COLLIN COLLEGE

Locations
Collin Higher Education Center
McKinney, Texas

Courtyard Center
Plano, Texas

Frisco Campus

McKinney Campus

Plano Campus

Public Safety Training Center
McKinney, Texas

Rockwall Center

Technical Campus
Allen, Texas

Wylie Campus

eCollin
www.collin.edu

District President
H. Neil Matkin, Ed.D.
3452 Spur 399
P.O. Box 8021
McKinney, Texas 75070
P | 972.758.3800
F | 972.758.3807
nmatkin@collin.edu
www.collin.edu

NOTICE is hereby given that the Collin County Community College District Board of Trustees will hold a meeting of the Finance and Audit Committee (Moses, Arias, and Menon) at 4:30 p.m. on Tuesday, August 18, 2020, in Board Conference Room 135 at the Collin Higher Education Center, 3452 Spur 399, McKinney, Texas 75069.

PUBLIC COMMENT

REVIEW AND DISCUSSION ITEMS

1. Review and Discussion of the Approval of the 2020-2021 Budget

2. Review and Discussion of the Approval of a Resolution Setting the 2020 Tax Rate

3. Review and Discussion of the Approval of a Resolution Designating the Collin County Tax Assessor/Collector as Officer to Calculate Tax Rate

4. Review and Discussion of the Appointment of Authorized Representatives to Engage in Investment Transactions with TexPool

5. Discussion of Internal Audit Results for the College

J. Robert Collins, Ph.D.
Chairman, Board of Trustees

Collin County Community College District Board of Trustees

1. Finance and Audit Committee — August 18, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Review and Discussion of the Approval of the 2020-2021 Budget

DISCUSSION: On July 28, 2020, the proposed budget for the 2020-2021 fiscal year was presented to the Finance and Audit Committee. The proposed budget was also presented to the Board of Trustees and the public on August 4, 2020 and scheduled to be presented again on August 18, 2020.

The proposed revenue budget for 2020-2021 is presented as follows:

Unrestricted	$227,787,131
Restricted	50,387,857
Interfund Transfers	61,487,241
Total	$339,662,229

The proposed expenditure budget for 2020-2021 is presented as follows:

Unrestricted	$223,118,369
Restricted	213,894,068
Interfund Transfers	61,487,241
Depreciation	16,630,452
Bond Principal	(12,880,000)
Capital Purchases	(139,761,417)
Total	$362,488,713

See Annual Budget – Fiscal Year Ending August 31, 2021

Collin County Community College District Board of Trustees

2020-08-3-X August 25, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Report Out of the Finance and Audit Committee and Consideration of Approval of the 2020-2021 Budget

DISCUSSION: On July 28, 2020, the proposed budget for the 2020-2021 fiscal year was presented to the Finance and Audit Committee. The proposed budget was also presented to the Board of Trustees and the public on August 4, 2020 and August 18, 2020.

The proposed revenue budget for 2020-2021 is presented as follows:

Unrestricted	$227,787,131
Restricted	50,387,857
Interfund Transfers	61,487,241
Total	$339,662,229

The proposed expenditure budget for 2020-2021 is presented as follows:

Unrestricted	$223,118,369
Restricted	213,894,068
Interfund Transfers	61,487,241
Depreciation	16,630,452
Bond Principal	(12,880,000)
Capital Purchases	(139,761,417)
Total	$362,488,713

See Annual Budget – Fiscal Year Ending August 31, 2021

DISTRICT PRESIDENT'S RECOMMENDATION: The District President recommends approval and adoption of the Fiscal Year 2020-2021 Budget.

SUGGESTED MOTION: This item comes as a motion and second out of committee. A suggested motion would be, "Mr. Chairman, I make a motion that the Board of Trustees of Collin County Community College District approves and adopts the Fiscal Year 2020-2021 Budget as presented."

Collin County Community College District Board of Trustees

2. Finance and Audit Committee — August 18, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Review and Discussion of the Approval of a Resolution Setting the 2020 Tax Rate

DISCUSSION: At its meeting on August 4, 2020, the Board of Trustees of Collin County Community College District voted on a proposed tax rate for 2020. Public hearings on the proposed tax rate was held on August 18, 2020. In addition, the Finance and Audit Committee reviewed and discussed the 2020 Tax Rate at its meeting on July 28, 2020.

The proposed total tax rate of $0.081222, is the same as the total rate approved in 2019.

The Maintenance & Operations portion of the total tax rate ($0.079100) will raise more taxes for Maintenance & Operations than last year's tax rate ($0.079100), and will raise more taxes for Debt Service ($0.002122) than last year's rate ($0.002122).

Resolution Setting 2020 Tax Rate
Collin County Community College District

WHEREAS, at its meeting of August 4, 2020, the Board of Trustees of Collin County Community College District voted on a proposed tax rate for 2020, and

WHEREAS, the Board of Trustees of Collin County Community College District held a public hearing on the proposed tax rate for 2020 on August 18, 2020,

NOW THEREFORE BE IT RESOLVED, at the recommendation of the District President, that the Board of Trustees of Collin County Community College District approves setting the tax rate for 2020 at $0.081222, which includes a Maintenance and Operations rate of $0.079100 and a Debt Service Rate of $0.002122.

Maintenance & Operations Tax Rate

THIS TAX RATE WILL RAISE MORE TAXES FOR MAINTENANCE & OPERATIONS THAN LAST YEAR'S TAX RATE. THE TAX RATE WILL EFFECTIVELY BE RAISED BY 3.36% AND WILL RAISE TAXES FOR MAINTENANCE & OPERATIONS ON A $100,000 HOME BY APPROXIMATELY $1.00.

_____ _____
President Secretary

Collin County Community College District Board of Trustees

2020-08-3-X August 25, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Report Out of the Finance and Audit Committee and Consideration of Approval of a Resolution Setting the 2020 Tax Rate

DISCUSSION: At its meeting on August 4, 2020, the Board of Trustees of Collin County Community College District voted on a proposed tax rate for 2020. Public hearings on the proposed tax rate was held on August 18, 2020. In addition, the Finance and Audit Committee reviewed and discussed the 2020 Tax Rate at its meetings on July 28, 2020 and August 18, 2020.

The proposed total tax rate of $0.081222 is the same as the total rate approved in 2019.

The Maintenance & Operations portion of the total tax rate ($0.079100) will raise more taxes for Maintenance & Operations than last year's tax rate ($0.079100), and will raise more taxes for Debt Service ($0.002122) than last year's rate ($0.002122).

DISTRICT PRESIDENT'S RECOMMENDATION: The District President recommends that the Board of Trustees of Collin County Community College District approves the Board of Trustees approval of the resolution setting the tax rate for 2020.

