-in-progress documents; this is to permit adjustments for future changes and needs in the district's culture, community, and/or its evolving environment.

The state of Arizona is not completely immune to unpredictable hazards which occur in different forms and categories, and which could disrupt business operations, such as:

- Geological – earthquakes, fissures, etc.
- Meteorological – tornadoes, windstorms, lightning, etc.
- Health – quarantines, pandemics, etc.
- Others – fires, floods, snow days, etc.
- Man-made – labor strikes, walkouts, cyberattacks, etc.

As stated by the University of Arizona College of Science, included in the Arizona Geological Survey: "Natural hazards abound in Arizona. At the top of the list: flash floods, severe weather, landslides and debris flows, earthquakes, and earth fissures. Other hazards include: problem soils - a multi-billion dollar problem annually in the U.S.; volcanism - Arizona has three active volcanic fields and thousands of extinct volcanoes, some of which are prone to collapse; locally, radon and arsenic can threaten health and human life. Across America, floods, landslides and severe weather cost billions of dollars annually and result in scores of deaths and thousands of injuries… Hazard preparedness at the family-, business-, and community-level is critical to building a resilient community capable of mitigating the worst of natural hazards events."[8]

The reactivated fissure immediately north of W. Houston Rd. in July 2017, was approximately 0.75 miles in length AZG Library

Flash Flood on the Santa Cruz River 2006. AZG Library

Thunderstorm Over West Tucson
Picture by John Hunnicut

The City of Tucson, where the majority of the District's infrastructure is located, might be one of the cities with the lowest risk and likelihood of facing a natural disaster. Prior to the current pandemic, the last time the District experienced an unpredictable event was the teachers' strike of 2018. Disasters of any type are primarily unforeseeable and unpredictable.
The following three excerpts are from the Education Facilities Sector-Specific Plan, which was prepared by the Department of Homeland Security and the Department of Education.

- "DHS defines a Risk Mitigation Activity (RMA) as a program, tool, or initiative that directly or indirectly reduces risk in the sector, including providing for the sector's resilience. RMAs for EFS were identified as being the most important activity for mitigating risk in the subsector and increasing its resilience."
- "To allow for the unique characteristics of the subsector and its vulnerabilities in respect to a wide range of manmade incidents and natural disasters, EFS has identified all-hazards, comprehensive emergency management plans as the most important risk mitigation activity that can support school and higher education infrastructure protection and resilience."
- "That all schools and universities are prepared to mitigate/prevent, respond to, and recover from all hazards, natural or man-made by having a comprehensive, all-hazards plan based on the key principles of emergency management to enhance school safety, to minimize disruption, and to ensure continuity of the learning environment."[9]

It is inconceivable to expect any organization, regardless of size or location, to be able to predict all potential disasters. However, not having a BCP and a DRP will impede the District's ability to get through and recover from a disaster. Record Nation said it best; "Hope for the Best, Plan for the Worst."

Image captured from Dynamic Quest 2021; Quote from Record Nation, 2021[10]

STATEMENT OF AUDITING STANDARDS

This audit was conducted following the Institute of Internal Auditors (IIA) as the authoritative guidance for Internal Audits.

In accordance with the IIA, "Implementation Standard 2310, the reliability of the audit information depends on the use of appropriate engagement techniques. Some techniques take longer or require more resources than others, but may be worth the investment because they enable a higher level of assurance. In general, simple manual audit procedures include: • Inspecting physical evidence, such as the physical property of the area under review. • Examining documentation from either the audit client or outside sources. Gathering testimonial evidence through interviews, surveys, or risk and control self-assessments. • Conducting a walk-through to observe a process in action. • Examining data that is continuously monitored via technology." [11]

AUDIT SCOPE, METHODOLOGY, AND EXCLUSIONS

The internal audit scope was intended to be August 1, 2020 through August 1, 2021.

The methodology involved researching governing standards, guidelines, and common BCP/DRP practices. In addition, it included reviewing documents provided by RM, conducting meetings with a Trust membership representative, walkthroughs, and brief surveys with District departments.

The following organizations were researched for this audit: Arizona Auditor General (AZ Auditor), International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Federal Emergency Management Agency (FEMA), Department of Emergency and Military Affairs (DEMA), Homeland Security, U.S. Government Accountability Office (GAO), and U.S. Department of Education (DOE).

Per IIA Standard 2210.A3 – "Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board. Interpretation: Type of criteria may include • Internal (e.g., policies and procedures of the organization). • External (e.g., laws and regulations imposed by statutory bodies). • Leading practices (e.g., industry and professional guidance)."[12]

The criteria for this audit was obtained from organizational standards, governing guidelines and procedures.

Excluded from this report were activities and processes not related to BCP/DRP requirements.

AUDIT PURPOSE AND OBJECTIVES

The purpose of the audit was to evaluate the District's DRP/BCP for overall effectiveness and efficiencies, its internal controls, accuracy of performance tests, third party contracts, and compliance with organizational policies, procedures, laws, regulations, and set guidelines.

