An OCPS Internal Audit Newsletter

AUDIT INSIGHTS

Volume 3, Issue 3

In the previous newsletter, we explored ERM Challenges and Tips. In today's fast-changing world, businesses face many risks. ERM helps companies spot and handle these risks. But with so much data and fast-moving threats, sometimes traditional methods may not be enough. AI is making ERM smarter and more powerful. In the future, businesses will be able to spot risks earlier, act faster, and make better decisions, turning risk into opportunity.

How ERM and AI Work Together
(Work Smarter Not Harder)

How AI Improves ERM:

Turning Data into Insights: Companies collect tons of data every day. AI can quickly scan this data to find warning signs of potential risks.

Predicting Future Problems: AI can look at past events to predict what might go wrong next— like a delay in supplies or a financial issue.

Watching in Real Time: AI tools can monitor systems 24/7 and alert teams if something unusual happens.

Helping with Decisions: AI can suggest ways to reduce risk and even act automatically in some cases.

Why It's Useful:

Faster response to risks

More accurate predictions

Saves time and money

Help leaders make smarter choices

Things to Watch Out For:

AI can be biased if the data is unfair.

Some AI systems are hard to understand.

Companies need to follow laws and be transparent.

Human judgment is still important— AI should help, not replace people.

This brings our ERM series to a close!

We hope the insights shared have been interesting, helpful and valuable to your understanding of Enterprise Risk Management (ERM).

Internal.Audit@ocps.net

Internal Audit Mission

We provide independent, objective assurance that adds value and enhances the district's performance, accountability, and transparency.

Client of the Quarter!!!

From Left to Right: Jessica Scheff, Lillie Adkins, Nicole Close (back), Allison Kibbey, Jennifer Norton, Margie Wells, and Sarah Kate McGuire

Our recent Library Media assessment, initiated in response to new legislative requirements, was successfully completed thanks to the exceptional collaboration and support from the Instructional Technology and Library Media (ITLM) department. Their team demonstrated a high level of professionalism and efficiency throughout the entire process, promptly responding to all inquiries and providing us with the necessary documentation and access. Their willingness to assist with onsite visits and their timely communication were instrumental in keeping the assessment on track and allowing for a thorough and efficient review of the district's library and instructional media programs.

Furthermore, the ITLM department proved to be a valuable resource in navigating the complexities of Florida statutes and the district's adaptation to recent legislative changes. Their deep understanding of the new requirements and the proactive measures they have implemented, from deploying new platforms like Beanstack to developing comprehensive training materials, provided us with a clear picture of the district's commitment to compliance. We extend our sincere thanks to the ITLM department for their outstanding service, dedication, and collaborative spirit, which greatly contributed to the successful completion of this assessment.

Congratulations!!

Contract Management Series

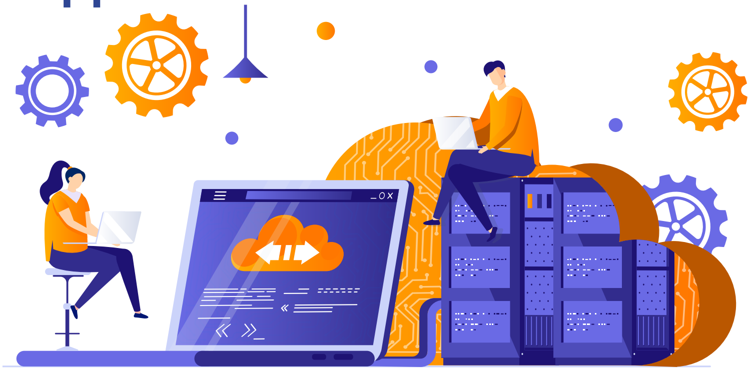
In a previous newsletter, we shared upcoming topics to be covered in future issues. Today, we're focusing on one of them:

10 Key Points to Consider Before Contracting a Project

1. **Project Scope and Complexity**
   Understand the project's scale and intricacy.
2. **In-House Capabilities**
   Assess your internal resources and skills.
3. **Cost and Budget**
   Determine the financial implications.
4. **Time Constraints**
   Consider the project's technical proficiency.
5. **Quality and Expertise**
   Evaluate the project's technical hazards.
6. **Potential Risks**
   Identify and analyze possible hazards.
7. **Specific Vendor Requirements**
   Note any criteria or standards for vendors.
8. **Contractual Obligations**
   Review the legal terms and conditions.
9. **Delivery of Product/Service**
   Verify the expectations for deliverables.
10. **Monitoring and Evaluation**
    Plan how to track progress and performance.

In our next issue, we'll explore how to identify potential vendors effectively.

IT General Controls and Application Controls Overview



In today's digital environment, organizations rely heavily on technology to manage operations, store data, and support decision-making.To ensure that these systems function reliably and securely, two key types of controls are used: IT General Controls (ITGCs) and Application Controls. ITGCs form the foundation of an organization's IT environment,helping to protect systems and data across the board. They cover areas like access management, system changes, and data backups. On the other hand, Application Controls are built into specific software programs and focus on ensuring that data entered, processed, and reported by those applications is accurate and complete. Together, these controls help maintain the integrity of financial reporting, compliance, and operational effectiveness.