SUGGESTED MOTION: This item comes as a motion and second out of committee. A suggested motion would be, "Mr. Chairman, I make a motion that the Board of Trustees of Collin County Community College District approves the resolution stating that property taxes be increased by the adoption of a tax rate of $0.081222 which includes a Maintenance & Operation rate of $0.079100 and a Debt Service rate of $0.002122, which is effectively a 3.4 percent increase of the total proposed rate over the total effective tax rate."

Collin County Community College District Board of Trustees

3. Finance and Audit Committee August 18, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Review and Discussion of the Approval of a Resolution Designating the Collin County Tax Assessor/Collector as Officer to Calculate Tax Rate

DISCUSSION: The Texas Tax Code Section 26.04(c) defines that Collin County Community College may designate “an officer or employee” to calculate the annual no-new revenue tax rate and the voter-approval tax rate and to sign and submit the Truth in Taxation forms required to be completed by the College.

RESOLUTION OF THE COLLIN COUNTY COMMUNITY COLLEGE DISTRICT BOARD OF TRUSTEES DESIGNATING COLLIN COUNTY TAX ASSESSOR COLLECTOR AS OFFICER TO CALCULATE TAX RATE INFORMATION REQUIRED UNDER TEXAS TAX CODE SECTION 26.04(C)

The Board of Trustees of the Collin County Community College makes the following findings and resolutions:

WHEREAS, pursuant to Texas Tax Code Section 26.04(c), Collin County Community College ("College") may designate "an officer or employee" to "calculate the annual no-new-revenue tax rate and the voter-approval tax rate" for the College and to sign and submit the Truth in Taxation forms required to be completed by the College;

WHEREAS, the Collin County Tax Assessor Collector, is willing to perform such functions on behalf of the College.

NOW, THEREFORE, BE IT RESOLVED AND ORDERED THAT the Collin County Community College hereby designates the Collin County Tax Assessor Collector as the officer designated pursuant to Texas Tax Code Section 26.04(c) to calculate, sign and submit the Truth in Taxation forms as required by Texas Tax Code Chapter 26 and the Texas Comptroller. This delegation shall remain in effect until revoked by the Board of Trustees for Collin County Community College.

ADOPTED and EXECUTED this _____ day of August, 2020.

_____

Chair, Board of Trustees

ATTEST:

_____

Secretary, Board of Trustees

Collin County Community College District Board of Trustees

2020-08-3-X August 25, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Report out of the Finance and Audit Committee and Consideration of Approval of a Resolution Designating the Collin County Tax Assessor Collector as Officer to Calculate the Tax Rate

DISCUSSION: The Texas Tax Code Section 26.04(c) defines that Collin County Community College may designate "an officer or employee" to calculate the annual no-new revenue tax rate and the voter-approval tax rate and to sign and submit the Truth in Taxation forms required to be completed by the College.

DISTRICT PRESIDENT'S RECOMMENDATION: The District President recommends that the Board of Trustees of Collin County Community College District approves the resolution designating Collin County Tax Assessor Collector as the Officer to calculate the tax rate.

SUGGESTED MOTION: This item comes as a motion and second out of committee. A suggested motion would be, "Mr. Chairman, I make a motion that the Board of Trustees of Collin County Community College District approves the resolution designating the Collin County Tax Assessor Collector as Officer to calculate the tax rate."

Collin County Community College District Board of Trustees

4. Finance and Audit Committee August 18, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Review and Discussion of the Appointment of Authorized Representatives to Engage in Investment Transactions with TexPool

DISCUSSION: The Texas Local Government Investment Pools (the "TexPool Portfolios") have been organized in conformity with the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code, and the Public Funds Investment Act, Chapter 2256 of the Texas Government Code. These two acts provide for the creation of public funds investment pools and permit eligible governmental entities to jointly invest their funds in authorized investments.

Texpool requires governing body approval of representatives who are authorized to conduct business on behalf of the Board of Trustees. The authorized representatives change from time-to-time, which requires an amended notification.

The Finance and Audit Committee will be presented with suggested authorized representatives of Collin College, Melissa Irby, Julie Bradley, Barbara Johnston, Suzanne Armstrong, and Keitha Carlton, to engage in investment transactions with TexPool.

Resolution Amending Authorized Representatives

Please complete this form to amend or designate Authorized Representatives. *This document supersedes all prior Authorized Representative forms.*

*** Required Fields**

1. Resolution

WHEREAS,

Collin County Community College District — Participant Name*

7 7 2 7 5 — Location Number*

("**Participant**") is a local government of the State of Texas and is empowered to delegate to a public funds investment pool the authority to invest funds and to act as custodian of investments purchased with local investment funds; and

WHEREAS, it is in the best interest of the Participant to invest local funds in investments that provide for the preservation and safety of principal, liquidity, and yield consistent with the Public Funds Investment Act; and

WHEREAS, the Texas Local Government Investment Pool ("**TexPool / Texpool Prime**"), a public funds investment pool, were created on behalf of entities whose investment objective in order of priority are preservation and safety of principal, liquidity, and yield consistent with the Public Funds Investment Act.

NOW THEREFORE, be it resolved as follows:

A. That the individuals, whose signatures appear in this Resolution, are Authorized Representatives of the Participant and are each hereby authorized to transmit funds for investment in TexPool / TexPool Prime and are each further authorized to withdraw funds from time to time, to issue letters of instruction, and to take all other actions deemed necessary or appropriate for the investment of local funds.

B. That an Authorized Representative of the Participant may be deleted by a written instrument signed by two remaining Authorized Representatives provided that the deleted Authorized Representative (1) is assigned job duties that no longer require access to the Participant's TexPool / TexPool Prime account or (2) is no longer employed by the Participant; and

C. That the Participant may by Amending Resolution signed by the Participant add an Authorized Representative provided the additional Authorized Representative is an officer, employee, or agent of the Participant;

List the Authorized Representative(s) of the Participant. Any new individuals will be issued personal identification numbers to transact business with TexPool Participant Services.

1. Melissa Irby — Name; Chief Financial Officer — Title
   9 7 2 7 5 8 3 8 3 1 — Phone; 9 7 2 7 5 8 3 8 4 1 — Fax; mirby@collin.edu — Email
   Signature

2. Julie Bradley — Name; Associate VP — Title
   9 7 2 7 5 8 3 8 2 1 — Phone; 9 7 2 7 5 8 3 8 4 1 — Fax; jbradley@collin.edu — Email
   Signature

3. Barbara Johnston — Name; Associate VP — Title
   9 7 2 9 8 5 3 7 3 2 — Phone; 9 7 2 7 5 8 3 8 4 1 — Fax; bjohnston@collin.edu — Email
   Signature

Form Continues on Next Page

1. Resolution (continued)

4. Keitha Carlton — Director of Accounting
Name — Title

9 7 2 5 9 9 3 1 0 3 — 9 7 2 7 5 8 3 8 4 1 — kacarlton@collin.edu
Phone — Fax — Email

Keitha Carlton
Signature

List the name of the Authorized Representative listed above that will have primary responsibility for performing transactions and receiving confirmations and monthly statements under the Participation Agreement.