OBJECTIVES

The objectives of the audit were to determine:

- The District's DRP and BCP processes and their reliability.
- The efficiency of their written processes.
- The response times to stabilize and restore essential District operations after a disaster.
- The District's overall coordination of standard operating procedures for key departments.
- Effectiveness of the managing department's testing documents during simulated testing.
- Compliance of the DRP and BCP procedures with the District's (District) existing policies.

This audit was completed by reviewing the information provided by RM, randomly selected departments, and research on governing BCP and DRP regulations for schools.

As stated by Ms. Spellings, Secretary of the U.S. Department of Education, "Knowing how to respond quickly and efficiently in a crisis is critical to ensuring the safety of our schools and students. The midst of a crisis is not the time to start figuring out who ought to do what. At that moment, everyone involved – from top to bottom – should know the drill and know each other."[13]

Audit observations and recommendations are listed below.

AUDIT OBSERVATIONS AND RECOMMENDATIONS

- **NO WRITTEN BCPs EXIST FOR THE DISTRICT OR ITS DEPARTMENTS.**

  Condition: The District and its departments do not have written BCPs.

  Criteria: The IIA, Standard 2120.A1, reads "The internal audit activity must evaluate risk exposure relating to the organization's governance, operations, and information systems regarding the:

  Achievement of the organization's strategic objectives.

  Reliability and integrity of financial and operational information.

  Effectiveness and efficiency of operations and programs.

  Safeguarding of assets.

  Compliance with laws, regulations, policies, procedures, and contracts." [14]

  According to the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO) 24762:2008, "…business continuity management is an integral part of any holistic risk management process and involves:

  - Identifying potential threats that may cause adverse impacts on an organization's business operations, and associated risks.
  - Providing a framework for building resilience for business operations.
  - Providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures."[15]

Additionally, the Arizona Auditor General lists several reasons why "a Contingency Plan is important:

- They reduce risk and service unavailability.
- Minimize impact and service restoration.
- Permits the continuity of business.
- Prevents worsening the situation.
- Written to fit the size, needs, and culture of the District and its key departments."[16]

IMAGE FROM THE AUDIT GENERAL RISK AND BUSINESS CONTINGENCY PLANNING [17]

Lastly, the International Organization for Standardization (ISO) 22301.01 states, "The outcomes of maintaining a Business Continuity Management System (BCMS) are shaped by the organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties. (Figure 1)"[18]

Effect: Without a written BCP, valuable time will be lost getting through and recovering from a disaster or unexpected crisis.

Unprepared individuals and departments will negatively affect the success and outcome of reestablishing functions during and after a disaster.

Recommendation:

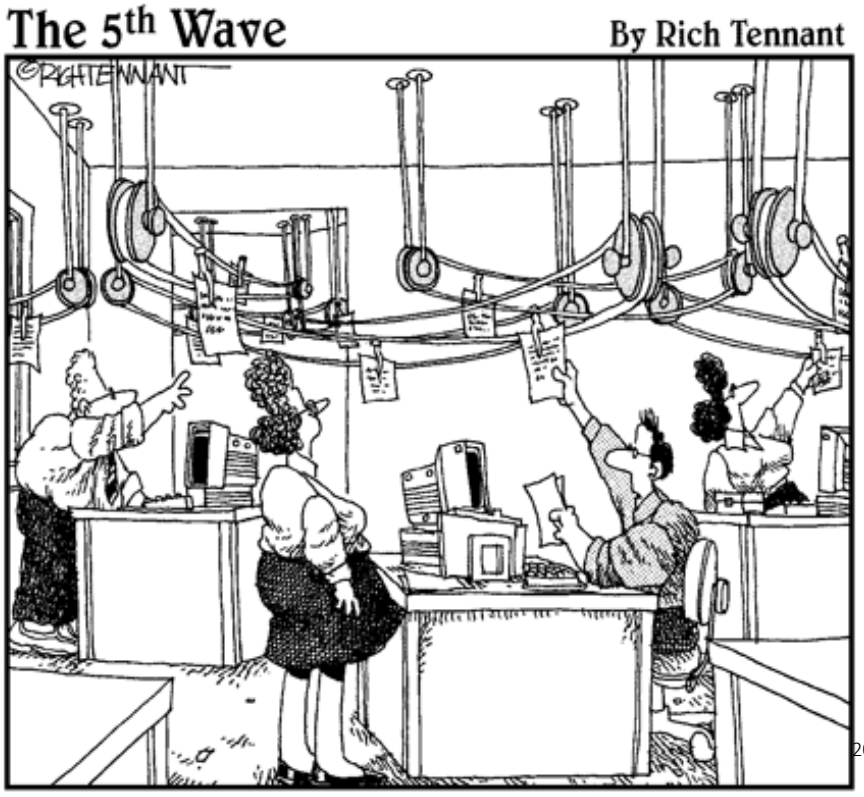
a. Discussing BCPs with upper management; BCPs are only effective when all levels of management understand the purpose and provide support.
    i. Developing BCPs for the District and departments that include:
        1. Roles and responsibilities
        2. Scope
        3. Resource requirements
        4. Training requirements
        5. Testing schedules
        6. Plan maintenance schedule
        7. Backup requirements

IMAGE IS FROM THE AUDITOR GENERAL RISK AND BUSINESS CONTINGENCY PLANNING [19]

ii. Ensuring staff member(s) are appointed to perform specific tasks in the BCP.

iii. Regularly test the efficiency and effectiveness of the BCPs.

b. Ensure the BCP complies with all applicable standards and regulations.