IT GENERAL CONTROLS

Basic controls for all systems and data

- Access controls
- Change management
- Backup and recovery
- System development controls
- Physical security

APPLICATION CONTROLS

Specific controls within individual software

- Input validation
- Processing controls
- Output controls
- Authorization checks

Scope	Organization-wide	Specific to individual applications
Purpose	Ensure overall system reliability	Ensure accurate data processing e.g., Input checks
Examples	Affects all systems	Affects specific business processes

FRAUD PREVENTION and AWARENESS TIP

Strong passwords are another tool to aid in fraud prevention. Strong passwords should be:

1. **Unique and complex** - use upper-case, lower-case letters, numbers, symbols.
2. **Long passwords** - use 16 characters or more.
3. **Avoid obvious** – steer clear of birthday, pet names that are easy to guess.
4. **Avoid reusing** – don't use the same password on social media, bank accounts, etc.
5. **Keep it confidential** – don't share or write it down where others can see.
6. **Regular update** – consider changing every 90 days.
7. **Extra layer** – Add an extra layer of security using a code from your phone or email.
8. **Watch for phishing** - Don't click on suspicious links or enter passwords on unfamiliar websites. Always check the URL and look for HTTPS.
9. **Watch for shoulder surfing** – Be aware of visual hacking where someone observes your screen or keyboard to steal information especially, in public places.

OCPS Report Phish

Cybersecurity Tip in collaboration with ITS

Spot and Report Phishing

Phishing is the most common way cybercriminals attempt to deceive you into revealing confidential information. It can happen via email, text (smishing – like the ones you get from "SunPass" every now and then), or phone calls (vishing) from senders impersonating trusted individuals or organizations. Always be on the lookout for urgent language, poor grammar, deceiving email address or unexpected requests for your password. **Never click on a suspicious link or provide information.** Instead, report the attempt immediately using the new **Report Phish** in the top-right corner of the email button in Outlook, or forward the email to *Phishing@ocps.net*.

Meet the Auditor – *Brandon Giraldo*

Brandon recently joined us as a Staff Internal Auditor after working at PricewaterhouseCoopers, where he specialized in Digital Assurance & Transparency for financial services clients. He holds both a master's and bachelor's degree in accounting from Queens College of the City University of New York. Originally from Queens, NY, Brandon brings a strong background in IT General Controls, data analytics, and risk assessment. Outside of work, Brandon is always on the move! He loves playing soccer, going to the beach, traveling the world, and trying new foods wherever he goes. If you ever need a restaurant recommendation or want to chat about your latest travel adventure, Brandon's your guy! We're excited to welcome Brandon to the team and look forward to the energy and expertise he brings to OCPS!

Internal Control *Tip*

A common cause of internal control breakdowns: inadequate supervisory and/or management oversight.

Reports issued since our last newsletter

- Consultant Competitive Negotiation Act (CCNA)
- Skyward Gradebook

All our reports are available for your reading enjoyment on our website at https://www.ocps.net/reports

Did you Know...

A typical fraud case lasts 12 months before detection.

Strengthening Quality Through Internal Self-Assessment

We are currently conducting an internal self-assessment which is a periodic internal review that evaluates:

- The internal audit department's conformance with the Institute of Internal Auditors Global Internal Audit Standards
- Compliance with internal policies and procedures
- Effectiveness of audit practices and deliverables

The internal self-assessment typically involves:

- Surveys and feedback from audit staff and stakeholders
- Cross-review of audit engagements to ensure objectivity and coverage

The internal self-assessment process helps us:

- Maintain independence and objectivity in our audit work
- Identify areas for continuous improvement
- Ensure our audits provide value and insight to stakeholders
- Prepare for the external quality assessment, which occurs every five years. Our next external quality assessment will take place in the fall of 2026.

The internal self-assessments are reviewed with the Audit Advisory Committee and shared with the School Board, reinforcing transparency and accountability.

Internal Audit Annual Report

We've had a dynamic and productive year!

Our latest **2025 Internal Audit Annual Report** *https://ocps.net/internal-audit-annual-report* highlights a year full of achievements and new initiatives.

Inside, you'll find:

- Key accomplishments of our internal audit team
- Benchmarking data comparing us with other large school districts
- Insights into our governance and adherence to professional standards
- Details on construction audits, audit activities, and several other impactful efforts

Take a look to see how we're driving accountability and continuous improvement across the district.

Internal Audit Annual Plan

Internal Audit Audit Plan

June 24, 2025

OCPS Orange County Public Schools

Each year, we create our audit plan through a thorough risk assessment process. The plan is then reviewed and approved by both the Audit Advisory Committee and the School Board. On June 24, the **2025–2026 Annual Audit Plan** *https://ocps.net/annual-audit-plan* was officially approved. This year's plan includes key focus areas such as:

- IT General Controls – Phase 3
- Schools' Technology Support
- Data Security Practices for Artificial Intelligence
- AI Governance
- Certificates of Insurance
- ...and several other audits