Suzanne Armstrong
Name

In addition and at the option of the Participant, one additional Authorized Representative can be designated to perform only inquiry of selected information. *This limited representative cannot perform transactions.* If the Participant desires to designate a representative with inquiry rights only, complete the following information.

Rikki Ramirez — Portfolio Analyst
Name — Title

5 1 2 3 2 0 5 0 4 2 — 5 1 2 3 2 0 5 0 4 1 — rikki@patterson.net
Phone — Fax — Email

D. That this Resolution and its authorization shall continue in full force and effect until amended or revoked by the Participant, and until TexPool Participant Services receives a copy of any such amendment or revocation. This Resolution is hereby introduced and adopted by the Participant at its regular/special meeting held on the 0 1 day of August, 2 0 2 0.

Note: Document is to be signed by your Board President, Mayor or County Judge and attested by your Board Secretary, City Secretary or County Clerk.

Name of Participant*

SIGNED

Signature*

H. Neil Matkin
Printed Name*

District President
Title*

ATTEST

Signature*

Kristy Horkman
Printed Name*

Secretary to Board of Trustees
Title*

2. Mailing Instructions

The completed Resolution Amending Authorized Representatives can be faxed to TexPool Participant Services at 1-866-839-3291, and mailed to:

TexPool Participant Services
1001 Texas Avenue, Suite 1150
Houston, TX 77002

Resolution Amending Authorized Representatives

Please complete this form to amend or designate Authorized Representatives. *This document supersedes all prior Authorized Representative forms.*

*** Required Fields**

1. Resolution

WHEREAS,

Collin County Community College District — Participant Name*

7 7 2 7 5 — Location Number*

("**Participant**") is a local government of the State of Texas and is empowered to delegate to a public funds investment pool the authority to invest funds and to act as custodian of investments purchased with local investment funds; and

WHEREAS, it is in the best interest of the Participant to invest local funds in investments that provide for the preservation and safety of principal, liquidity, and yield consistent with the Public Funds Investment Act; and

WHEREAS, the Texas Local Government Investment Pool ("**TexPool / Texpool Prime**"), a public funds investment pool, were created on behalf of entities whose investment objective in order of priority are preservation and safety of principal, liquidity, and yield consistent with the Public Funds Investment Act.

NOW THEREFORE, be it resolved as follows:

A. That the individuals, whose signatures appear in this Resolution, are Authorized Representatives of the Participant and are each hereby authorized to transmit funds for investment in TexPool / TexPool Prime and are each further authorized to withdraw funds from time to time, to issue letters of instruction, and to take all other actions deemed necessary or appropriate for the investment of local funds.

B. That an Authorized Representative of the Participant may be deleted by a written instrument signed by two remaining Authorized Representatives provided that the deleted Authorized Representative (1) is assigned job duties that no longer require access to the Participant's TexPool / TexPool Prime account or (2) is no longer employed by the Participant; and

C. That the Participant may by Amending Resolution signed by the Participant add an Authorized Representative provided the additional Authorized Representative is an officer, employee, or agent of the Participant;

List the Authorized Representative(s) of the Participant. Any new individuals will be issued personal identification numbers to transact business with TexPool Participant Services.

1. Suzanne Armstrong — Name; Accountant — Title

9 7 2 7 5 8 3 8 2 3 — Phone; 9 7 2 7 5 8 3 8 4 1 — Fax; sarmstrong@collin.edu — Email

Suzanne Armstrong — Signature

2. Name; Title

Phone; Fax; Email

Signature

3. Name; Title

Phone; Fax; Email

Signature

1. Resolution (continued)

4. Name | Title

Phone | Fax | Email

Signature

List the name of the Authorized Representative listed above that will have primary responsibility for performing transactions and receiving confirmations and monthly statements under the Participation Agreement.

Suzanne Armstrong
Name

In addition and at the option of the Participant, one additional Authorized Representative can be designated to perform only inquiry of selected information. *This limited representative cannot perform transactions.* If the Participant desires to designate a representative with inquiry rights only, complete the following information.

Rikki Ramirez
Name

Portfolio Analyst
Title

5123205042
Phone

5123205041
Fax

rikki@patterson.net
Email

D. That this Resolution and its authorization shall continue in full force and effect until amended or revoked by the Participant, and until TexPool Participant Services receives a copy of any such amendment or revocation. This Resolution is hereby introduced and adopted by the Participant at its regular/special meeting held on the 01 day of August, 2020.

Note: Document is to be signed by your Board President, Mayor or County Judge and attested by your Board Secretary, City Secretary or County Clerk.

Name of Participant*

SIGNED

Signature*

H. Neil Matkin
Printed Name*

District President
Title*

ATTEST

Signature*

Kristy Horkman
Printed Name*

Secretary to Board of Trustees
Title*

2. Mailing Instructions

The completed Resolution Amending Authorized Representatives can be faxed to TexPool Participant Services at 1-866-839-3291, and mailed to:

TexPool Participant Services
1001 Texas Avenue, Suite 1150
Houston, TX 77002

Collin County Community College District Board of Trustees

2020-08-3-X August 25, 2020

Resource: Melissa Irby
Chief Financial Officer

AGENDA ITEM: Report Out of the Finance and Audit Committee and Consideration of Approval of the Appointment of Authorized Representatives to Engage in Investment Transactions with TexPool

DISCUSSION: The Texas Local Government Investment Pools (the "TexPool Portfolios") have been organized in conformity with the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code, and the Public Funds Investment Act, Chapter 2256 of the Texas Government Code. These two acts provide for the creation of public funds investment pools and permit eligible governmental entities to jointly invest their funds in authorized investments.

Texpool requires governing body approval of representatives who are authorized to conduct business on behalf of the Board of Trustees. The authorized representatives change from time-to-time which requires an amended notification. At its meeting on August 18, 2020, the Finance and Audit Committee reviewed the recommended appointments of authorized representatives to engage in investment transactions with TexPool.

DISTRICT PRESIDENT'S RECOMMENDATION: The District President recommends approval of the appointment of Melissa Irby, Julie Bradley, Barbara Johnston, Suzanne Armstrong, and Keitha Carlton as authorized representatives of Collin College and, as such, are authorized to engage in investment transactions with TexPool, and further, that TexPool be notified of such approval.