"It's all part of the business continuity plan if e-mail goes down." [20]

2. NO WRITTEN DRP FOR THE DISTRICT OR MOST OF ITS DEPARTMENTS.

Condition: The District, and most of its departments, do not have written DRPs.

Criteria: Arizona Auditor General (AZ Auditor) states, "The items necessary for each plan may vary by entity, but some basic DRP components include the following:

- Identification of critical equipment, data, and resources…allow for emergency data processing.
- Contact list of key individuals including their roles and responsibilities.
- Procedures for regularly backing up systems and data, and regularly testing backups.
- Procedures for activating the DRP, notifying appropriate parties, and assessing the severity of the disruption and the required response.
- Steps and procedures for restoring systems to full functionality.
- Supporting information as necessary to ensure a comprehensive plan such as business impact analysis, vendor contract information, etc."[21]

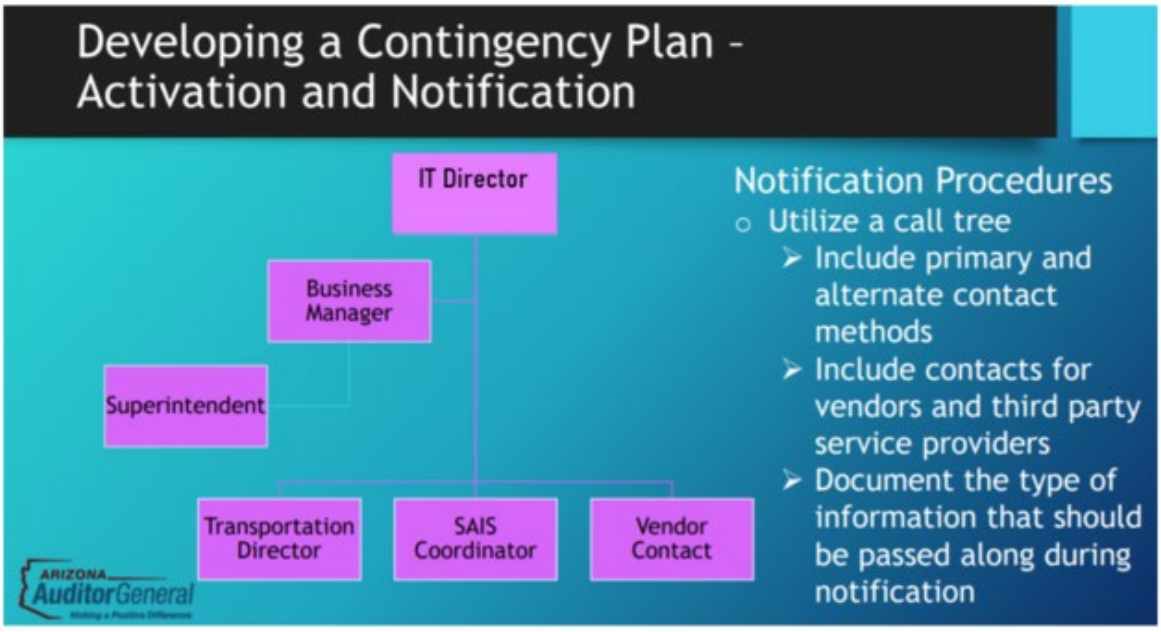


IMAGE IS FROM THE AUDITOR GENERAL RISK AND BUSINESS CONTINGENCY PLANNING [22]

The U.S. Department of Education states, "Every school needs a crisis plan that is tailored to its unique characteristics. Within a school district, however, it is necessary for all plans to have certain commonalities." [23]

Risk Evaluation and Mitigation Strategy (REMS), reads "Recovery in schools and school districts comprises four components:

1. Academics recovery. Learning is the primary purpose of schools, and the ability to resume academic activities is essential to a school's recovery…
2. Physical and structural recovery. This type of recovery is needed to support education and involves the restoration of the school's buildings, equipment, and supplies…

3. Business functions recovery. The school's or school district's business operations that also serve as a support function to education, such as payroll and contracts, need to be fully restored if impacted by an emergency...
4. Social, emotional, and behavioral recovery. Even though academics, physical and structural, and business functions recovery may have ended, the social, emotional, and behavioral recovery of students, teachers, and staff may continue long after." [23]

Image from Readiness and Emergency Management for Schools (REMS). 24

Effect: Not having a DRP for the District or its departments could result in chaos during an already bewildering situation. The lack of planning could result in the waste of valuable time and resources while deciding where to start; who will be appointed to lead a situation, what responsibilities to assign, how to coordinate processes…etc., all being done in the midst of a disaster.

