
KPMG
Own your future.
Focus on results.
See what's on the horizon
for your business.

KPMG

Managing Cloud and On-premise ERP Fraud and Cyber Risk

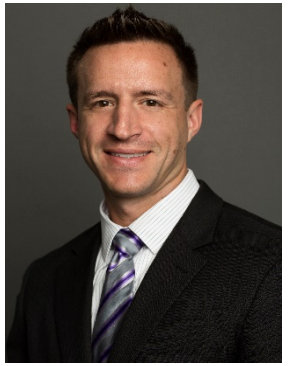
Session ID: BUS6552

October 22, 2018

ORACLE OPEN WORLD

With you today…..

ORACLE Platinum Partner Cloud Elite



Nick Seeman
Managing Director / KPMG LLP
nseeman@kpmg.com

Beau Bollinger
Manager of IT Security, Risk and Compliance /
Advanced Drainage Systems, Inc.
Beau.Bollinger@ads-pipe.com

Join the conversation
@KPMG_US
#KPMGoow #oow18

KPMG

Advanced Drainage Systems

Advanced Drainage Systems is the leading manufacturer of high performance thermoplastic corrugated pipe, providing a comprehensive suite of water management products and superior drainage solutions for use in the construction and infrastructure marketplace. Its innovative products are used across a broad range of end markets and applications, including non-residential, residential, agriculture and infrastructure applications.

Agenda

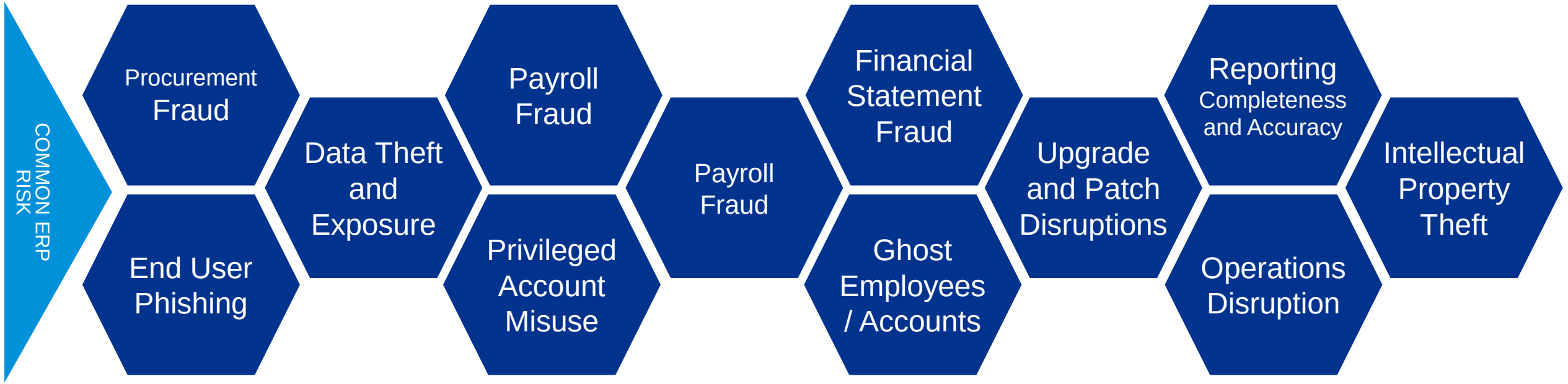
- **Fraud and Cyber ERP Risk**
- **Cloud Adoption Risk**
- **Risk Mitigation Strategies**
- **Real Life Fraud Risk Scenarios**
- **Real Life Cyber Risk Scenario**
- **Closing Remarks**

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

Fraud and Cyber ERP Risk

ERP Risk is a persistent, global challenge for executives and board members. Managing the risk of fraud and financial misstatement has grown more complex as technology changes and companies face an increased volume of cyber threats and no let-up in the more traditional forms of wrongdoing, such as the falsification of books and records.

ERP, HCM, Supply Chain and BI related fraud, cyber security, and weak controls are serious and persistent problems for many organizations. On premise and cloud applications are not immune to the challenge.