SUGGESTED MOTION: This item comes as a motion and second out of committee. A suggested motion would be, "Mr. Chairman, I make a motion that the Board of Trustees of Collin County Community College approves the appointment of authorized representatives to engage in investment transactions with TexPool."

Collin County Community College District Board of Trustees

5. Finance and Audit Committee August 18, 2020

Resource: Ali Subhani
Director of Internal Audit

DISCUSSION ITEM: Discussion of Internal Audit Results for the College

AGENDA: Results for the following internal audit project will be outlined:

- Report Number 20-02 – TAC 202 Audit

COLLIN COLLEGE

OFFICE OF

Internal Audit

August 19, 2020

Dr. Neil Matkin, President
Members of the Board of Trustees:

An audit of Texas Administrative Code (TAC) 202 for fiscal year 2020 has been completed. The objective of the audit was to assess the college's compliance with TAC 202 requirements.

Overall, a framework of policies and procedures to facilitate full compliance with TAC 202 requirements has not been completely developed. Opportunities exist to enhance the college's compliance with the Security Control Standards Catalog.

Please let me know if you have any questions or comments regarding this audit.

We appreciate the courtesies and considerations extended to us during the engagement.

Ali Subhani

Director of Internal Audit

Report Distribution:

Collin College:

Mr. Michael Dickson

Members of the Board of Trustees:

Trustee Dr. J. Robert Collins
Trustee Andrew Hardin
Trustee Jim Orr
Trustee Dr. Raj Menon
Trustee Stacy Anne Arias
Trustee Dr. Stacey Donald
Trustee Greg Gomel
Trustee Fred Moses
Trustee Jay Saad

TABLE OF CONTENTS

OFFICE OF

Internal Audit

EXECUTIVE SUMMARY

AUDIT OBJECTIVE & SCOPE

The objective of the audit was to assess the college's compliance with TAC 202 requirements. The scope of the audit encompassed current operations.

AUDIT RECOMMENDATIONS

Recommendation	Risk Level	Implementation Date
1. Develop Policies to Facilitate Full Compliance with TAC Requirements	**High**	June 2021
2. Develop Framework to Implement Separation of Duties	**Medium**	August 2021
3. Strengthen Governance of Shared Accounts	**Medium**	February 2021
4. Enhance User Management	**Medium**	August 2021
5 Deploy Logon Banners on Technology Resources	**Low**	February 2021

DESIGNATED MANAGEMENT

Responsible Parties

Mr. Michael Dickson,
Chief Innovation Officer

Mr. Matthew Shane Ammons,
Chief Information Security Officer

CONCLUSION

Overall, a framework of policies and procedures to facilitate full compliance with TAC 202 requirements has not been completely developed. Opportunities exist to enhance the college's compliance with the Security Control Standards Catalog.

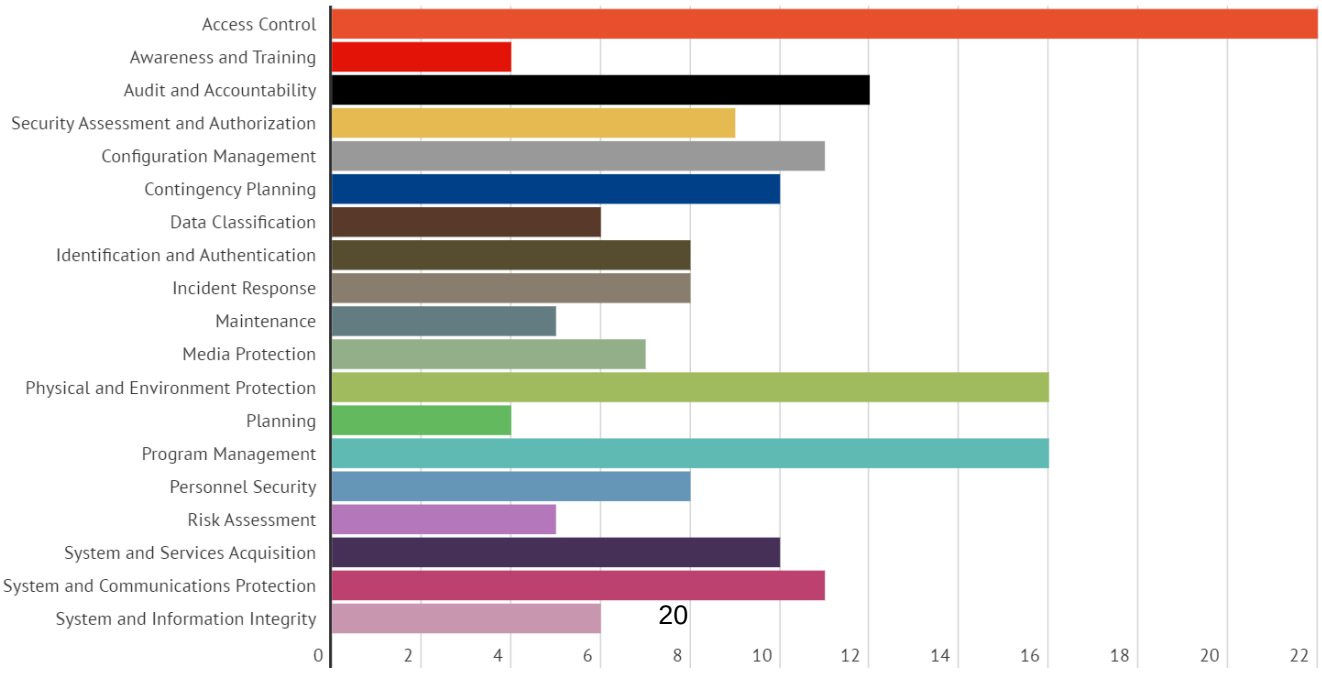
BACKGROUND

Texas Administrative Code (TAC) Title 1, Part 10, Chapter 202, Information Security Standards, Subchapter C, Security Standards for Institutions of Higher Education, outlines the security policies of the State of Texas that apply to institutions of higher education as follows:

TAC Code	Description
§202.70	Responsibilities of the Institution Head
§202.71	Responsibilities of Information Security Officer
§202.72	Security Reporting
§202.73	Staff Responsibilities
§202.74	Institution Information Security Program
§202.75	Managing Security Risks
§202.76	Security Control Standards Catalog (SCSC)

The information security controls prescribed by TAC 202 are expansive and encompass multiple facets of the technology landscape. Overall, there are 19 mandated controls groups. The following chart outlines the control groups and the number of requirements within each group that must be implemented.

Control Groups Mandated by the Security Control Standards Catalog



BACKGROUND

The desired goal with prescribing TAC 202 requirements is to improve an organization's information security posture. Per the Texas Department of Information Resources (DIR), the SCSC "initiated by DIR to help state agencies and higher education institutions implement security controls. It specifies the minimum information security requirements that state organizations must employ to provide the appropriate level of security relevant to level of risk".

