



# Payroll and Benefits Internal Audit Status Update



April 19, 2021

# Agenda

- ▲ **1** Introductions
- ▲ **2** Project Overview and Status
- ▲ **3** Preliminary Opportunities for Improvement
- ▲ **4** Next Steps



# Introductions

BerryDunn Team



**Rob Smalley**  
CPA, CGMA, CFE  
Engagement Principal



**Katy Balukas**  
CPA  
Manager

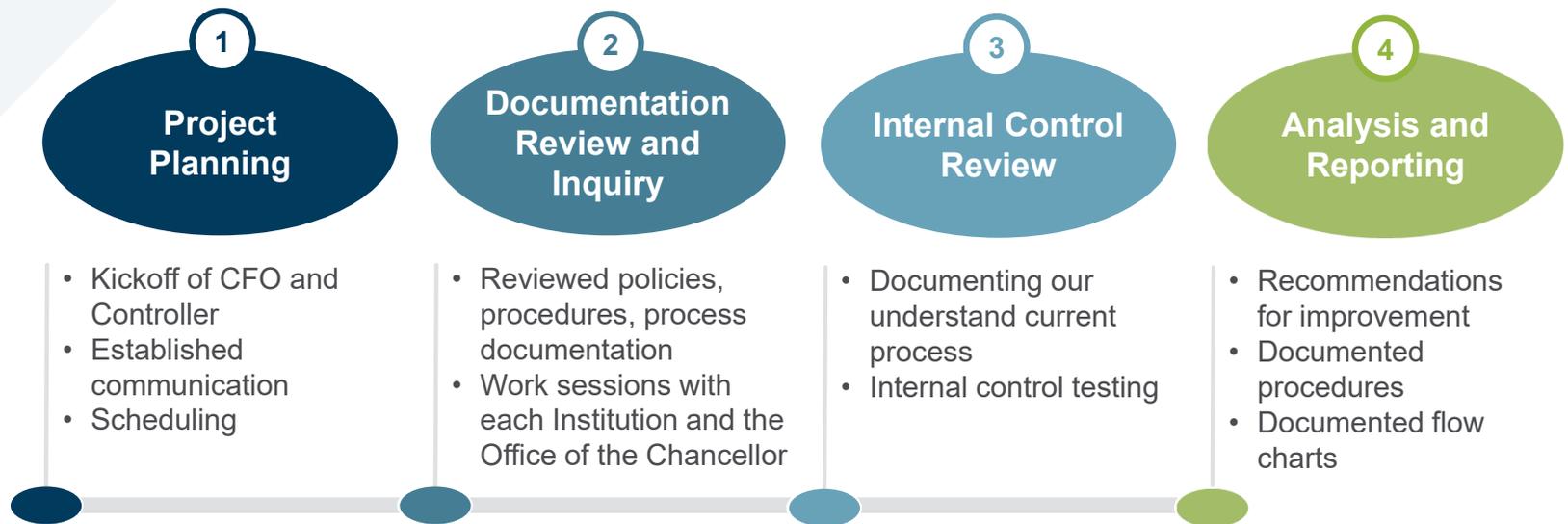


**Courtney Lindsay**  
CPA  
Lead Analyst



# Project Overview and Status

## Our Approach



\*We are currently working in steps 3 and 4



## Preliminary Opportunities for Improvement

- ▲ Review and validation of changes made to payroll
- ▲ Standardization of processes and forms utilized
- ▲ Time reporting
- ▲ Management of terminated employees



# Next Steps

Estimated Timeline

Project Tasks	March	April	May
Project Planning	█		
Documentation Review and Inquiry		█	
Internal Control Review		█	
Analysis and Report Development		█	



# Contact Information

**Rob Smalley, CPA**

Principal

[rsmalley@berrydunn.com](mailto:rsmalley@berrydunn.com)

603.518.2627

**Katy Balukas, CPA**

Manager

[kbalukas@berrydunn.com](mailto:kbalukas@berrydunn.com)

603.518.2648



This report/communication is intended solely for the information and use of the Board of Trustees and its committee and management and is not intended to be, and should not be, used by anyone other than these specified parties.

[berrydunn.com](http://berrydunn.com)

Information Technology  
Security and Readiness



# Brief Overview

This presentation will provide a general overview of threats, both internal and external, facing the organization and an assessment of the technology the VSCS uses to protect its environment. Our team will also share the steps Information Technology is taking today to address these internal and external threats. Finally, we will also offer insights into the ways in which the system expects to address risks, and take advantage of opportunities, as it looks forward towards system transformation.

# Executive Summary

## VSCS Threat Mitigation

- Anti-phishing, Virus and Malware
- Secure Email
- Firewalls to Limit Access
- System Redundancy and Backups
- Security Mindset Workforce



Adequate Tools and  
Technology for Most Threats

## Areas of Deficiency

- Maintaining the Environment
  - Technology Updates and Refresh
  - Hardware & Software Updates and Replacement
- Governance Risk and Compliance (GRC)
- Resources
  - Single Person / No Person Support
  - Retention and Attrition
  - Skills Development
- Decentralized Ownership



Gaps in Fundamental  
Programs Resulting in a  
High Risk to the  
Organization

# Our Threats and Challenges

## What Are We Protecting?

- Organization Data
- Personal Information (Name, SSN, Etc.)
- Financial Information
- Medical Data



## What Are We Protecting it From?

- IT Interruption and Outages
  - Technology Failure
  - External Event (cut communications line)
  - 3<sup>rd</sup> Party Risk
- Security Events
  - Ransomware, Phishing
  - Data Theft and/or Destruction

## External Threats

- Education is becoming a popular target due to weaker controls and funding
- Stolen data can be easily sold on the black market
- Distance education will continue to be popular post-pandemic
- Increasing technology costs and resource shortages

What are the Challenges?

## Internal Challenges

- Very Large User Base: 80K User Mailboxes, 4 Schools + OC
- Enterprise Standards and Consistency
- Out of Support Platforms
- Single Person Risk
- Security as a Foundation

# Our Defenses

Event Type	Examples	Our Defenses
Major System Outage	<ul style="list-style-type: none"><li>• Data Center Failure</li><li>• Cut Communication Lines</li><li>• Catastrophic Event (Fire, Explosion, etc.)</li></ul>	<ul style="list-style-type: none"><li>• Redundant Network Paths between Critical Infrastructure</li><li>• 3<sup>rd</sup> Party Hosting at TechVault Data Center (Hardened Facility)</li><li>• Data Replication to Servers in Winooski</li></ul>
Software / Hardware Failure	<ul style="list-style-type: none"><li>• Server Crash or Drive Failure</li><li>• Corrupt Data</li><li>• Accidental Data Deletion</li></ul>	<ul style="list-style-type: none"><li>• Data Backups</li><li>• Software as a Service (SaaS) for Several Major Applications *<ul style="list-style-type: none"><li>• Library &amp; Learning Management System</li><li>• Admissions, HR, Payroll &amp; Canvas</li><li>• Video Conferencing, Identity Management, Email &amp; Security Tools</li></ul></li></ul>
Threat Management	<ul style="list-style-type: none"><li>• Virus, Malware &amp; Ransomware</li><li>• Spam and Phishing</li><li>• Unauthorized Access</li><li>• Malicious Links</li><li>• Disgruntled Employee</li></ul>	<ul style="list-style-type: none"><li>• Scanning and Threat Assessment of all Incoming Email and Links</li><li>• External Sending Warnings</li><li>• Secure Email System</li><li>• WiFi Security</li><li>• Vulnerability Scanning</li></ul>

# Highest Urgency

- Equipment Lifecycle and Maintenance
- Security Vulnerability Remediation
- Cloud & Infrastructure Strategy
- GRC (Governance Risk and Compliance)
  - Access Controls
  - Enterprise Retention
  - Standardized Business Processes and Policy Adherence
- Incident Logging, Event Correlation & Operations Support
- Resource Investment

# Strategy

- Build off COVID Relief Investment
  - Where were we before, where do we go?
- Focus on High-risk Areas and Quick Wins
- Programs Established
  - Enterprise Security Council
  - Monthly Phishing Assessments
  - Monthly Vulnerability Reviews
  - Enhancements to Email Security
- In Progress
  - Hardware /Software Review Process
  - User ID Hardening
  - Standards
- Develop a Sustainable Infrastructure Roadmap
- Transformation Opportunities Ahead