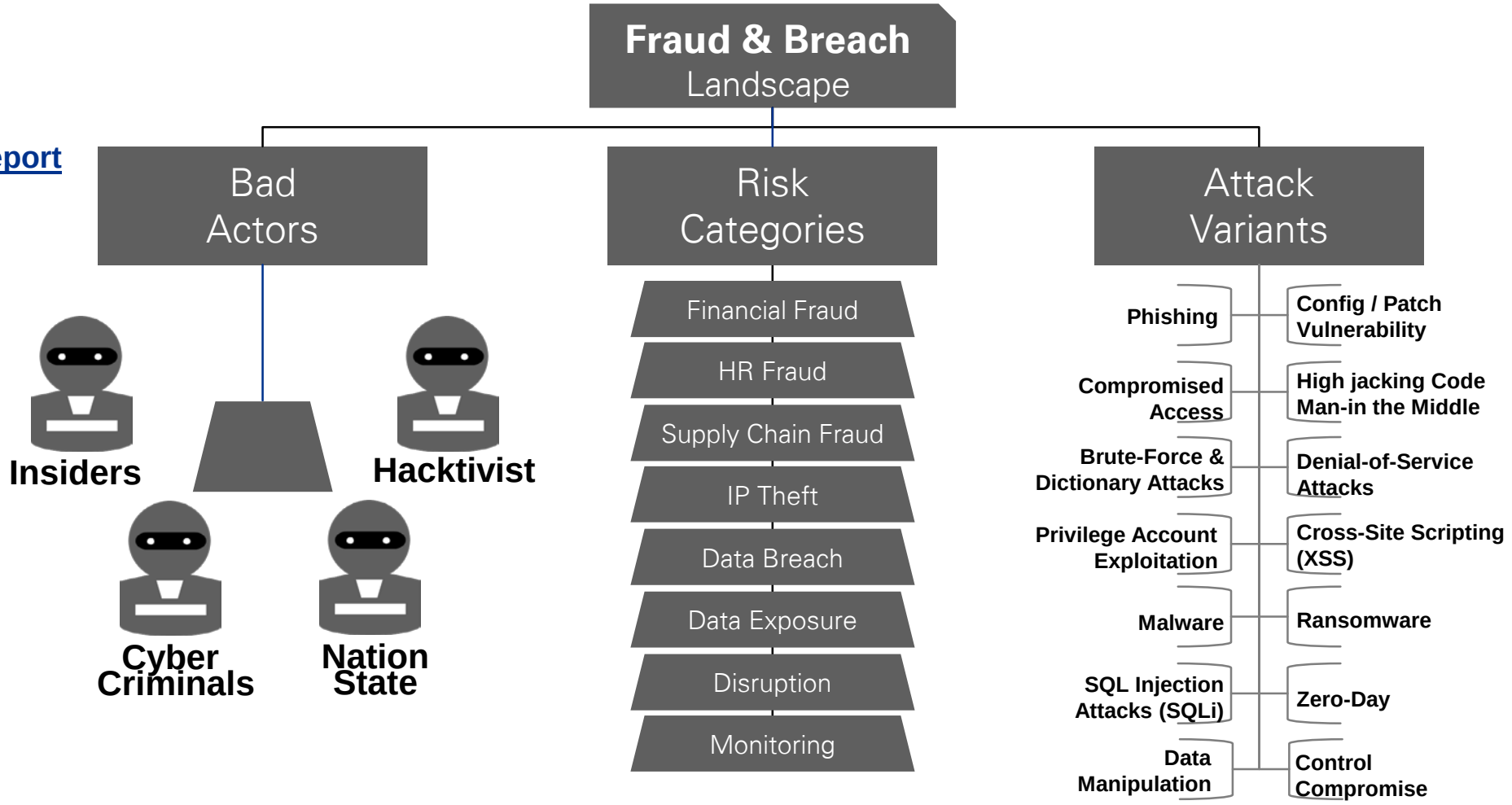


Fraud and Cyber ERP Risk

Fraud & Cyber Breach Landscape

[Kroll Annual Global Fraud & Risk Report]

84% of companies surveyed worldwide experienced a fraud incident in 2017, 86% reported at least one cyber incident, and 70% reported security incidents, according to the Kroll Annual Global Fraud & Risk Report



Cloud Adoption Risk

Cloud adoption promises the benefit of increased flexibility, agility, and significant cost savings, so migrating more and more applications including business-critical applications to the cloud is becoming a growing priority for companies of all sizes.