TAC 202 was updated by a statewide committee of information security officers in 2015 to move it closer to Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

TAC 202 TIMELINE

November 2004
TAC 202 is amended to apply to institutions of higher education

March 2015
TAC 202 updated in line with federal requirements

September 2019
Requirements of Senate Bill 64 go into effect and mandate compliance with information security standards for junior colleges

COMPLIANCE NOTED

The following instances of compliance were noted as the audit was completed:

- An information security officer has been designated.
- The required security plan was submitted to the Department of Information Resources (DIR) as required for fiscal year 2020.
- Information security training to educate users on information security risks was offered to employees.

AUDIT OBJECTIVE AND SCOPE

The objective of the audit was to assess the college's compliance with TAC 202 requirements. The scope of the audit encompassed current operations.

METHODOLOGY

To satisfy audit objectives, the following procedures were performed:

- Reviewed and gained an understanding of existing policies and procedures over information security.
- Interviewed Information Security personnel to gain an understanding of relevant processes.
- Reviewed the Information Security Plan that was submitted to the Department of Information Resources (DIR).
- Tested supporting documentation and identified controls for compliance with TAC 202 Security Control Standards.

The examination was conducted in partial conformance with the guidelines set forth in the Institute of Internal Auditor's International Standards for the Professional Practice of Internal Auditing. The Standards are statements of core requirements for the professional practice of internal auditing. Those standards require that sufficient and appropriate evidence is obtained in performing and planning the audit to provide a reasonable basis for the findings and conclusions based on the audit objectives. With the exception of compliance with Standard - 2340 related to supervision, the evidence obtained provides a reasonable basis for the findings and conclusion based on the audit objectives.

AUDIT RESULTS & MANAGEMENT RESPONSES

1. Develop Policies to Facilitate Full Compliance with TAC Requirements

Risk Level: High	Category: Governance

TAC §202.74 -Institution Information Security Program states :

"Each institution of higher education shall develop, document, and implement an institution of higher education-wide information security program.....

The program shall include:
policies, controls, standards, and procedures that

(A) are based on the risk assessments required by §202.75 of this chapter;

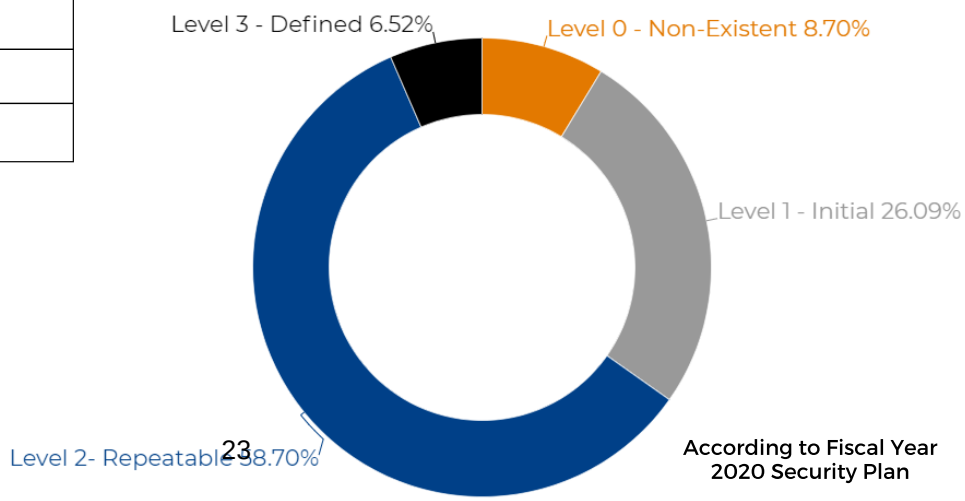
(B) cost-effectively reduce information security risks to a level acceptable to the institution head;

(C) ensure that information security is addressed throughout the life cycle of each institution of higher education information resource"

DIR's Prescribed Ranking Tiers
Level 0 - Non-Existent
Level 1 - Initial
Level 2 - Repeatable
Level 3 - Defined
Level 4- Managed
Level 5 - Optimized

In a review of the security plan submitted to the DIR, the prescribed methodology for completing the report offered six ranking tiers when self-assessing the college in fulfilling applicable TAC 202 requirements. Level zero signified the least mature control state, whereas level five signified the most mature control state. Since the college does not have comprehensive policies to address all the security controls applicable under TAC 202, 43 out of the 46 security controls noted on the annual security plan are below the defined state. See Appendix 1 for additional detail on the ranking of each security control that was submitted to DIR. Without formal policies that address all the domains of TAC 202, the college risks non-compliance with applicable requirements.

Maturity of Security Controls



According to Fiscal Year 2020 Security Plan

Recommendation:

Security policies to facilitate full compliance with TAC requirements should be developed. Subsequently, a plan to achieve the defined maturity level at a minimum for all the security controls should be developed.

Management Response:

IT Management will work with Collin College Leadership and DIR to design and implement an online IT Security Policy Page. The specific goal will be to improve each of the 43 objectives within the Collin College Security Plan, 25% by June 10, 2021.

Person Responsible for Implementation:

Matthew Shane Ammons, Chief Information Security Officer

2. Develop Framework to Implement Separation of Duties

Risk Level: Medium	Category: Governance / Compliance

SCSC Control AC-5 states:
"State organizations shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity."

There is currently no process in place to ensure that conflicting job responsibilities are kept separated when access is assigned to users. As a result, the following instances to improve segregation exist:

- Individuals outside of the Office of Procurement have privileges to set up a vendor and process accounts payable payments.
- Individuals who serve in information technology-related roles maintain the capability to perform business functions such as setup vendors, onboard employees, and process payroll.

The annual access review performed in the fiscal year 2019 did not identify the segregation of duty conflicts. Without consistent segregation of duties (SOD), individuals may be able to override controls. Overall, the concept of least privilege is not consistently followed as multiple individuals had higher privileges assigned than was necessary to accomplish their assigned job duties.

Recommendation:

The responsible data-owners should identify the conflicting responsibilities that should be separated. (A non-exhaustive SOD matrix is included in Appendix 2). Subsequently, the Office of Technology should develop a separation of duties matrix that can be utilized at the time privileges are assigned to ensure conflicting responsibilities are not assigned to the same individual. The concept of least privilege should be followed when security is assigned in WorkDay.

Management Response:

Current implementation and migration from BANNER to Workday provide a developed framework for separation of duties. This recommendation will be complete with the Workday implementation.

Person Responsible for Implementation:

Matthew Shane Ammons, Chief Information Security Officer

3. Strengthen Governance of Shared Accounts

Risk Level: Medium	Information Technology / Security

SCSC Control AC-3 states:

"Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access."

SCSC Control AC-2 states:

"Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group."

A documented risk analysis has not been performed for all shared accounts that are utilized at the college. Additionally, there is no established process for reissuing credentials at the time when an individual who had knowledge of the shared account leaves the institution.

Without an established process for updating the credentials for shared accounts after employee turnover, unauthorized access to information systems may not be prevented, and since shared accounts are not designated to specific users, it would be difficult to identify unauthorized access.

Recommendation:

A documented risk analysis for all shared accounts should be performed. Additionally, a process for reissuing account credentials for shared accounts should be implemented when organizational changes take place.

Management Response:

Current implementations of OneLogin and Workday provide embedded governance of shared accounts. IT Management will work to develop and implement future policies and procedures in accordance with TAC 202 guidelines.

Person Responsible for Implementation:

Matthew Shane Ammons, Chief Information Security Officer

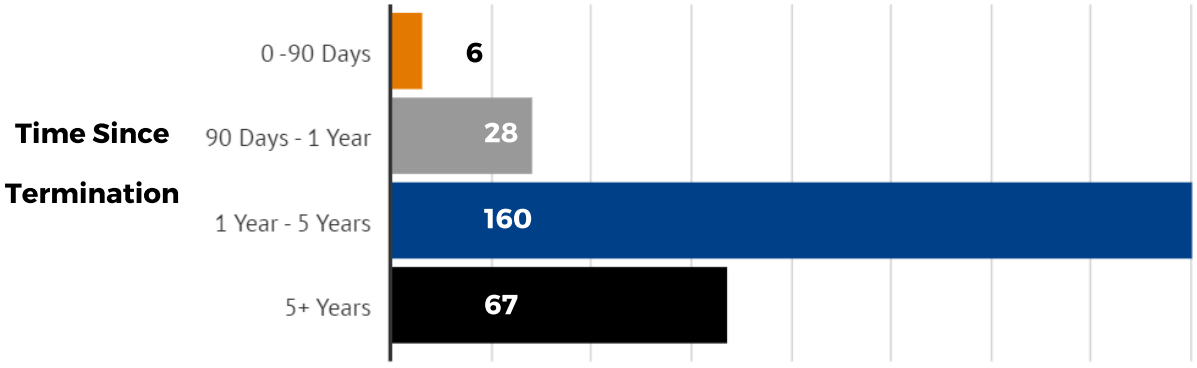
4. Enhance User Management

Risk Level: Medium	Information Technology / Security

SCSC Control PS-4 states:
"The organization, upon termination of individual employment: a. Disables information system access."

271 users were identified that maintained access to the college's IT resources after they were terminated in payroll. The department responsible for processing the access termination requests is required to wait on an authorization to terminate users. Unauthorized access to the college's IT resources may not be prevented if access is not terminated in a timely manner.

Number of Terminated Users That Maintained Access



Recommendation:

User management practices should be enhanced to terminate access privileges consistently.

Management Response:

IT Management is working with Collin College Leadership to develop policies and procedures for account provisioning and decommissioning. User management will be enhanced with the automated tools provided in Workday.

Person Responsible for Implementation:

Matthew Shane Ammons, Chief Information Security Officer

5. Deploy Logon Banners on Technology Resources

Risk Level: Low	Information Technology / Security

SCSC AC- 8 System Use Notification states:

"System identification/logon banners shall have warning statements that include the following topics: • Unauthorized use is prohibited; • Usage may be subject to security testing and monitoring; • Misuse is subject to criminal prosecution; and • Users have no expectation of privacy except as otherwise provided by applicable privacy laws."

The College's technology resources (applications and computing devices) are not configured to display banners that fulfill the requirements of TAC 202. Logon banners may offer the college legal recourse after a security violation has occurred.

Recommendation:

Logon banners in line with TAC requirements should be consistently deployed on technology resources.

Management Response:

IT Management will work with the server team to develop access-based policies to display login banners based on industry security standards and TAC 202.

Person Responsible for Implementation:

Matthew Shane Ammons, Chief Information Security Officer

CONCLUSION

Overall, a framework of policies and procedures to facilitate full compliance with TAC 202 requirements has not been completely developed. Opportunities exist to enhance the college's compliance with the Security Control Standards Catalog.

PRIORITY FINDINGS AND RISK MATRIX

Definitions of Risks

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact Collin College. If not addressed timely, could directly impact achievement of a strategic or important operational objective of Collin as a whole.
High	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to the college's operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose the college. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to the college will be minimal.

AUDIT OBSERVATION CATEGORIES

- Compliance
- Cost Savings
- Financial Reporting
- Governance
- Information Technology / Security
- Operations
- Reputation

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
1.	Privacy and Confidentiality	Ensuring the appropriate security of retained information and approved sharing under defined conditions with required safeguards and assurance. Includes the requirements of HIPAA, Texas Business & Commerce Code, and agency defined privacy policies that include and expand upon regulatory and legal requirements for establishing contractual/legal agreements for appropriate and exchange and protection.	Level 2
2.	Data Classification	Data classification provides a framework for managing data assets and information resources based on utility to the organization, intrinsic financial value and impact of loss and other associated risks. To apply the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations, data, whether electronic or printed, must be classified. The data owner should consult with the Information Security organization and legal counsel on the classification of data as Restricted, Confidential, Agency-Internal, or Public. Consistent use of data classification reinforces with users the expected level of protection of data assets in accordance with required security policies.	Level 2
3.	Critical Information Asset Inventory	Identification and prioritization of all of the organization's information assets so that they are prioritized according to criticality to the business, so that protections can be applied commensurate with the assets importance.	Level 0
4.	Enterprise Security Policy, Standards and Guidelines	Maintain the organization's security policy framework, standards, and guidelines. Defines the acceptable use policy for agency information resources. Contributes to the definition of enterprise standards and secure configuration standards to ensure alignment to security specifications and risk management requirements. There will be situations where the strict application of an information security standard would significantly impair the functionality of a service. The exception management process provides a method for evaluating the risks associated with non-compliant conditions and tracking the exception until expiration.	Level 1
5.	Control Oversight and Safeguard Assurance	Catalog the security activities that are required to provide the appropriate security of information and information resources throughout the Enterprise. Evaluate the control activities that have been implemented in terms of maturity, scope/breadth of implementation, effectiveness or associated deficiency to assure required protection levels as specified by security policy, regulatory/legal requirements, compliance mandates, or organizational risk thresholds. Ensure that control activities are performed as required and performed in a manner that is auditable and verifiable. Identify control activities that are not implemented or are not effective at achieving the defined control objectives. Oversee the implementation of required controls to ensure ongoing audit readiness and effective control implementations.	Level 0