U.S. Department of Education: *Practical Information on Crisis Planning Guide* – a guide for schools and communities – states, "A crisis is the time to follow the crisis plan, not to make a plan from scratch."[25]

The GAO states, "The range of issues school communities face when recovering from natural disasters provides a sense of what schools across the nation are trying to manage as they re-start school operations during the COVID-19 pandemic. This includes academic, structural, financial, and emotional considerations that can affect both students and staff (see fig. 1)." [26]

Figure 1: Characteristics of School Recovery from a Natural Disaster or Emergency

Source: GAO analysis of Readiness and Emergency Management for Schools (REMS) Technical Assistance Center Recovery Fact Sheet . | GAO-21-82R

Recommendations:

a. Discussing DRPs with upper management; DRPs are only effective when all levels of management understand the purpose and provide support.
b. Developing DRPs for the District and departments that include:
    i. Ensuring staff member(s) are appointed to perform specific tasks in the DRP.
    ii. Regularly test the efficiency and effectiveness of the DRPs.
    iii. Adjust the plan as needed based on needs and lessons learned.
c. Ensure the DRP complies with all applicable standards and regulations.

CONCLUSION

This audit was based on general research of business continuity and disaster recovering plans, testing, and methodologies were designed to detect areas of needed improvement; documents provided were reviewed and analyzed to determine their relativity to the objectives.

Risk-based audits are to determine if set controls are within the organization's acceptable risk limits, and if they support the organization's goals.

According to School Business Affairs, "Now more than ever, schools need to turn to risk management practices to generate short-and long- range planning for losses that affect the schools' budgets." [27]

Audit findings were reviewed with RM to facilitate exchange of opinions and to assist with management's questions, explanations and/or suggestions.

Provided recommendations are based on research, best practices, and applicable standards. The U.S. Department of Education, Practical Information on Crisis Planning, reads "The time to plan is now. If you do not have a crisis plan in place, develop one. If you do have a plan in place, review, update and practice that plan regularly."[28]

A follow up on this audit may be performed approximately six months from the date this final report is delivered to the Governing Board. The follow up will focus on the recommendations and Management Response and Commitments (MRC) that have been implemented, preventative measures that have been established, processes that are work in progress, and/or the analysis of accepted risk by senior management.

ACKNOWLEDGMENT

The Office of Internal Audit expresses its appreciation to the RM department, Legal Counsel, and the School Safety department for their assistance during this audit.

Report No. 001-FY 2021-2022; provided to Management, Superintendent and its staff on October 25, 2021.

Martha Smith 10/25/2021

Martha Smith — Date

Internal Auditor

Report Distributed to:

Superintendent and Management

Dr. Gabriel Trujillo, Superintendent for Tucson Unified School District
Mr. Robert Ross, General Counsel
Ms. Nicole Lowery, Manager of Risk Management.

Audit Committee Members

APPENDIX A

REFERENCES

1. **Institute of Internal Auditors (IIA)** – IIA defines risk-based internal auditing (RBIA) as a methodology that links internal auditing to an organization's overall risk management framework. RBIA allows internal audit to provide assurance to the board that risk management processes are managing risks effectively, in relation to the risk appetite.
   https://global.theiia.org/standards-guidance/topics/documents/201501guidetorbia.pdf

2. **Policy Code A: Foundation and Basic Commitments:** "The District's mission, in partnership with parents and the greater community, is to assure each pre-K through 12th grade student receives an engaging, rigorous and comprehensive education. The District is committed to inclusion and non-discrimination in all District activities." http://govboard.tusd1.org/Policies-and-Regulations/Policy-Code-A

3. **School Business Affairs:** "School districts are held accountable not only for the monies that contribute to the education system but also for mitigating any issues that threaten student learning. Some school districts are fortunate to have professional risk managers on staff who can identify and control the many risks that are unique to school systems. Most schools, however, place that responsibility on the shoulders of the school business manager or chief financial officer, who may not have the experience to identify and address those risks. Whether certified or not, school risk managers are responsible for a wide range of issues, including property and casualty insurance; benefits, such as health care, workers' compensation, and unemployment; facility and environmental safety; crisis management; and the personnel training associated with these programs. The Importance of Teamwork to be effective, the school risk manager must have the support of the administration and a well-thought-out risk management team." By Cheryl P. Johnson, ARM, and Steve Levering, CSRM, CTSBO. *Today's School Risk Manager*, June 2009 (p. 12). School Business Affairs. Retrieved from: https://files.eric.ed.gov/fulltext/EJ919336.pdf

4. **Business Continuity Plan (BCP):** "A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

5. **Disaster Recovery Plan (DRP):** "Management policy and procedures used to guide an enterprise response to a major loss of enterprise capability or damage to its facilities. The DRP is the second plan needed by the enterprise risk managers and is used when the enterprise must recover (at its original facilities) from a loss of capability over a period of hours or days." https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

6. **Understanding the Incident Timeline** –Graph-The Research Gate, by Dipankar Gosh, 2021. https://www.researchgate.net/figure

7. **Arizona Auditor General** - Contingency Planning Process –Image- From Auditor General –Risk and Business Contingency Planning. https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf

8. Natural Hazards in Arizona: Natural hazards abound in Arizona. At the top of list: flash floods, severe weather, landslides and debris flows, earthquakes, and earth fissures. Other hazards, include: problem soils - a multi-billion dollar problem annually in the U.S.; volcanism - Arizona has three active volcanic fields and thousands of extinct volcanoes, some of which are prone to collapse; locally, radon and arsenic can threaten health and human life.
Across America, floods, landslides and severe weather cost billions of dollars annually and result in scores of deaths and thousands of injuries. The best most efficacious way of managing natural hazards is to build a comprehensive historical, and whenever possible, prehistorical (e.g., trenching active faults to document thousands of years of activity), record of hazard events. Civil authorities, land managers, and the emergency management community can leverage that record to stage and deploy meaningful land management and emergency preparedness at the community level. Hazard preparedness at the family-, business-, and community-level is critical to building a resilient community capable of mitigating the worst of natural hazards events. Including the Fissure and Flash Flood pictures. https://azgs.arizona.edu/center-natural-hazards

9. Education Facilities Sector-Specific Plan An Annex to the Government Facilities Sector-Specific Plan https://files.eric.ed.gov/fulltext/ED541452.pdf

10. Disaster Recovery Picture: https://dynamicquest.com/the-difference-between-disaster-recovery-and-business-continuity/
Phrase, "Hope for the best, plan for the worst" came from https://www.recordnations.com/2018/08/what-is-disaster-recovery-plan-why-important/

11. Institute of Internal Auditors (IIA) – *Implementation Standard 2310*- In accordance with the IIA, Implementation Standard 2310, the reliability of the audit information depends on the use of appropriate engagement techniques. Some techniques take longer or require more resources than others, but may be worth the investment because they enable a higher level of assurance. In general, simple manual audit procedures include: • Inspecting physical evidence, such as the physical property of the area under review. • Examining documentation from either the audit client or outside sources. Gathering testimonial evidence through interviews, surveys, or risk and control self-assessments. • Conducting a walk-through to observe a process in action. • Examining data that is continuously monitored via technology." https://na.theiia.org/standards-guidance/Member%20Documents/IG2310-2016-12.pdf

12. IIA Standard 2210.A3 – "Adequate criteria are needed to evaluate governance, risk management, and controls. Internal auditors must ascertain the extent to which management and/or the board has established adequate criteria to determine whether objectives and goals have been accomplished. If adequate, internal auditors must use such criteria in their evaluation. If inadequate, internal auditors must identify appropriate evaluation criteria through discussion with management and/or the board. Interpretation: Type of criteria may include • Internal (e.g., policies and procedures of the organization). • External (e.g., laws and regulations imposed by statutory bodies). • Leading practices (e.g., industry and professional guidance)." https://na.theiia.org/standards-guidance/Member%20Documents/IG2310-2016-12.pdf

13. U.S. Department of Education - "Knowing how to respond quickly and efficiently in a crisis is critical to ensuring the safety of our schools and students. The midst of a crisis is not the time to start figuring out who ought to do what. At that moment, everyone involved –from top to bottom- should know the drill and know each other." Margaret Spellings, Secretary, Introduction 2007 (pg. 1-1). https://rems.ed.gov/docs/practicalinformationoncrisisplanning.pdf

14. IIA, Standard 2120.A1, reads "The internal audit activity must evaluate risk exposure relating to the organization's governance, operations, and information systems regarding the:
Achievement of the organization's strategic objectives.
Reliability and integrity of financial and operational information.
Effectiveness and efficiency of operations and programs.
Safeguarding of assets.
Compliance with laws, regulations, policies, procedures, and contracts." https://na.theiia.org/standards-guidance/Member%20Documents/IG2310-2016-12.pdf

15. International Electrotechnical Commission (IEC): "IEC and the International Organization for Standardization (ISO) 24762:2008, "business continuity management is an integral part of any holistic risk management process and involves:
    - Identifying potential threats that may cause adverse impacts on an organization's business operations, and associated risks.
    - Providing a framework for building resilience for business operations.
    - Providing capabilities, facilities, processes, action task lists, etc., for effective responses to disasters and failures." https://www.iec.ch/who-we-are

16. Arizona Auditor General, lists several reasons why Contingency Planning is important:
    - They reduce risk and service unavailability.
    - Minimize impact and service restoration.
    - Permits the continuity of business.
    - Prevents worsening the situation.
    - Written to fit the size, needs, and culture of the District and its key departments." https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf

17. Auditor General – One size fits all (Image). https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf

18. International Organization for Standardization (ISO) -22301.01-(2019) "The outcomes of maintaining a BCMS are shaped by the organization's legal, regulatory, organizational and industry requirements, products and services provided, processes employed, size and structure of the organization, and the requirements of its interested parties." https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

19. Auditor General – List of Items in a BCP - General Risk and Business Contingency Planning. https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf

20. The 5th Wave, by Rick Tennant, 2021. Cartoon. https://the5thwave.com

21. Auditor General – AZ Auditor states "The items necessary for each plan may vary by entity, but some basic DRP components include the following:

a. Identification of critical equipment, data, and resources, including off-site locations to store backup data and maintain redundant system resources to allow for emergency data processing.
b. Contact list of key individuals including their roles and responsibilities.
c. Procedures for regularly backing up systems and data, and regularly testing backups.
d. Procedures for activating the DRP, notifying appropriate parties, and assessing the severity of the disruption and the required response.
e. Steps and procedures for restoring systems to full functionality
f. Supporting information as necessary to ensure a comprehensive plan such as business impact analysis, vendor contract information, etc." https://www.azauditor.gov/reports-publications/school-districts/faqs/information-technology

22. Auditor General – Organizational chart of BCP –Image- General Risk and Business Contingency Planning. https://www.azauditor.gov/sites/default/files/Contingency%20Planning_2.pdf

23. Readiness and Emergency Management for Schools (REMS) - Four Components of Recovery U.S. Department of Education "Every school needs a crisis plan that is tailored to its unique characteristics. Within a school district, however, it is necessary for all plans to have certain commonalities in schools and school districts comprises four components: Audit General Risk and Business Academics recovery. Learning is the primary purpose of schools, and the ability to resume academic activities is essential to a school's recovery. The resumption of teaching and learning begins to restore normalcy to the school environment through routines, which can be very important in the psychological and emotional health of students, teachers, and staff. 2. Physical and structural recovery. This type of recovery is needed to support education and involves the restoration of the school's buildings, equipment, and supplies. 3. Business functions recovery. The school's or school district's business operations that also serve as a support function to education, such as payroll and contracts, need to be fully restored if impacted by an emergency. 4. Social, emotional, and behavioral recovery. Even though academics, physical and structural, and business functions recovery may have ended, the social, emotional, and behavioral recovery of students, teachers, and staff may continue long after." https://rems.ed.gov/Docs/Recovery_Fact_Sheet_508C.pdf

24. REMS -Contingency Planning –Once size fits all (Figure). https://rems.ed.gov/Docs/Recovery_Fact_Sheet_508C.pdf

25. U.S. Department of Education – *Practical Information o Crisis Planning – A Guide for Schools and Communities- Response* section (page 36), 4-1 "A crisis is the time to follow the crisis plan, not to make a plan from scratch." https://rems.ed.gov/docs/practicalinformationoncrisisplanning.pdf

26. Government Accountability Office (GAO). "The range of issues school communities face when recovering from natural disasters provides a sense of what schools across the nation are trying to manage as they re-start school operations during the COVID-19 pandemic. This includes academic, structural, financial, and emotional considerations that can affect both students and staff (see fig. 1)." GAO-21-62R Disaster Recovery K-12 Schools (October 14, 2020) –Pg. 2. https://www.gao.gov/assets/gao-21-62r.pdf

27. School Business Affairs, "Now more than ever, schools need to turn to risk management practices to generate short-and long- range planning for losses that affect the school budgets." https://files.eric.ed.gov/fulltext/EJ919336.pdf

28. The U.S. Department of Education, Practical Information on Crisis Planning, -"The time to plan is now. If you do not have a crisis plan in place, develop one. If you do have a plan in place, review, update and practice that plan regularly."
https://www2.ed.gov/admins/lead/safety/crisisplanning.html

APPENDIX B

GLOSSARY

American Institute of Certified Public Accountants (IACPA): "Is the national professional organization of Certified Public Accountants in the United States, with more than 418,000 members in 143 countries in business and industry, public practice, government, education, student affiliates and international associates." https://www.aicpa.org/

Arizona Auditor General (AZ Auditor) - The Arizona Auditor General serves as an independent source of impartial information concerning State and local governmental entities and provides specific recommendations to improve the operations of those entities" https://www.azauditor.gov/office-overview.

Arizona Regulation Statute §11-952.01(A) Intergovernmental agreements and contracts.

A. If authorized by their legislative or other governing bodies, two or more public agencies or public procurement units by direct contract or agreement may contract for services or jointly exercise any powers common to the contracting parties and may enter into agreements with one another for joint or cooperative action or may form a separate legal entity, including a nonprofit corporation, to contract for or perform some or all of the services specified in the contract or agreement or exercise those powers jointly held by the contracting parties.

https://www.azleg.gov/ars/11/00952-01.htm

Arizona Strategic Enterprise Technology (ASET) - In alignment with the strategic missions of state agencies, ADOA-ASET develops and executes the statewide information technology strategy, as well as provides capabilities, services and infrastructure to ensure the continuity of mission critical and essential systems for the State of Arizona" https://aset.az.gov/about

Best Practice - "A procedure that has been shown by research and experience to produce optimal results and that is established or proposed as a standard suitable for widespread adoption." Defined by Merriam Webster

Continuity of Operations Plan (COOP) - A predetermined set of instructions or procedures that describe how an organization's mission-essential functions will be sustained within 12 hours and for up to 30 days as a result of a disaster event before returning to normal operations.
https://csrc.nist.gov/glossary/term/continuity_of_operations_plan

Contract - Defined by Arizona state legislature: "means all types of state agreements, regardless of what they may be called, for the procurement of materials, services, construction, construction services or the disposal of materials."
https://www.azleg.gov/viewdocument/?docName=https://www.azleg.gov/ars/41/02503.htm

Control - The Institute of Internal Auditors (IIA) defines control as any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goal will be achieved. https://csrc.nist.gov/glossary/term/continuity_of_operations_plan

Department of Emergency and Military Affairs (DEMA): is the state agency that works with local jurisdictions after a disaster has hit. https://dema.az.gov/node/547

Disaster Recovery Plan – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

https://csrc.nist.gov/glossary/term/disaster_recovery_plan

Federal Emergency Management Agency (FEMA): The assistance from FEMA will strengthen these recovery efforts and help local communities get back on they're feet."
This Major Disaster Declaration provides public assistance and hazard mitigation for local recovery efforts. It also provides additional funding for eligible emergency response costs, emergency protective measures, debris removal, and the repair or replacement of damaged public infrastructure in the affected counties. 9/14, 2021 https://azgovernor.gov/governor/news/2021/09/governor-duceys-request-federal-assistance-approved-fema

General Accepted Auditing Standards (GAAS): Are sets of standards against which the quality of audits are performed and may be judged. Several organizations have developed such sets of principles, which vary by territory. https://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00150.pdf

Generally Accepted Government Auditing Standards (GAGAS): Also known as the Yellow Book, are the guidelines for audits created by the Comptroller General and the audit agency of the United States Congress, the Government Accountability Office. https://www.gao.gov/yellowbook/overview

Industry Standard – "Is the average by which those in a particular field govern themselves. It is the ordinary manner of doing things in that field and can serve to establish different things in various legal settings." Defined by HG Legal Resources https://www.hg.org/legal-articles/what-is-the-relevance-of-industry-standards-under-the-law-36794

Information Systems Auditor and Control Association (ISACA) – "ISACA has served our professional community for more than 50 years. The association was incorporated as the EDP Auditors Association in 1969 by a small group of individuals who recognized a need for a centralized source of information and guidance in the new field of electronic data processing audit. Today, ISACA serves 145,000 professionals in 180 countries, who span several roles in assurance, governance, risk and information security." https://www.isaca.org/why-isaca/about-us

Internal Auditing – IIA's definition "Internal auditing is an independent, objective, assurance and consulting activity designed to add value and improve an organization's operations. At its simplest, internal audit involves identifying the risks that could keep an organization from achieving its goals, making sure the organization's leaders know about these risks, and proactively recommending improvements to help reduce the risks." Additionally, "Internal auditors are explorers, analysts, problem-solvers, reporters, and trusted advisors. They bring objectivity and a variety of skills and expertise to the organization." https://global.theiia.org/about/about-internal-auditing/pages/about-internal-auditing.aspx

Internal Control – "A plan of organization under which employees' duties are arranged, and records and procedures are designed, to make it possible to exercise effective control over processes. Internal control procedures which call for proper authorizations by designated officials for all actions performed that must be specified and followed." https://global.theiia.org

International Organization for Standardization (ISO) – "Organizations subordinate to federal agencies may use the term Senior Information Security Officer or Chief Information Security Officer to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers. https://csrc.nist.gov/glossary/term/isoNational Institute of Standards and Technology

International Electrotechnical Commission (IEC) – Founded in 19060, the IEC is the world's leading organization for the preparation and publication of international standards for all electrical electronic, electronica and related technologies. These are known collectively as "electrotechnology". https://www.iec.ch/who-we-are

International Organization for Standardization (ISO): "is a worldwide federation of national standards bodies (ISO member bodies).The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization."
https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en

ISO 22301 - Is applicable to all organizations, regardless of size, industry or nature of business. It is also relevant to certification and regulatory bodies as it enables them to assess an organization's ability to meet its legal or regulatory requirements. Based on ISO's High-Level Structure (HLS), it aligns with many other internationally recognized management system standards, such as ISO 9001 (quality management) and ISO 14001 (environmental management). As such, it is designed to be integrated into an organization's existing management processes. ISO 22301 is useful for business continuity and risk professionals, supply chain directors, audit managers and associates, developers of corporate social responsibility reports, regulatory bodies and anyone else involved or interested in business continuity. https://csrc.nist.gov/glossary/term/isoNational Institute of Standards and Technology

National Center for Education Statistics (NCES) – "Is the primary federal entity for collecting and analyzing data related to education in the U.S. and other nations. NCES is located within the U.S. Department of Education and the Institute of Education Sciences. NCES fulfills a Congressional mandate to collect, collate, analyze, and report complete statistics on the condition of American education; conduct and publish reports; and review and report on education activities internationally." https://nces.ed.gov/about/

The National Incident Management System (NIMS) is a comprehensive, nationwide, systematic approach to incident management for any situation regardless of cause, size, location, or complexity. NIMS is a set of standardized concepts and principles applicable to all threats, hazards, and events. Use of the system allows various organizations and jurisdictions to effectively work together during an incident to achieve common objectives. Governor's Executive Order 2007-23 designates NIMS as the basis for all incident management in Arizona. The goal of the NIMS program in Arizona is to enhance statewide NIMS implementation. The Planning Branch provides NIMS outreach, education, and technical assistance to organizations and jurisdictions statewide. https://dema.az.gov/emergency-management/preparedness/planning-branch

National Institute of Standards and Technology (NIST) – "The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time—a second-rate

measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany, and other economic rivals.

From the smart electric power grid and electronic health records to atomic clocks, advanced nanomaterials, and computer chips, innumerable products and services rely in some way on technology, measurement, and standards provided by the National Institute of Standards and Technology." www.nist.gov

Organizational Chart – "Organizational charts are the presentation of reporting relationships and employee roles in an enterprise. A well-structured organizational structure would help improve productivity, but a poor organizational structure can weak the organization."
https://www.orgcharting.com/poor-organizational-structure/

Ready – "Launched in February 2003, Ready is a national public service campaign designed to educate and empower the American people to prepare for, respond to and mitigate emergencies, including natural and man-made disasters." https://www.ready.gov

The Institute of Internal Auditors (IIA) – "Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator."
https://na.theiia.org/standards-guidance/Member%20Documents/PG-Business-Continuity-Management.pdf

U.S. Department of Education (DOE) – "Is the agency of the federal government that establishes policy for, administers and coordinates most federal assistance to education. It assists the president in executing his education policies for the nation and in implementing laws enacted by Congress." https://www2.ed.gov

United States Government Accountability Office (GAO) – "GAO, often called the "congressional watchdog," is an independent, non-partisan agency that works for Congress. GAO examines how taxpayer dollars are spent and provides Congress and federal agencies with objective, non-partisan, fact-based information to help the government save money and work more efficiently." https://www.gao.gov/about

Document was received by Internal Auditor on 11/5/21 at 4:21 PM; was sent by Risk Manager, Ms. Lowery.

TUCSON UNIFIED
SCHOOL DISTRICT

RISK MANAGEMENT DEPARTMENT
1010 E. 10TH STREET TUCSON, AZ 85719
P.O. BOX 40400 TUCSON, AZ 85717
PHONE: (520) 225-6601 FACSIMILE: (520) 225-6631

To: **Martha Smith, Internal Auditor**

From: **Nicole Lowery, Risk Manager**

Date: **November 5, 2021**

RE: **Risk Management Internal Audit Report**

Risk Management has received the Internal Audit Report and reviewed the published findings.

As stated in the official Audit Report, Tucson Unified currently lacks published district wide protocols for a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP). I completely agree that formalized plans to address business interruption or a disaster, natural or otherwise, are ideal for every entity. Such plans are typically adopted by an agent of the organization with leadership authority within the agency to adopt district wide directives. Currently, no district policy or Risk Management job description delegates that level of authority.

A task presently in my scope is managing the district response to losses tied to property damage, general liability, personal injury (to students, staff, or visitors), as well as auto physical damage claims, theft, and excess liability. This department, along with the assistance of our insurer The Trust deploys staff, resources, remediation crews and other assistance in response to property and liability losses. While some of this response could fall within a disaster recovery plan or impact business continuity, the functions covered by my department are only a slice of a district wide response.

The scope and scale of a BCP and DRP could be extensive and require effort and coordination between all levels and layers within the district. Development of such plans could be handled by an authorized district authority or could be drafted with the help of a qualified vendor to assist in the creation of a school district specific plan. Last week, I was a participant in a national Public Risk Management Conference and while networking with other participants I did not find a single school district participating had either a BCP or DRP. A quick search of on-line resources or templates find municipal agencies and corporations have published plans, but school districts are far less common.

While business continuity and disaster recovery are not specifically published, TUSD is a school district leader within the State of Arizona when it comes to detailed site-specific Emergency Response Plans. These plans, managed by the School Safety Department, identify evacuation locations, emergency protocols, reunification information and address location-based protocols specific to each individual school site in TUSD. Within these Emergency Plans, response to such events as a flood, gas leak, school wide evacuation, lock down or other emergency are outlined step-by-step for each specific site. These

TUCSON UNIFIED
SCHOOL DISTRICT

RISK MANAGEMENT DEPARTMENT
1010 E. 10TH STREET TUCSON, AZ 85719
P.O. BOX 40400 TUCSON, AZ 85717
PHONE: (520) 225-6601 FACSIMILE: (520) 225-6631

plans include action required if a disaster rendered an entire campus out of service. There may certainly be some overlap between the existing emergency plans and the BCP and CRP.

In closing, I agree that the district would benefit from the adoption of BCP and DRP plans. I will await further communication from leadership on its expectations as to the role I or the Risk Management Department will play in this new process.