



District Audit Findings Follow-Up

Florida Association of Management Information Systems
2024 FAMIS Summer Conference

June 11 – 13, 2024



Introduction

Florida Statute 1010.30

- (1) School districts, Florida College System institutions, and other institutions and agencies under the supervision of the State Board of Education and state universities under the supervision of the Board of Governors are subject to the audit provisions of ss. 11.45 and 218.39.

- (2) If an audit contains a significant deficiency or material weakness, the district school board, the Florida College System institution board of trustees, or the university board of trustees shall conduct an audit overview during a public meeting. The audit overview shall describe the corrective action to be taken and a timeline for completion of such action.



FLORIDA DEPARTMENT OF
EDUCATION
fldoe.org

Audit Findings

The Office of Funding and Financial Reporting is responsible for reviewing reports on audits of the school districts and notifying appropriate internal departments of the need to follow up on area specific audit findings with the districts.

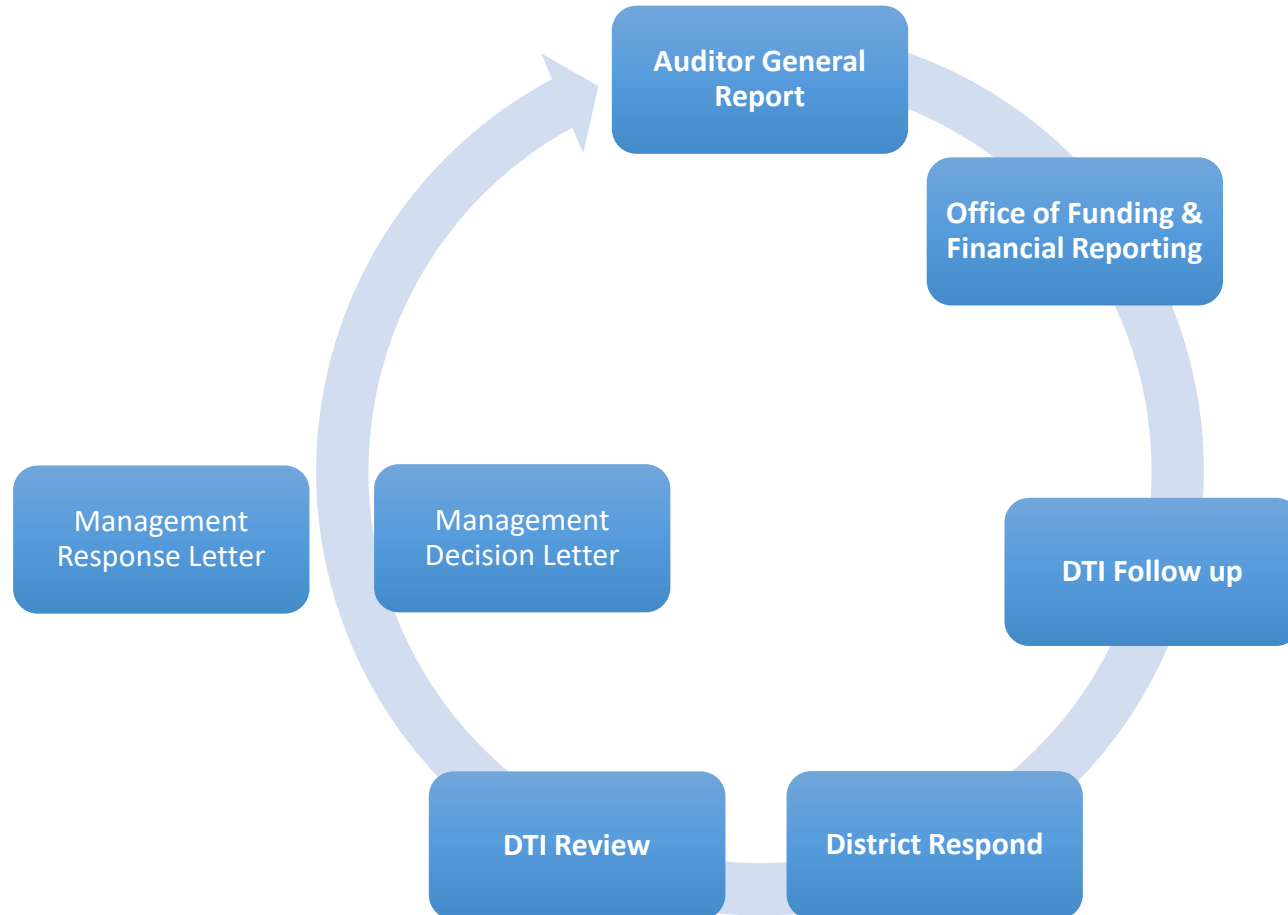


FLORIDA DEPARTMENT OF
EDUCATION
fldoe.org

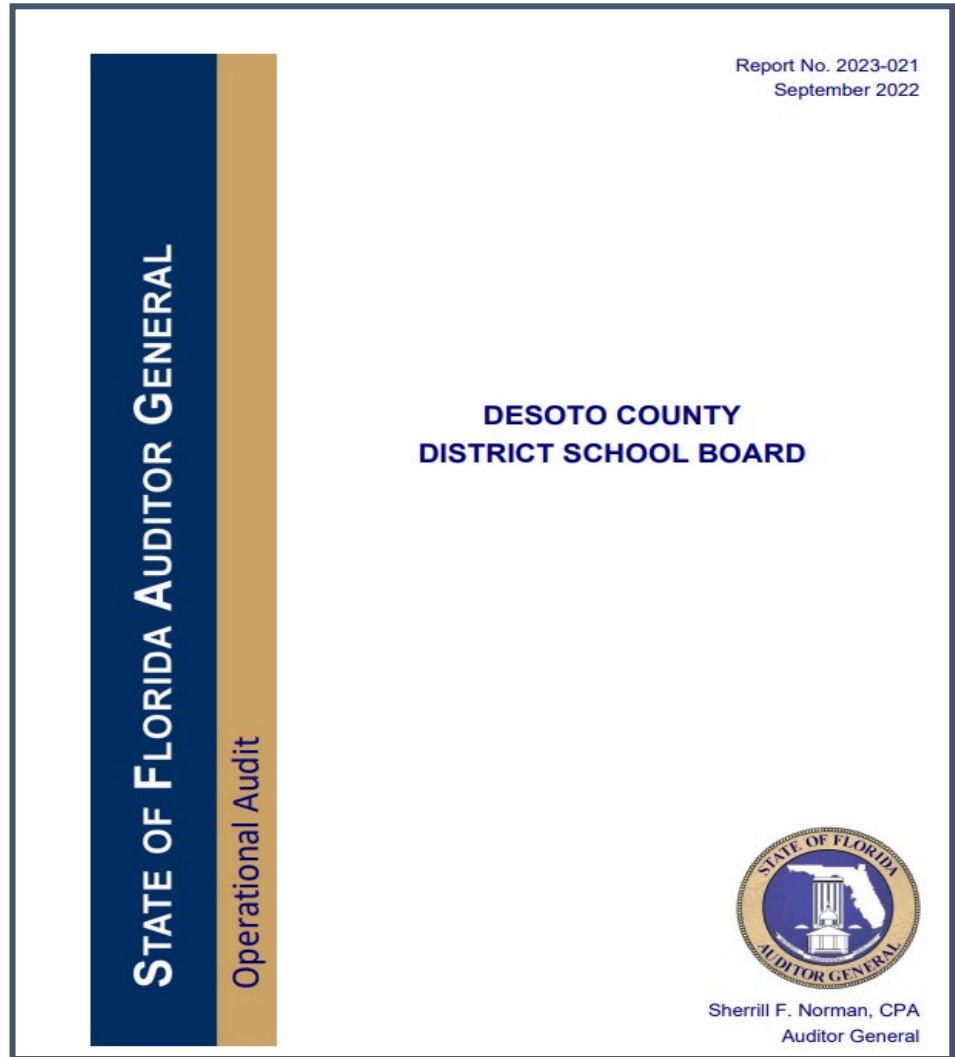
Responsibility

It is the responsibility of the Division of Technology and Innovation (DTI) to follow up with each school district for audit findings that are IT related.