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
6.	Information Security Risk Management	The assessment and evaluation of risk within the information resources and technology to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.	Level 2
7.	Security Oversight and Governance	The set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly.	Level 0
8.	Security Compliance and Regulatory Requirements	Monitor the legislative and industry landscape to ensure security policy is updated in consideration of changes that are pertinent or applicable to the organization. Facilitate any validation audits, assessments or reporting that is necessary to assure compliance to applicable laws, regulations, or requirements. Includes the HIPAA Privacy Office(r), IRS Safeguard Reviews, and responses to third party inquiries into the security of the organization.	Level 3
9.	Cloud Usage and Security	The assessment and evaluation of risk with the use of "cloud" technologies including Software as a Service (SAAS), Platform as a Service (PAAS), and Information as a Service (IAAS), to ensure that business operations are capable of delivering programs and services efficiently and effectively within acceptable tolerances potential negative outcomes.	Level 1
10.	Security Assessment & Authorization / Technology Risk Assessments	Evaluate systems and applications in terms of design and architecture in conjunction with existing or available controls to ensure that current and anticipated threats are mitigated within acceptable risk tolerances. Includes an analysis of in-place systems periodically or when significant change occurs as well as the analysis of the introduction of new technology systems.	Level 1
11.	External Vendors and Third Party Providers	Evaluation of third party providers and external vendors to ensure security requirements are met for information and information resources that will be transmitted, processed, stored, or managed by external entities. Includes contract review as well as the development of service level agreements and requirements.	Level 2
12.	Enterprise Architecture, Roadmap and Emerging Technology	An enterprise information security architecture that is aligned with Federal, State, Local and agency data security and privacy requirements. Using a roadmap and emerging technology evaluation process, the Information Security Program will stay abreast of the continued evolution of security solutions, processes, and technology to identify continuous, ongoing ways to deliver technology and information securely.	Level 1

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
13.	Secure System Services, Acquisition & Development	Ensure that the development and implementation of new systems meets the requirements necessary to assure the security of information and resources.	Level 2
14.	Security Awareness and Training	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on security related information, threats, and technology risks.	Level 3
15.	Privacy Awareness and Training	Define, prepare, deliver, and facilitate an ongoing awareness campaign utilizing a wide variety of mediums and delivery mechanisms to effectively and constantly educate the organization on privacy requirements and information related to the protection of privacy risks and protections.	Level 2
16.	Cryptography	Establish the rules and administrative guidelines governing the use of cryptography and key management in order to ensure that data is not disclosed or made inaccessible due to an inability to decrypt.	Level 1
17.	Secure Configuration Management	Ensure that baseline configurations and inventories of information systems (including hardware, software, firmware, and documentation) are established and maintained throughout the respective system development life cycles. Establishes and enforces security configuration settings for information technology products employed in information systems. Ensures all systems are operating under configurations that have been agreed upon according to organizational risk management.	Level 2
18.	Change Management	Establishes a set of rules and administrative guidelines to manage changes in a rational and predictable manner. In addition, it provides for the necessary documentation of any changes made so as to reduce any possible negative impact to the Users of IR systems. Changes include, but are not limited to implementation of new functionality, interruption of service, repair of existing functionality, and the removal of existing functionality.	Level 2
19.	Contingency Planning	Plans for emergency response, backup operations, and post-incident occurrence recovery for information systems are established, maintained and effectively implemented to ensure the availability of critical information resources and continuity of operations in emergency situations. Backing up data and applications is a business requirement.	Level 2

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
20.	Media	The protection of digital and non-digital information system media, the assurance that access to information on information system media is limited to authorized users, and requirements that information system media is sanitized or destroyed before disposal or release for reuse.	Level 2
21.	Physical and Environmental Protection	Assure that physical access to information systems, equipment, and the respective operating environments is limited to authorized individuals. Protect the physical locations and support infrastructure for information systems to ensure that supporting utilities are provided for to limit unplanned disruptions.	Level 2
22.	Personnel Security	Ensuring that individuals responsible for agency information are identified and their responsibilities are clearly defined. Any individuals occupying positions of responsibility within the agency (including third-party service providers) are trustworthy and meet established security criteria for those positions. Ensuring that information resources are protected during and after personnel actions such as terminations and transfers.	Level 2
23.	Third-Party Personnel Security	Requires all third party providers to comply with all security policies and standards. Establishes personnel security requirements including roles and responsibilities with limits on access requirements defined in accordance to least privileged and data minimization methodologies. Monitors providers for compliance.	Level 2
24.	System Configuration Hardening and Patch Management	Ensure that systems are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and service disruptions by configuring operation systems and software with appropriate parameters. Includes the removal of default accounts/passwords, disablement of unnecessary protocols/ports/services, and the ongoing distribution and installation of service packs/patches.	Level 2
25.	Access Control	Processes used to ensure access to applications, servers, databases, and network devices in the environment is limited to authorized personnel. Access is to be limited to authorized users, processes acting on behalf of authorized users, or authorized devices.	Level 2
26.	Account Management	Account Management establishes the standards for the creation, monitoring, control, and removal of accounts. A request process for accounts that includes authorization, approval for access by data owners, and acknowledgement of the user of their responsibilities are controls that assure proper account management. Periodic reviews of access entitlements as well as prompt removal of access during role change or employment termination are also controls that are part of account management.	Level 2

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
27.	Security Systems Management	The design, implementation, configuration, administration, maintenance, monitoring, and ongoing support of security systems used to enforce security policy and provide security services. Systems include firewalls, Intrusion Prevention Systems (IPS), Internet Proxy Servers, Security Information and Event Management (SIEM) systems, and other control enforcement or monitoring systems.	Level 0
28.	Network Access and Perimeter Controls	Network equipment such as servers, workstations, routers, switches and printers should be installed in a manner that prevents unauthorized access while limiting services to only authorized users. A perimeter should be established to delineate internal systems and prevent unauthorized external parties from tampering, attempting access or connecting without approved remote access methods.	Level 2
29.	Internet Content Filtering	The enforcement of controls used to block access to Internet websites based upon categories of content, application types and granular application functions, time of day or amount of utilization, or the dynamically updated reputation of the destination.	Level 2
30.	Data Loss Prevention	Solution designed to detect and prevent potential data breach incidents where sensitive may be disclosed to unauthorized personnel by malicious intent or inadvertent mistake. Detection of data at risk can be performed while in use at the endpoint, while in motion during transmission across the network, and while at rest on data storage devices.	Level 2
31.	Identification and Authentication	The verification of the claimed identity of users, processes, or devices as a prerequisite to permitting access. Password standards establish the rules for the creation, length and complexity requirements, distribution, retention and periodic change as well as suspension or expiration of authenticators.	Level 2
32.	Spam Filtering	As digital messaging (e-mail, cellular messaging, etc.) has become an integral part of the business process, its abuse has also grown. This abuse often is manifested as “SPAM” or “junk” messaging which has the potential to, beyond its annoying nature, slow-down and/or clog the infrastructure required to process electronic messages. To limit the effects of “SPAM”, messages will be examined for content and filtered as required.	Level 2
33.	Portable and Remote Computing	Additional considerations must be made for portable devices and the specific configuration and enforcement of controls will likely require special consideration.	Level 2