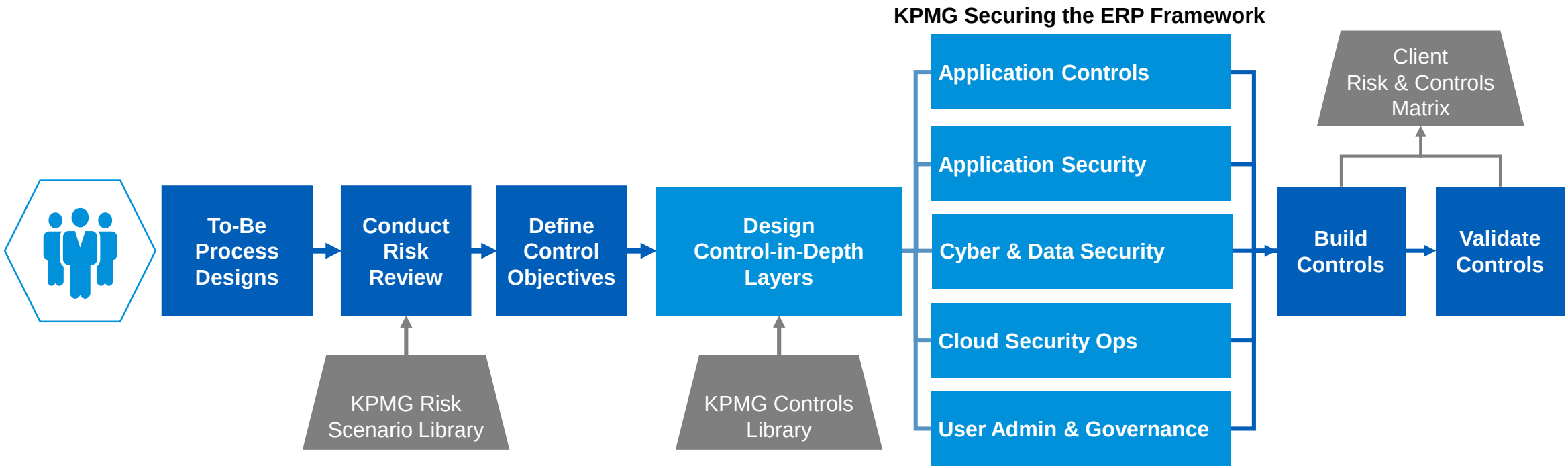
Although many enterprises adopt new applications on a regular basis, *few have real-world experience in securely adopting or using cloud services*. Migrating enterprises' business-critical applications and services to the cloud has a more significant risk profile than any single software upgrade. Often, cloud adoption is part of a companywide initiative that represents a new paradigm for doing business. This new paradigm introduces new risk and those risks have to be mitigated.

> "Many organizations are faced with the need to close the gap between their organization's use of the cloud and their readiness to secure a growing cloud footprint…"
>
> – Oracle and KPMG Cloud Threat Report 2018

Risk Mitigation Strategy: Controls in Depth

Managing risk in today's on premise and cloud ERP applications require defining policies and implementing a controls-in-depth program which leverages well-defined functional roles, automated business process controls and cloud cyber and data solutions to protect business processes and sensitive data as functional transactions are moved out of the traditional on-premise IT environment to the cloud.

Our KPMG controls-in-depth architects leverage our proprietarily controls library for ERP and our controls-in-depth design approach to help our clients define a risk and controls program that balances enablement with protection.