Audit Follow-Up Process



Example Audit Report



Notification from the Office of Funding and Financial Reporting

 <p>FLORIDA DEPARTMENT OF EDUCATION fldoe.org</p> <p>Department of Education Manny Diaz, Jr., Commissioner</p>	<h2>OFFICE MEMORANDUM</h2> <p>FLORIDA DEPARTMENT OF EDUCATION Affirmative action/equal opportunity employer</p>		
To: Andre Smith, Vaneshia Plummer	Date: 12/13/2022	DTI Room	<u>Turlington</u> Name of Building
From: Mark Eggers	Phone: 245-9105	814 Room	<u>Turlington</u> Name of Building
Subject: <i>Follow-Up: Auditor General Report # 2023-01, [REDACTED] County District School Board</i>			
<p>The Office of Funding and Financial Reporting is responsible for reviewing reports of the Auditor General or other independent accountants on audits of school districts, and notifying appropriate Department of Education offices of the need to follow up on certain audit findings with the districts.</p> <p>The attached audit report indicates Finding(s) [REDACTED] relate to your program area. Department procedures require that the District be contacted to determine what action has been taken, or is planned, to correct the deficiencies, and to determine whether or not any questioned costs (if applicable) should be restored to the respective program.</p> <p>Please provide a copy of the management decision letter that satisfactorily concludes your office's follow up to the audit findings and proof of restoration of questioned costs (if applicable) to the Office of Funding and Financial Reporting as soon as possible. Although most findings may be resolved within 30 days, we do understand that follow up may take longer.</p> <p>This memorandum serves as an official notice and assignment of the audit findings to your program office. If you have any</p>			

District Audit Review and Follow-Up

DISTRICT AUDIT REVIEW AND FOLLOW-UP

District: County **Audit Report No.:** 20xx-0xx **Report Date:** Month ~~yyyy~~

Follow-up by Division of Technology and Innovation: mm/dd/~~yyyy~~

Follow-up With:

Follow-up Date:

Finding # 7

Information

Technology User Access

Privileges to the

Business Application

Recommendation: The District should continue efforts to ensure that access privileges are limited to those necessary for individuals to perform their assigned duties. Such efforts should include enhanced, documented, periodic evaluations of IT user access privileges to ensure those privileges restrict individuals from performing incompatible functions or functions outside their areas of responsibilities.

Example Audit Finding & Recommendation

Finding 7: Information Technology User Access Privileges – Sensitive Personal Information

Finding 7: Some unnecessary or incompatible information technology access privileges existed that increased the risk for unauthorized disclosure of sensitive personal information of students to occur. A similar finding was noted in report No. 2020

Recommendation: The District should continue efforts to ensure that only those employees who have a demonstrated need to access sensitive personal information, including student SSNs, have such access. In addition, the District should document periodic evaluations of individual access privileges and promptly remove any inappropriate or unnecessary access.



Response Section

The district will provide their response to the audit finding(s) in the Response Section of the template. A response showing what action plan, policies, or procedures have been implemented to address the finding(s) will be inserted.

Response Process

Once the findings are plugged into the template as displayed on the previous slide, a response is requested within 30 calendar days.

If a response is not received by the given date stated in the initial follow-up notice from DTI, another email will follow each month until the district responds and satisfies the areas noted.

Response must include the following:

- Satisfaction of all areas noted:
 - Action Plan
 - Policies and/or procedures implemented
 - Progress following the implementation
 - Copies of new or revised policies

Response Section

What action plans, policies or procedures have the district implemented to address the finding? What progress has been made since the audit? Please provide copies of any new or revised policies adopted to address this finding.