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
34.	Security Systems Management	Establishes the requirements for protections such as link encryption, secure file transmission protocols, retention of files on source and destination systems, integrity validation, and restrictions for access at all levels (i.e. user/process, system, and network).	Level 1
35.	Vulnerability Assessment	Assessment and monitoring of vulnerability detection and remediation including patch management processes, configuration management, system, database and application security vulnerabilities. Test and evaluate security controls and security defenses to ensure that required security posture levels are met. Perform and/or facilitate ongoing and periodic penetration testing of security defenses. Evaluate results of various penetration tests to provide risk based prioritization of mitigation.	Level 1
36.	Malware Protection	The prevention, detection and cleanup of Malicious Code (including virus, worm, Trojan, Spyware and other similar variants). Protection is accomplished at varying layers including at the host, at the network, or at the gateway perimeter. Protection mechanisms must be updated periodically and frequently to address evolving threats and monitored to provide manual intervention where required.	Level 1
37.	Security Monitoring and Event Analysis	Analysis of security events and alerts as detected by the array of security enforcement devices and log collection facilities implemented throughout the Enterprise environment.	Level 1
38.	Cyber-Security Incident Response	Establishes an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities. The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities.	Level 1
39.	Privacy Incident Response	Management of events, issues, inquiries, and incidents when detected or reported to include all phases from investigation through resolution. Responsible for notifying and escalating incidents to appropriate personnel and coordinating activities to ensure timely isolation and containment, impact analysis, and any resulting remediation / resolution requirements.	Level 1
40.	Portable and Remote Computing	Managing the recovery of data and applications in the event of loss or damage (natural disasters, system disk and other systems failures, intentional or unintentional human acts, data entry errors, or systems operator errors).	Level 2

APPENDIX 1 - SECURITY PLAN SUBMITTED TO DIR

	Security Objective	Definition	Maturity Level
41.	Audit Logging and Accountability	Processes, policies, and procedures that enable organizations to establish an accurate and verifiable record of system relevant actions whether manual or automated for investigatory and accountability purposes.	Level 1
42.	Information Systems Currency	Ensures that the necessary knowledge, skills, hardware, software, and supporting infrastructure are available at a reasonable cost to support information systems operations. Includes the monitoring and planning of future system developments that enable the organization to leverage modern technology and reduce technical debt.	Level 1
DS 1.	Secure Application Development	Ensuring that the code and processes that go into developing applications are as secure as possible. Includes not only the application's processes, but the processes used in the development of the application.	Level 2
DS 2.	Security Monitoring and Event Analysis	Analysis of security events and alerts as detected by the array of security enforcement devices and log collection facilities implemented throughout the Enterprise environment.	Level 2
DS 3.	Cyber-Security Incident Response	Establishes an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and response activities. The Incident Response program is used to track, document, and report incidents to appropriate officials and/or authorities.	Level 2
DS 4.	Vulnerability Testing	Scanning a system for known vulnerabilities, quantifying the vulnerabilities' risk levels based on the system's exposure to them, and preparing risk plans for each vulnerability.	Level 3

APPENDIX 2 - SEGREGATION OF DUTIES MATRIX

Process	COSO	Procedure/Function	Grp	1 Create Requisition	2 Approve Requisition	3 Create PO	4 Approve PO	5 Create Voucher	6 Approve Voucher	7 Cut Check	8 Add/Edit Vendor	9 Approve Vendor	10 Bank Reconciliation	11 Enter JE	12 Approve JE	13 Custody of Cash	14 Approval of Bank Dep	15 Post Receipts	16 Add/Edit Customers	17 TGRRCON (BANNE	18 Hire Employee	19 Change Compensat	20 Change Benefits	21 Create Paycheck	22 ADP Recon
Purchasing	R	Create Requisition	1		X		*		*	X	X	X	X		*										
	A	Approve Requisition	2	X		*		*		X	X	X	X	*												
	R	Create PO	3		*		X		*	X	X	X	X		*											
	A	Approve PO	4	*		X		*		X	X	X	X	*												
	R	Create Voucher	5		*		*		X	X	X	X	X		*											
	A	Approve Voucher	6	*		*		X		X	X	X	X	*												
	C	Cut Check	7	X	X	X	X	X	X		X	X	X	X	X											
	A	Add/Edit Vendor	8	X	X	X	X	X	X	X		X														
	A	Approve Vendor	9	X	X	X	X	X	X	X	X															
Reconciliation	RX	Bank Reconciliation	10	X	X	X	X	X	X	X				*	X	X	X	X							X	
Journal Entry	R	Enter JE	11		*		*		*	X			*		X	X	X	X								
	A	Approve JE	12	*		*		*		X			X	X		X	X	X								
Cash Receipts	C	Custody of Cash	13										X	X	X		X	X	X	X		X	X	X		
	A	Approval of Bank Deposit	14										X	X	X	X		X	X	X						
	R	Post Receipts	15										X	X	X	X	X		X	X						
	A	Add/Edit Customers	16													X	X	X		X						
	RX	TGRRCON (BANNER)	17													X	X	X	X							
Emp Comp	R	Hire Employee	17																			X	X	X	X	X
	A	Change Compensation	18													X					X			X	X	
	A	Change Benefits	19													X					X					X
	C	Create Paycheck	20										X			X					X	X				X
	RX	ADP Recon	22																		X	X	X	X		
				Purchasing									EJ	Journal		Cash Receipts					Employee Comp					

COSO Category	
R	Record
A	Authorize
C	Custody
RX	Reconcile

SOD Risk Level	
X	Elevated Risk
*	Low Risk

SOURCE: USG

Collin County Community College District Board of Trustees

2020-08-3-X August 25, 2020

Resource: Ali Subhani
Director of Internal Audit

AGENDA ITEM: Report Out of the Finance and Audit Committee and Discussion of Internal Audit Results for the College

DISCUSSION: Results for the following internal audit project will be outlined:

- Report Number 20-02 – TAC 202 Audit

DISTRICT PRESIDENT'S RECOMMENDATION: No recommendation. This item is for presentation only.

SUGGESTED MOTION: This item is for presentation only. No action is required.