Fraud Risk Scenarios

Fraud Risk Scenario #1

ERP Risk	Financial Fraud – Sales and Billing

Bad Actor	Insider
Risk Category	Financial Fraud
Attack Variant	Business Process & Access Controls Compromises

Business Process	Record to Report
Risk Level	High
Data	Sales / Billing Data

Risk Narrative

1) Accounting manager stole at least $3.5 million
2) Manager sold grain to customers at below cost and was responsible for accounting of those sales
3) Manager created false accounting records and meddled with payment procedures to send herself payments
4) By reversing the false entries, inventory at the plant was booked as depleted, but the commensurate revenue was no longer booked as a receivable,
5) Manager was able to receive incoming payments from customers for delivered products 'off the radar' without the accounting team anticipating prompt receipt of those payments
6) Payments from the customers were required to go to a lockbox controlled by a third party. The invoices automatically generated by the company's ERP software instructed customers to send their payment to the third party. Instead, the Manger created hundreds of fraudulent invoices in Microsoft Word instructing customers to send payment to herself
7) The company total losses estimated from $25 million to $50 million in cash, market share, public relations, hours for manpower, attorneys and auditors.

Controls-In-Depth Considerations

Application Controls	Application Security	Cyber & Data Security	User Access Administration	Cloud Security Operations
Preventative Controls: • Invoice workflow approvals • Accounting change approvals • Customer Master approval workflow Detective Controls: • Accounting entries changes and write-off analytics, alerts and notifications • Customer Master Controls analytics • Override notifications	Least Privilege Role design **Segregation of Duties**	Configuration monitoring Customer Master data Change Monitoring User behavior analytics	Positioned based role assignments to user	Appropriate ERP solution patching and update testing focused on Financial controls options Controls testing and validation

Fraud Risk Scenario #2

ERP Risk	Financial Fraud – Payment Fraud

Bad Actor	Insider
Risk Category	Financial Fraud
Attack Variant	Business Process & Access Controls Compromises

Business Process	Record to Report
Risk Level	High
Data	Payables Data

Risk Narrative

1) Multinational insurance and finance company suffered a $30 million net loss from the massive fraud committed by its senior accountant
2) Senior accountant was sentenced to at least seven years' in jail, the company recovered only a third of the $45.3 million the 42-year-old stole over five years
3) Senior accountant made 200 illegal transfers into her personal accounts or directly to shops and real estate agents
4) Senior accountant used the computer log-ins of former staff to delete the records or alter them so the transactions appeared legitimate
5) When police went to the Senior Accountant's workplace, they found 21 boxes stored under her desk and nearby
6) When these boxes were searched, police found large quantities of jewelry, fountain pens, champagne, crystal and Michael Jackson memorabilia
7) Senior Accountant was leading a normal life with her husband in a suburban house and none of the money was used to pay off any of their debt.
8) At times the Senior Account would spend millions of dollars in a single lunch hour and she lavished gifts on the shop assistants
9) The Senior Accountant claimed that part of the reason for engaging in fraud was resentment towards the Company and her wanting revenge

Controls-In-Depth Considerations

Application Controls	Application Security	Cyber & Data Security	User Access Administration	Cloud Security Operations
Preventative Controls: • Payment approval workflow • Write-Offs and deletion change approvals Detective Controls: • Accounting entries changes and write-off analytics, alerts and notifications • Override notifications	Least Privilege Role design Segregation of Duties	User behavior analytics across applications	**Automated user lifecycle management and termination of accounts**	Appropriate ERP solution patching and update testing focused on Financial controls options

Cyber Risk Scenario

Cyber Risk Scenario #1

ERP Risk	Phishing

Bad Actor	Cyber Criminal
Risk Category	Financial Fraud
Attack Variant	Phishing / Malware

Business Process	Payables
Risk Level	High
Data	Accounting Data / Bank Details / Video & Audio Surveillance