Response:

Common Questions

Common questions related to responses:

- **Q: Who should respond?**
- A: Superintendents
- **Q: Is it fine if the response is not on the template?**
- A: Yes, there are times where there is a need to send policies and/or procedures to support your response.

Common Questions (continued)

- **Q: How should I submit a response?**
- A: Input the information within the template provided, or let DTI know there is a need to send the response in a secured manner.

Review

- DTI will review the response.
- An acknowledgment of receipt will be sent via email to the district stating we will review the response and follow up with questions or a letter that will conclude the follow-up.

Request/Approve

- If the response is not adequate, a Request Letter is sent.
- If the district's response demonstrates that appropriate corrective measures were taken, a Management Decision Letter will be provided. This will conclude the follow-up.

Management Response – Additional Documentation and/or Clarification Required

Example Request Letter:

Date

District Name
District Address

RE: Auditor General Report Number __

Dear _____:

Thank you for responding to our request for the documentation relative to the finding(s) from the above-referenced Auditor General Report pertaining to Information Technology.

We have reviewed the documentation and believe this/these audit finding(s) has/have not been addressed.

Finding(s) will need additional documentation and/or clarification to fully provide the requested response to the Auditor General, please respond when this/these finding(s) has/have been addressed.

Management Decision Letter

Example

Date

District Name

District Address

RE: Auditor General Report Number ___

Dear _____:

Thank you for your response to our request for documentation relative to the finding from the above-referenced Auditor General Report pertaining to Information Technology.

We have reviewed the documentation related to Information Technology finding(s), Number ____, and believe that appropriate corrective measures have been taken to resolve this/these finding(s).

Please remember to update your IT policies or procedures based on your corrective measures, and no further action is required relative to this/these finding(s) as it/they has/have been appropriately addressed.



Notifying Office of Funding and Financial Reporting

Following the completion of an audit follow-up, DTI will send the generated Management Decision Letter to the school district and Office of Funding and Financial Reporting.

Common IT Findings

- Information Technology Disaster Recovery Plan
- Information Technology User Access Privileges
– Sensitive Personal Information
- Information Technology User Access Privileges
– Timely Deactivation
- Information Technology User Access Privileges

What is an IT Security Framework

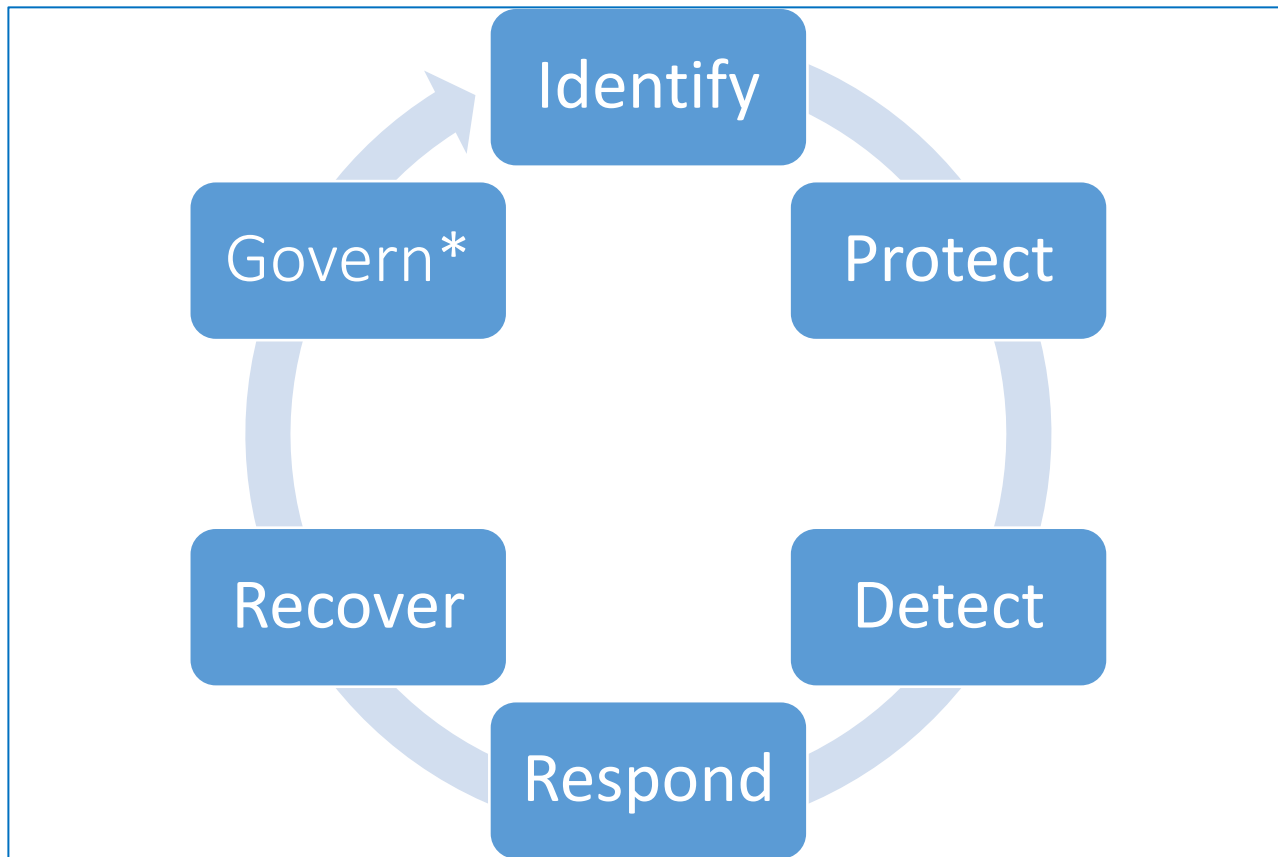
An IT security framework is a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls. These frameworks are a blueprint for managing risk and reducing vulnerabilities.

[Top 10 IT security frameworks and standards explained | TechTarget](#)

Security Framework Examples

- **ISO** – International Organization for Standardization
- **NIST** – National Institute of Standards and Technology
- **COBIT** – Control Objectives for Information Technologies
- **CIS Controls** – Center for Internet Security

State of Florida Cybersecurity Standards



Identify

- Asset Management
- Business Environment
- Governance
- Risk Assessment
- Risk Management Strategy
- Supply Chain Risk Management

Protect

- Identity Management, Authentication, & Access Controls
- Awareness and Training
- Data Security
- Information Protection, Processes, and Procedures
- Maintenance
- Protective Technology

Detect

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

Respond

- Communications
- Analysis
- Mitigation
- Improvements

Recovery

- Recovery Planning
- Improvements
- Communications

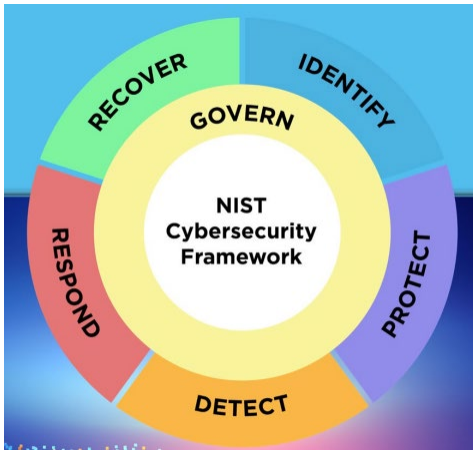
Govern*

- Organizational Context
- Risk Management Strategy
- Cybersecurity Supply Chain Risk Management
- Roles, Responsibilities and Authorities
- Policies, Processes, and Procedures
- Oversight
- Govern Agency Requirements

NIST 2.0

National Institute of Standards and Technology

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to manage cybersecurity risks.



CSF COMPONENTS

- CSF Core
- CSF Organizational Profiles
- CSF Tiers

CSF Core, Profiles, and Tiers are used to *understand, assess, prioritize, and communicate* cybersecurity risks.



FLORIDA DEPARTMENT OF
EDUCATION
fldoe.org

Questions?



www.FLDOE.org



www.FLDOE.org