Risk Narrative

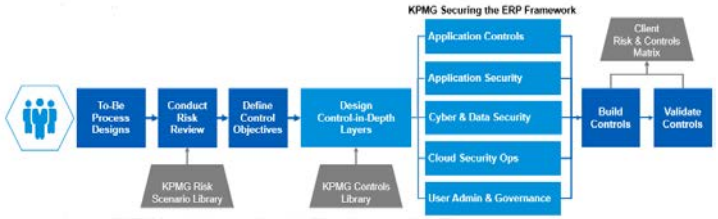
1) Spear-Phishing email attacks are installing legitimate remote administration software on the systems of nearly 400 industrial production companies
2) Each email addresses the employee by full name, accurately reflects the activity of the targeted organization, and specifies work performed by the employee to whom the email was sent
3) The personalized emails indicate that the attacks are carefully prepared and are uniquely created for each victim
4) Emails either contain malicious attachments or have message text designed to lure users to links that lead to external resources that result in downloading malware
5) The malware allows cyber criminals to take control and search for purchase documents, or financial and accounting software
6) This allows for various forms of financial fraud, including spoofing the bank details used to make payments
7) According to experts, industrial companies are the targets of these attacks due to lower cyber threat-awareness than other industries
8) It is important to note that the use of legitimate remote administration software evades detection by antivirus solutions
9) These attacks additionally collected: sensitive employee and customer data, video surveillance, and audio and video via devices connected to infected machines

Controls-In-Depth Considerations

Application Controls	Application Security	Cyber & Data Security	User Access Administration	Cloud Security Operations
<u>Preventative Controls:</u> • Vendor payment workflow • First vendor payment after bank detail changes require a manual check • PII data masking • Two or three-way matching configuration <u>Detective Controls:</u> • Accounting entries changes and write-off analytics, alerts and notifications • Common account number notification or report • Vendor payment reviews • Vendor reviews	Adaptive or Multifactor Authentication Least privilege application roles with SOD	Transaction geo monitoring User Behavior Analytics configured to look at payment changes **Anti-Phishing tools / Awareness Training**	Privilege Access Management program/tool	Appropriate ERP solution patching and update testing focused on financial controls options

Closing Remarks

SOX Is Not Enough!!!



Attention:

Clients with mature internal control environments and SOX programs are just as, if not more vulnerable to Financial implications due to fraud or cyber events as those with immature control environments because they believe effective SOX controls will protect them from fraudulent activity and any financial impact from Cyber Attacks.

The truth is that Controls-in-Depth is one of the only practical ways to reduce cost and maximize assurance over financial risk mitigation.

Controls-in-Depth Solution Matrix for Risk Scenarios

Cloud ERP Application Controls

Process Controls
- ✓ Automated Workflow Approval
- ✓ Approval Authority Limits
- ✓ Configuration Controls

Controls Analytics
- ✓ ERP Analytics Managed Services
- ✓ Manual Journal Entry Analysis
- ✓ Master Data Analytics

Cloud ERP Application Security

Access Controls
- ✓ Multifactor Authentication
- ✓ Geo Authentication monitoring
- ✓ RBAC Roles aligned with business processes
- ✓ Segregation of Duty controls
- ✓ Excess access Controls
- ✓ Privilege Access Controls
- ✓ Least Privilege Controls

Cyber & Data Security

Cyber Security
- ✓ Cyber policies
- ✓ Financial Event & Log monitoring with orchestration
- ✓ Privilege Access Controls
- ✓ End-to-End solution configuration monitoring

Data Security
- ✓ Data risk prioritization
- ✓ PII data security
- ✓ Key management
- ✓ Data masking
- ✓ Data encryption
- ✓ DRM
- ✓ Interface & Conversion controls

Cloud ERP User Access Admin

User Admin Controls
- ✓ Employee lifecycle integration with User Lifecycle processes
  - Add User
  - Change User
  - Suspend User
  - Remove User
- ✓ User Lifecycle management technologies
- ✓ Access certification
- ✓ User archival
- ✓ Password Management
- ✓ User Analytics

Cloud ERP Security Ops

Cloud Ops Controls
- ✓ Cloud Shared Responsibility model monitoring
- ✓ IT General Controls
- ✓ Cloud Financials Patch and release validation & management
- ✓ Code Reviews
- ✓ Testing support
- ✓ Configuration controls

Thank you

Nick Seeman
Managing Director / KPMG LLP
nseeman@kpmg.com

Beau Bollinger
Manager of IT Security, Risk and Compliance / Advanced Drainage Systems, Inc.
Beau.Bollinger@ads-pipe.com

Join the conversation
@KPMG_US
#KPMGoow

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia