Greenlight
TECHNOLOGIES

A Financial Executive’s Guide to Internal Controls & Fraud Prevention in the Cloud

July 2018

Speakers

James Rice

Vice President of Customer Solutions

Greenlight Technologies

Mark Kissman

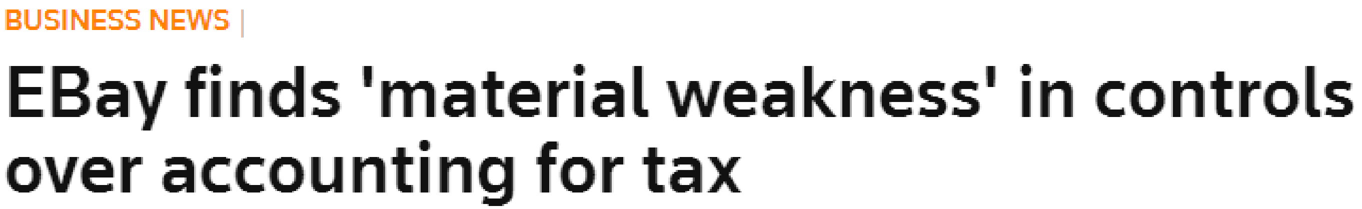
CFO

Greenlight Technologies

CFOs Under More Scrutiny for ICFR

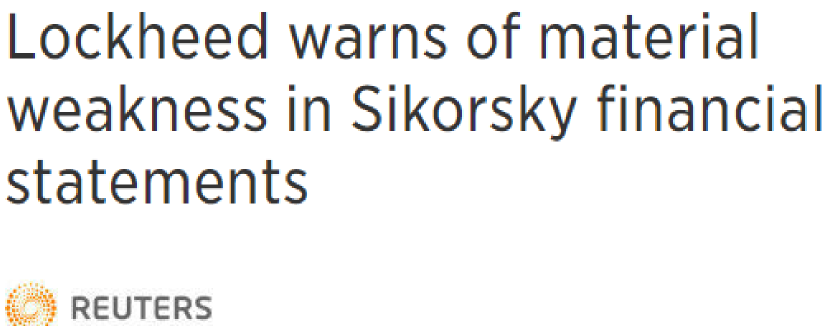
"SEC enforcers have been investigating and prosecuting a broader range of Internal Controls Financial Reporting (ICFR) violations than ever before."

Howard Scheck, former chief accountant of the SEC
CFO Magazine



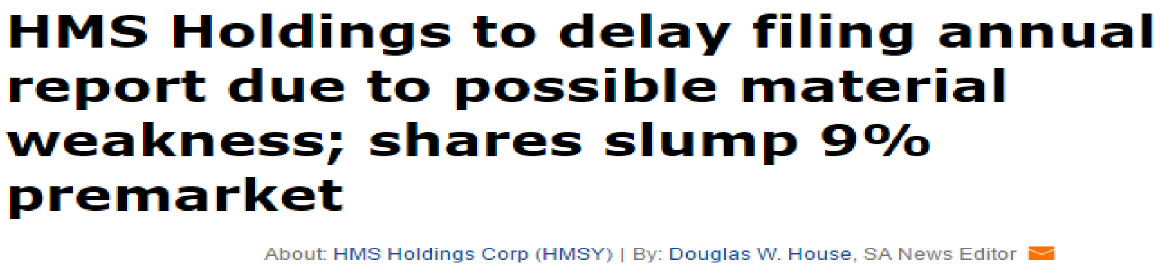
BUSINESS NEWS |

EBay finds 'material weakness' in controls over accounting for tax



Lockheed warns of material weakness in Sikorsky financial statements

REUTERS



HMS Holdings to delay filing annual report due to possible material weakness; shares slump 9% premarket

About: HMS Holdings Corp (HMSY) | By: Douglas W. House, SA News Editor

"Demonstrating a commitment to financial reporting integrity — before an incident occurs and during the handling of an incident — positions subjects to be viewed in the most favorable light by SEC staff, thus increasing the odds of a favorable outcome."

Agenda

1. Review of Internal Controls over Financial Reporting (ICFR)
2. What Changes are Auditors Requiring?
3. Segregation of Duties (SoD) Management Maturity
4. Why Is SoD Quantification Important?
5. Customer Use Case Examples
6. FEI Survey Results

What are Internal Controls over Financial Reporting?

“**Internal controls**” refer to those procedures within a company that are designed to reasonably ensure compliance with the company’s policies.

Under the framework developed by the Committee on Sponsoring Organizations (COSO), there are three types of internal controls:

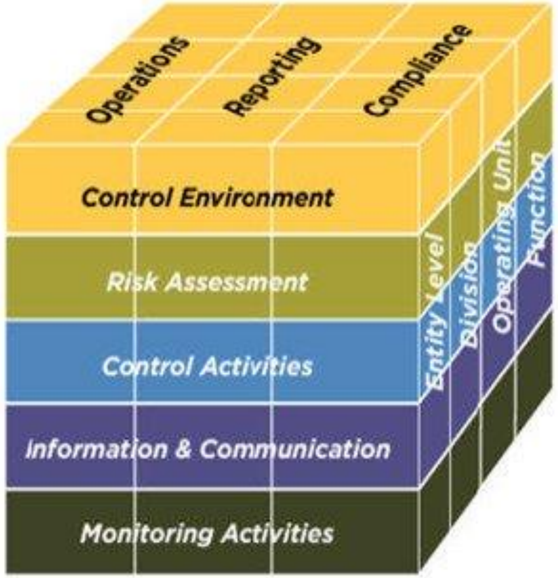
- Those that affect a company’s operations (e.g. effectiveness and efficiency)
- Those that affect a company’s compliance (e.g. laws and regulations)
- Those that affect a company’s **financial reporting** (e.g. reliability)

Internal Control Framework Review

The COSO model defines internal control as "a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance of the achievement of objectives".

There are five interrelated "components" of an effective internal control system. These are derived from the way the company is managed on a day-to-day basis.

1. **Control Environment**
2. **Risk Assessment**
3. **Control Activities**
4. **Information & Communication**
5. **Monitoring Activities**



What is a "material weakness" in ICFR?

A material weakness exists if there is a flaw within the company's overall control system such that it is at least reasonably possible that a material misstatement in the company's financial statements will not be prevented or corrected.

SOX 404 segregation of duties examples:

- Person that creates a vendor also pays the same vendor
- Person that receives commission from a sale also approves the loan agreement and reconciles the bank account
- Person that receives goods can also adjust inventory
- Person that enters fictitious purchase orders for personal use and accept the goods through goods receipt

POLL QUESTION

How would you rate your company's maturity with regards to ICFR?

1. Initial - at a starting point using an undocumented repeat process.
2. Repeatable - the process is documented sufficiently such that repeating the same steps may be attempted.
3. Defined - the process is defined/confirmed as a standard business process.
4. Capable - the process is quantitatively managed in accordance with agreed-upon metrics.
5. Efficient - process management includes deliberate process optimization/improvement.

FEI Survey Results

How Mature Is Your ICFR Program?

Financial executives were asked to rate their internal controls process using Capability Maturity Model (CMM). As the survey reveals, there are significant differences of perceived maturity based on compay size.

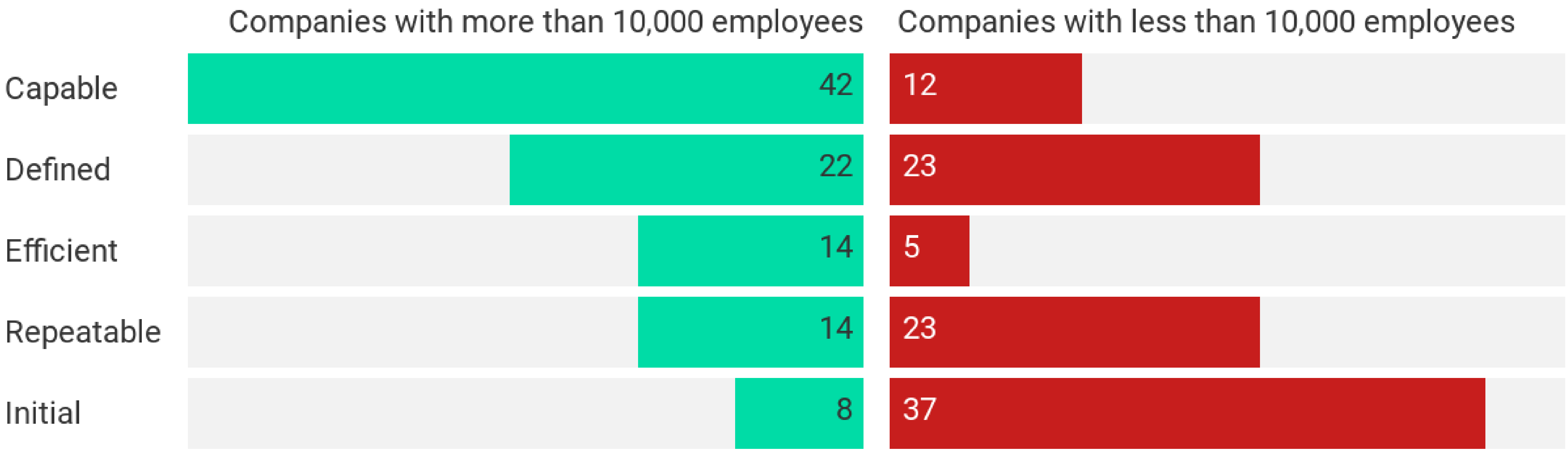


Chart: Financial Executives Research Foundation • Get the data • Created with Datawrapper

What’s Changing?

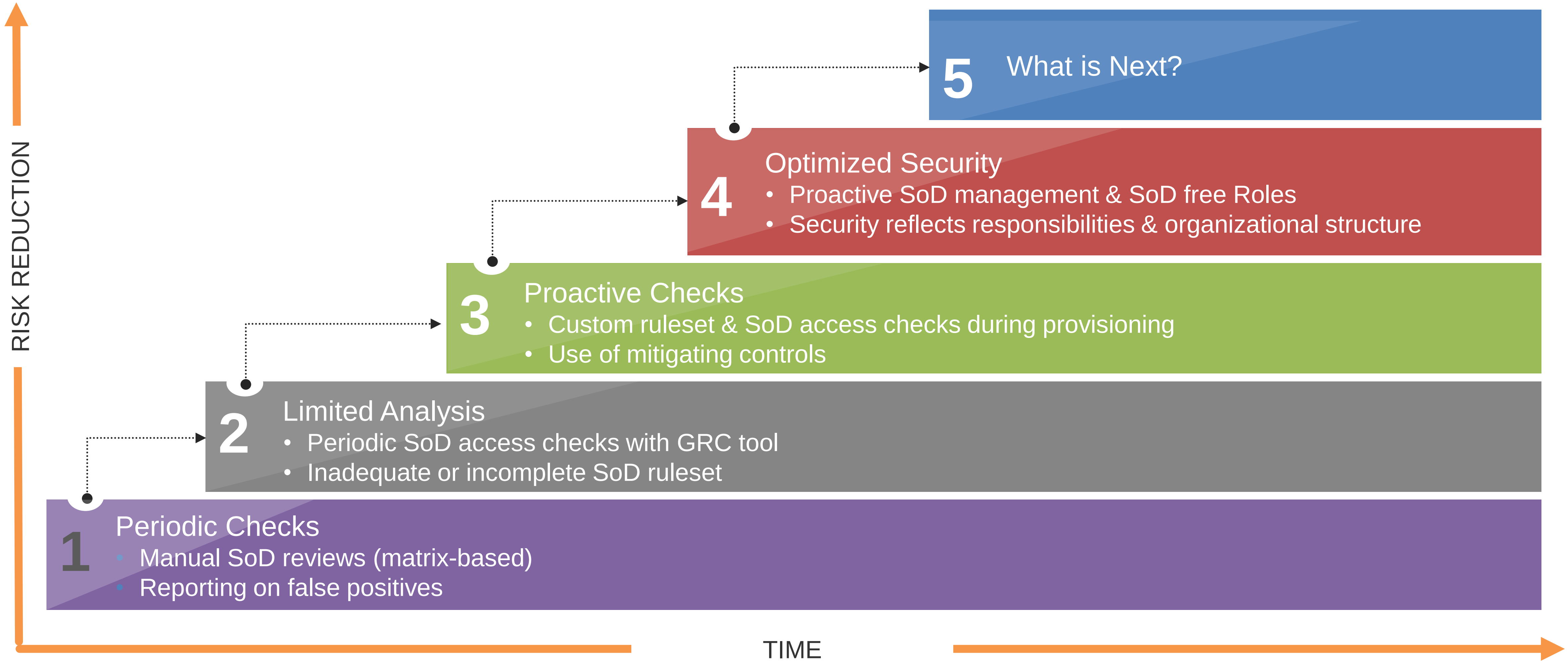
Auditors are now digging deeper into SOD management and identifying inadequate controls and incomplete procedures

- SOD solutions find the potential issues
- When issues remain in the business, a control must be identified

Challenges:

- No controls are defined – companies stop at the point of which users have risky access
- ‘Dummy’ controls are in place to mask risks from being reported as uncontrolled
- A business process control is identified and assigned that does not adequately monitor user risk
- Controls are defined, haphazardly being performed, or not at all
- Controls are defined for on-premise solutions but not cloud applications

SoD Risk Management Maturity



5 What is Next?

4 Optimized Security

- Proactive SoD management & SoD free Roles
- Security reflects responsibilities & organizational structure

3 Proactive Checks

- Custom ruleset & SoD access checks during provisioning
- Use of mitigating controls

2 Limited Analysis

- Periodic SoD access checks with GRC tool
- Inadequate or incomplete SoD ruleset

1 Periodic Checks

- Manual SoD reviews (matrix-based)
- Reporting on false positives

Is There A Better Way to Manage SoD?

Provisioning w/SoD Solutions

- Prevent & identify “potential” violations
- Occurrences are investigated if issues are identified (audit or fraud)
- Potential risks may be classified as “known” SoD’s

SoD Quantification

- ‘Who’ had SoD issues (mitigated or unmitigated)
- How many times did they execute these SoD?
- For how much? What is the risk exposure?

Accumulation of events between provisioning & certifications

Potential Risk vs. Actual Violations

Risk Policies

Risk Monitoring

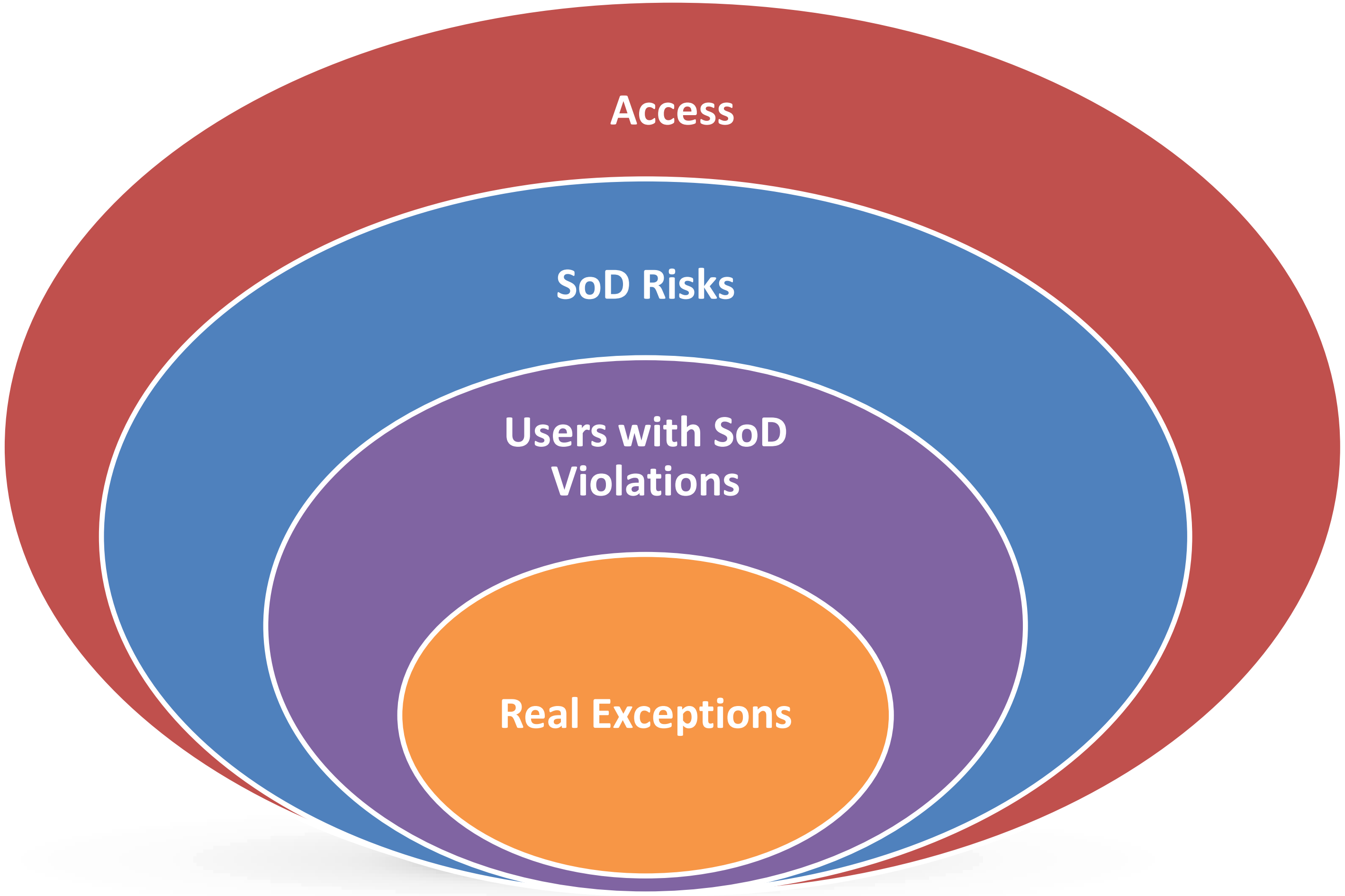
SOD Reviews — Potential

Reviewing user access rights and **monitoring** application security tables + Leveraging **SoD** rule sets = Visibility into users and roles with the **capability** to perform high risk transactions

Transaction Monitoring — Actual

Reviewing transaction meta data and **monitoring** usage in transaction tables + Leveraging **analytics** rule sets = Visibility into actual usage and violations **executed** against high risks in conflict with policy

What is SoD Quantification?



Access

SoD Risks

Users with SoD Violations

Real Exceptions

How Impactful Is SOD Quantification?

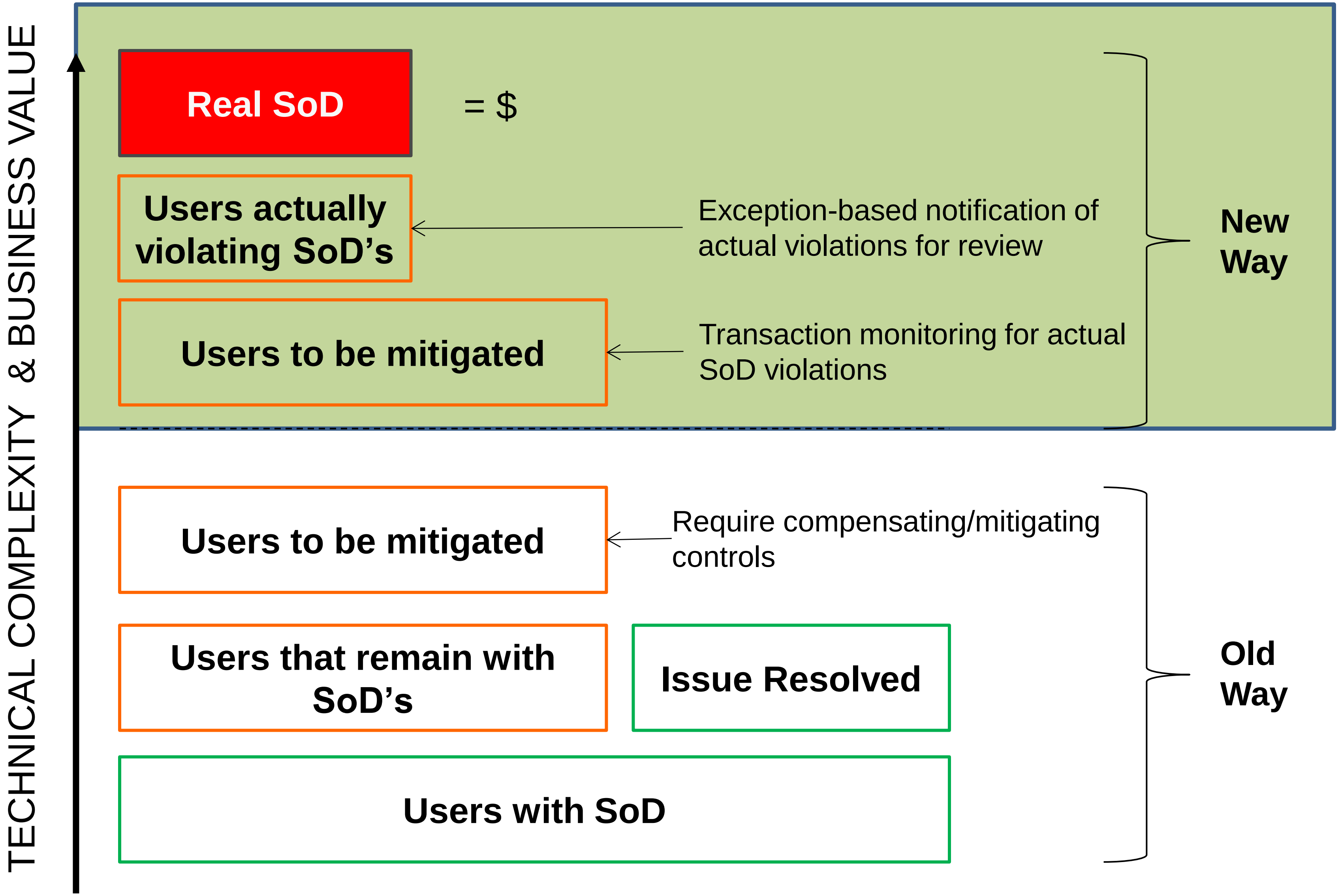
Summarized results help distinguish between ‘potential areas of risk’, which would require additional follow-up, and areas of ‘no concern’:

Actually happened

Risk	SoD Risk Description	Business Process	SoD Conflicts reported from User Access		SoD Violations reported from Quantification Analysis		
			# Users	# Violations	# Users	Total # Transaction Occurrences	Total $ Value (US $)
F001	Create a fictitious GL account and generate Journal activity or hide activity via posting entries	General Ledger	**21**	**2,116**	**0**	**0**	**$0**
P001	Maintain a fictitious vendor and enter a vendor invoice for automatic payment	Purchasing and Payables	**72**	**10,383**	**4**	**91**	**$493,108**

Potential to Perform

Prioritize Controls Based on Business Impact



TECHNICAL COMPLEXITY & BUSINESS VALUE

Real SoD = $

Users actually violating SoD's ← Exception-based notification of actual violations for review

Users to be mitigated ← Transaction monitoring for actual SoD violations

New Way

Users to be mitigated ← Require compensating/mitigating controls

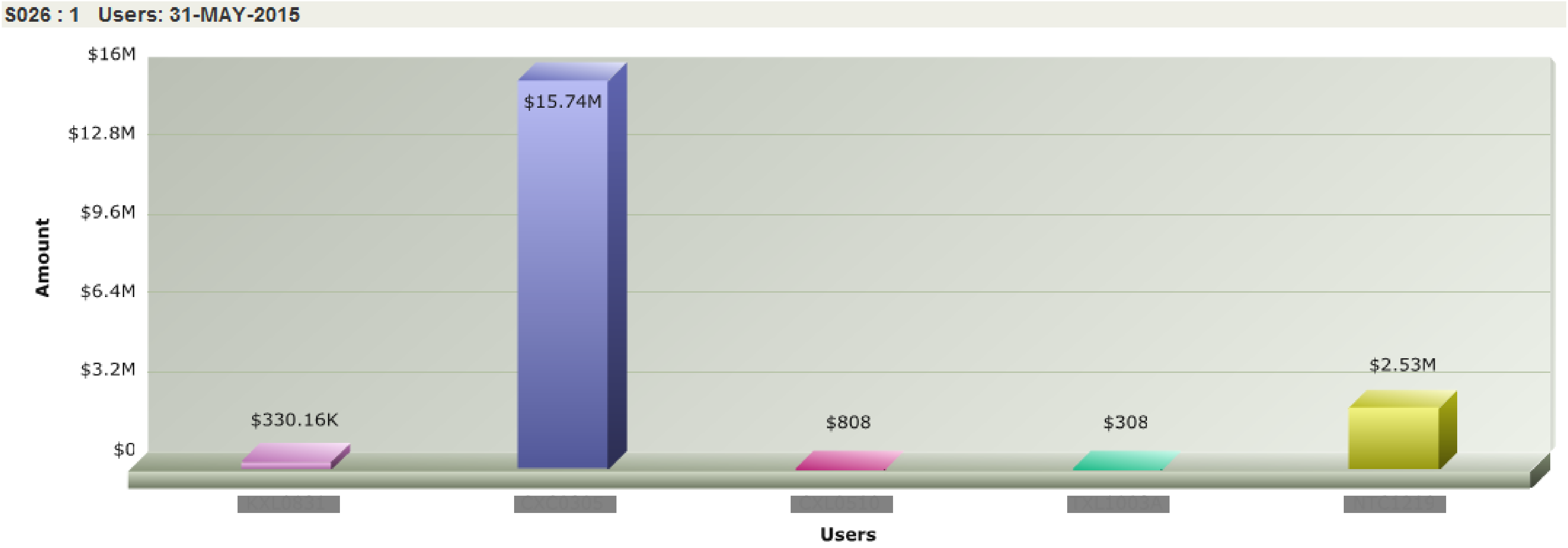
Users that remain with SoD's

Issue Resolved

Users with SoD

Old Way

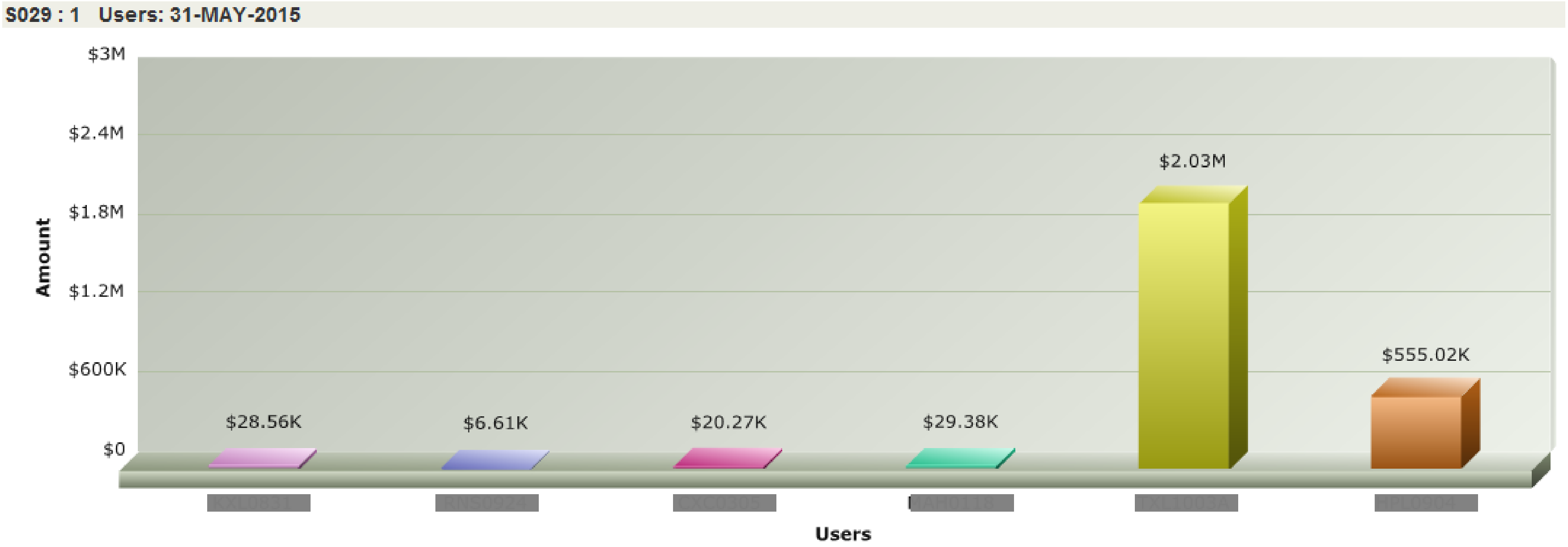
Customer Example: Invoicing & Processing Payments



- 140 users are reported by a GRC solution to have the authorizations to perform the risk
- 100% transaction monitoring shows detail of transactions for 5 users

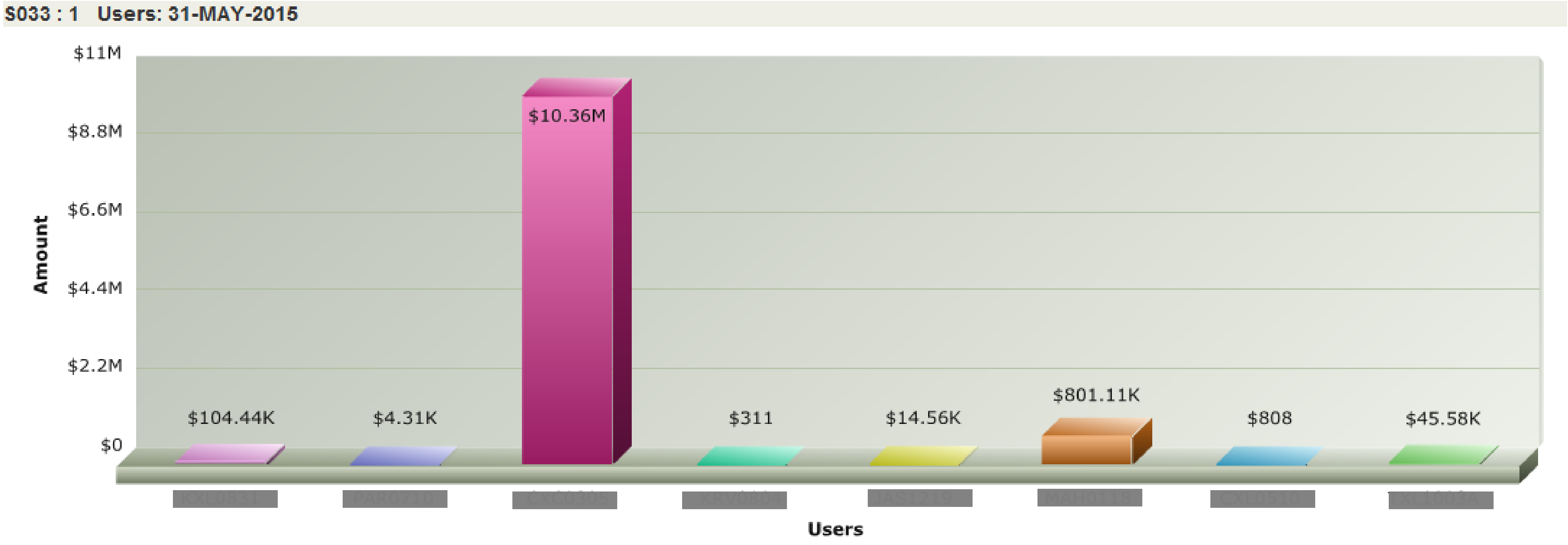
Find where the risk is materializing, have controls that are built into the business process and ensure transparency to the actual bottom-line business value ($) exposure allows senior management, compliance or audit to identify fraud much quicker than with typical manual monitoring

Customer Example: Credit Memo & Clear Balance



- 72 users are reported by a GRC solution to have the authorizations to perform the risk
- 100% transaction monitoring shows detail of transactions for 6 users

Customer Example: Invoicing & Clear Balances



- 76 users are reported by a GRC solution to have the authorizations to perform the risk
- 100% transaction monitoring shows detail of transactions for 8 users

POLL QUESTION

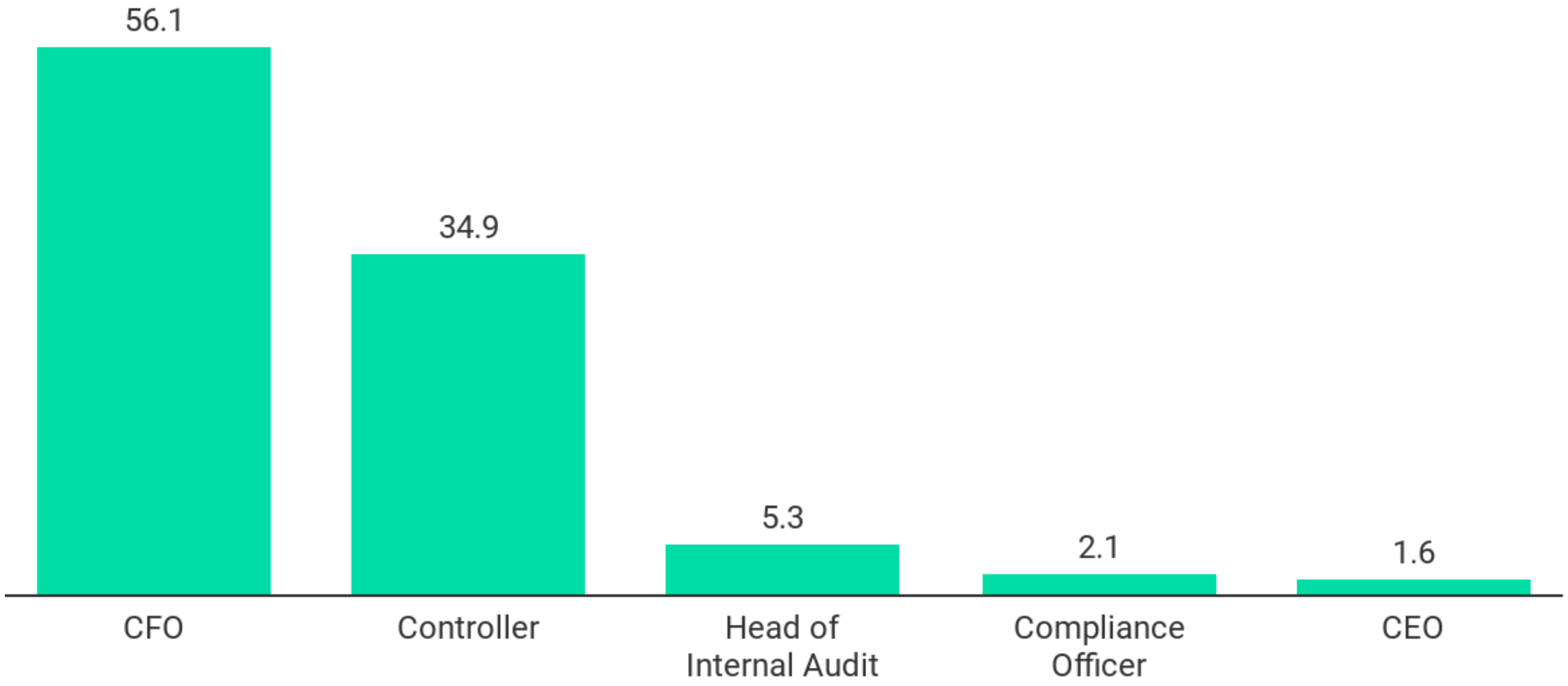
Who owns the ICFR process?

1. CEO
2. CFO
3. Controller
4. Compliance Officer
5. Head of Internal Audit
6. Other

FEI Survey Results

Who Owns ICFR?

While a majority of all respondents to the survey put CFOs squarely in charge of internal controls, it should be noted that a majority of the companies with less than 10,000 employees shifted those ICFR responsibilities to the Controller

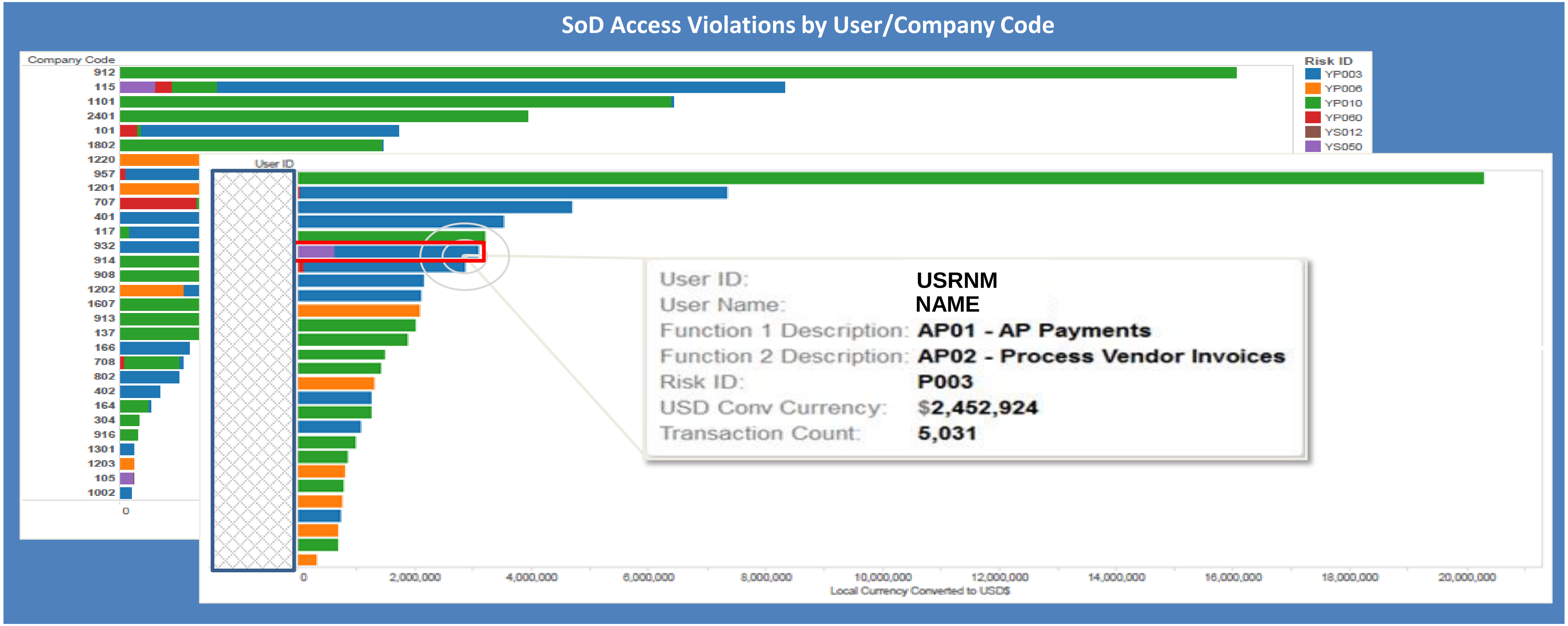


All results in percentages.

Chart: Financial Executives Research Foundation • Get the data • Created with Datawrapper

How Else Can SOD Quantification Be Used?

Utilize dashboards with drill-down functionality to increase visibility and gain control of risk exposure for high volume sites or business groups:

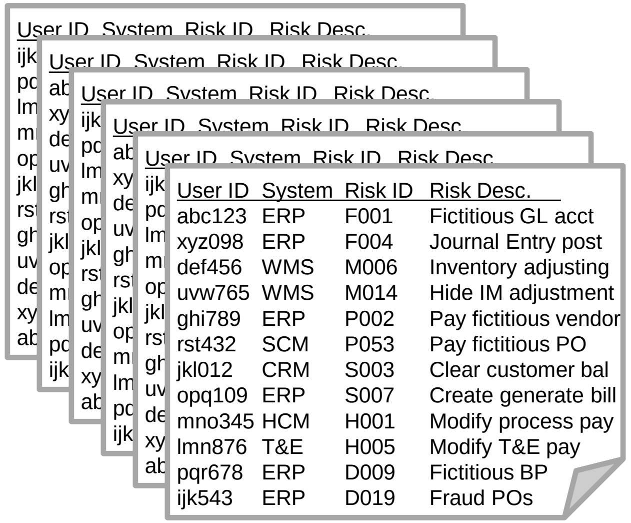


SoD Access Violations by User/Company Code

User ID: USRNM
User Name: NAME
Function 1 Description: AP01 - AP Payments
Function 2 Description: AP02 - Process Vendor Invoices
Risk ID: P003
USD Conv Currency: $2,452,924
Transaction Count: 5,031

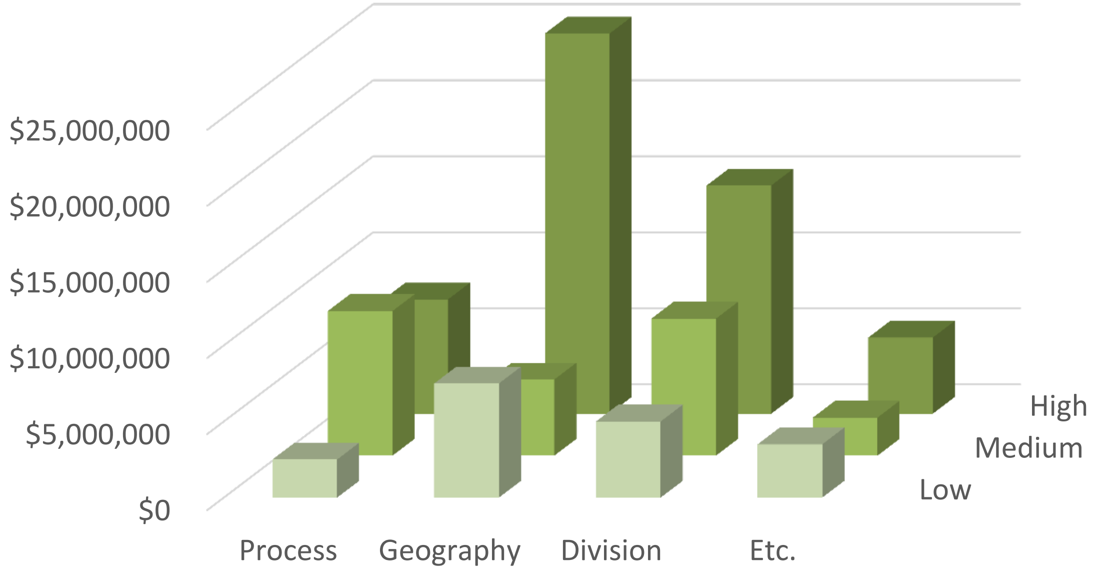
Drive Financially Based Business Decisions that Ensure Significant Return on Investment

Would you rather review potential risks that might occur…



User ID	System	Risk ID	Risk Desc.
abc123	ERP	F001	Fictitious GL acct
xyz098	ERP	F004	Journal Entry post
def456	WMS	M006	Inventory adjusting
uvw765	WMS	M014	Hide IM adjustment
ghi789	ERP	P002	Pay fictitious vendor
rst432	SCM	P053	Pay fictitious PO
jkl012	CRM	S003	Clear customer bal
opq109	ERP	S007	Create generate bill
mno345	HCM	H001	Modify process pay
lmn876	T&E	H005	Modify T&E pay
pqr678	ERP	D009	Fictitious BP
ijk543	ERP	D019	Fraud POs

Or review the impact actual material violations are having on your business?



Knowing the financial impact and business risk exposure let’s you:

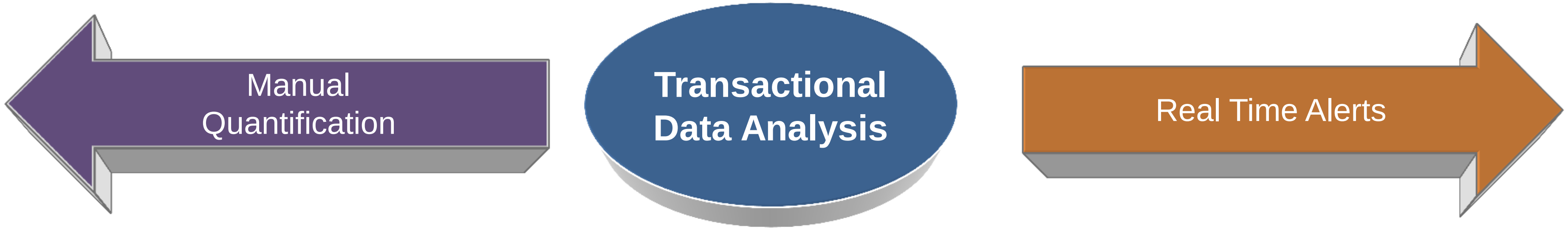
- Focus on the highest risk areas by process, geography, division, etc.
- Report on business issues not compliance failures
- Reduce risk exposure while ensuring audit readiness
- Embed risk and compliance into your business process

SoD Quantification Options

To comprehensively assess SoD violations, companies should evaluate data to identify control or risk issues & search for anomalies:

Historical Data

Future Transactions



Manual Quantification

Transactional Data Analysis

Real Time Alerts

- **Point-in-time assessment (Defined time period)**
- Detect actual SoD Violations
- Multiple point in time assessment tools available

- **Ongoing Review**
- Manage Financial Risk
- Security Remediation
- Focused Audits
- Process Improvements

Analyze All Users, Processes, Transactions and Risks

Analyze all user activity within your end-to-end business process with a solution designed to meet your current (ERP) and future technology (cloud, SaaS, etc.) roadmap

- Make more informed decisions by assessing your financial exposure
- Analyze access risk across organizational elements and business processes

With automation you can:

- Identify and resolve actual risks in your processes based on business and transactional activity
- Monitor direct access to and suspicious activity around PII, financial, and other critical master data
- Correlate administrator and power user activities over time to identify trends and suspicious activity
- Provide visibility and value quantification for financial risks based on user activities

POLL QUESTION

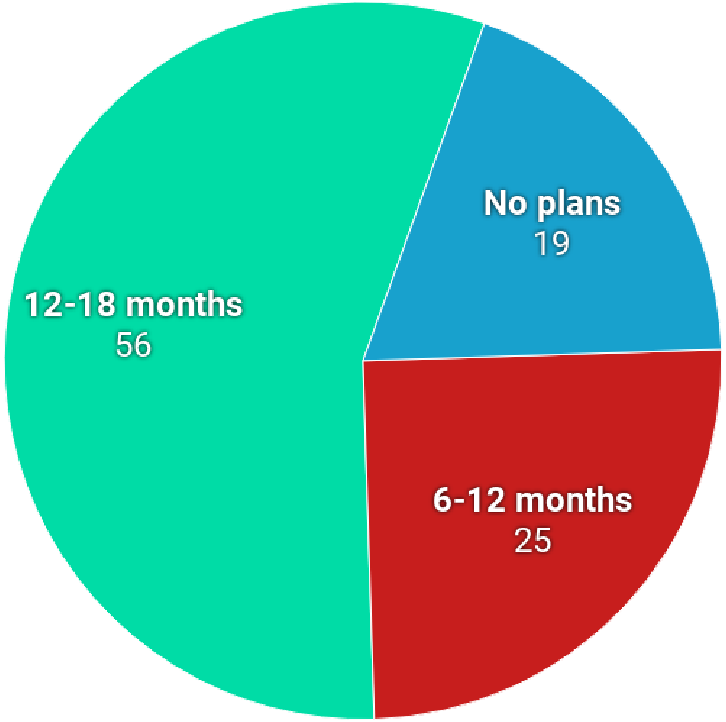
Do you have plans to increase the automation of your internal controls testing?

1. Already fully automated
2. 6-12 months
3. 12-18 months
4. No plans

FEI Survey Results

Big Companies Plan to Automate ICFR ...

Nearly 80% of respondents with 10,000 or more employees said they plan to increase investment in ICFR automation in the next 6-18 months.



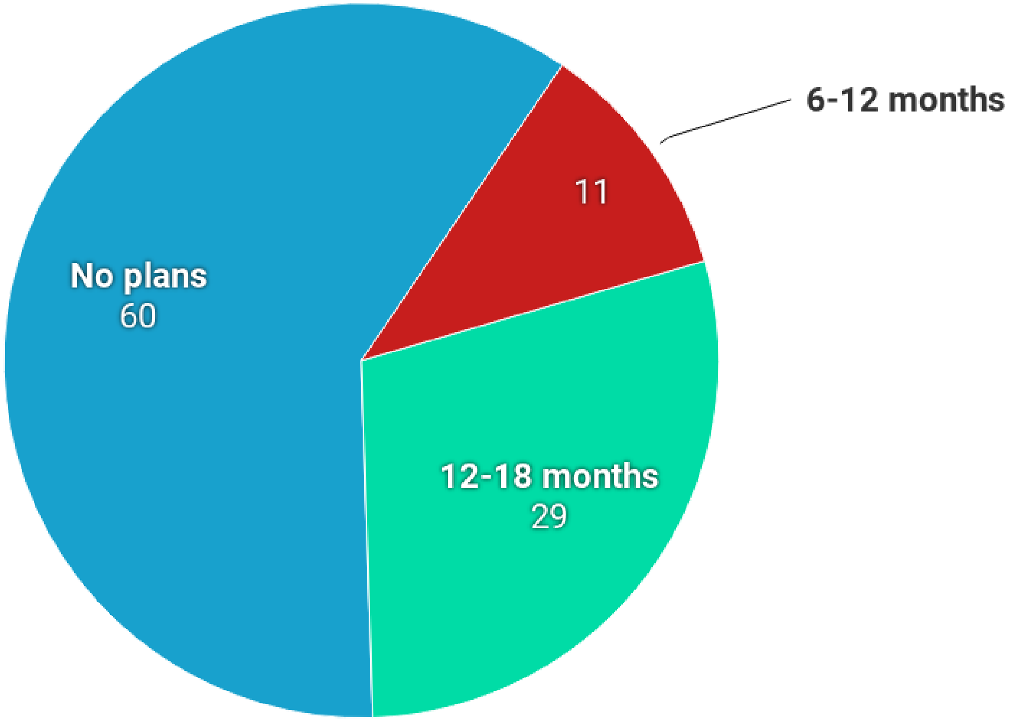
All numbers are percentages

Chart: Financial Executives Research Foundation • Get the data • Created with Datawrapper

FEI Survey Results

... While SMEs Sit On The Technology Sidelines

Three times the number of senior-level financial executives at smaller companies that responded to the survey said they have no plans to automate ICFR.

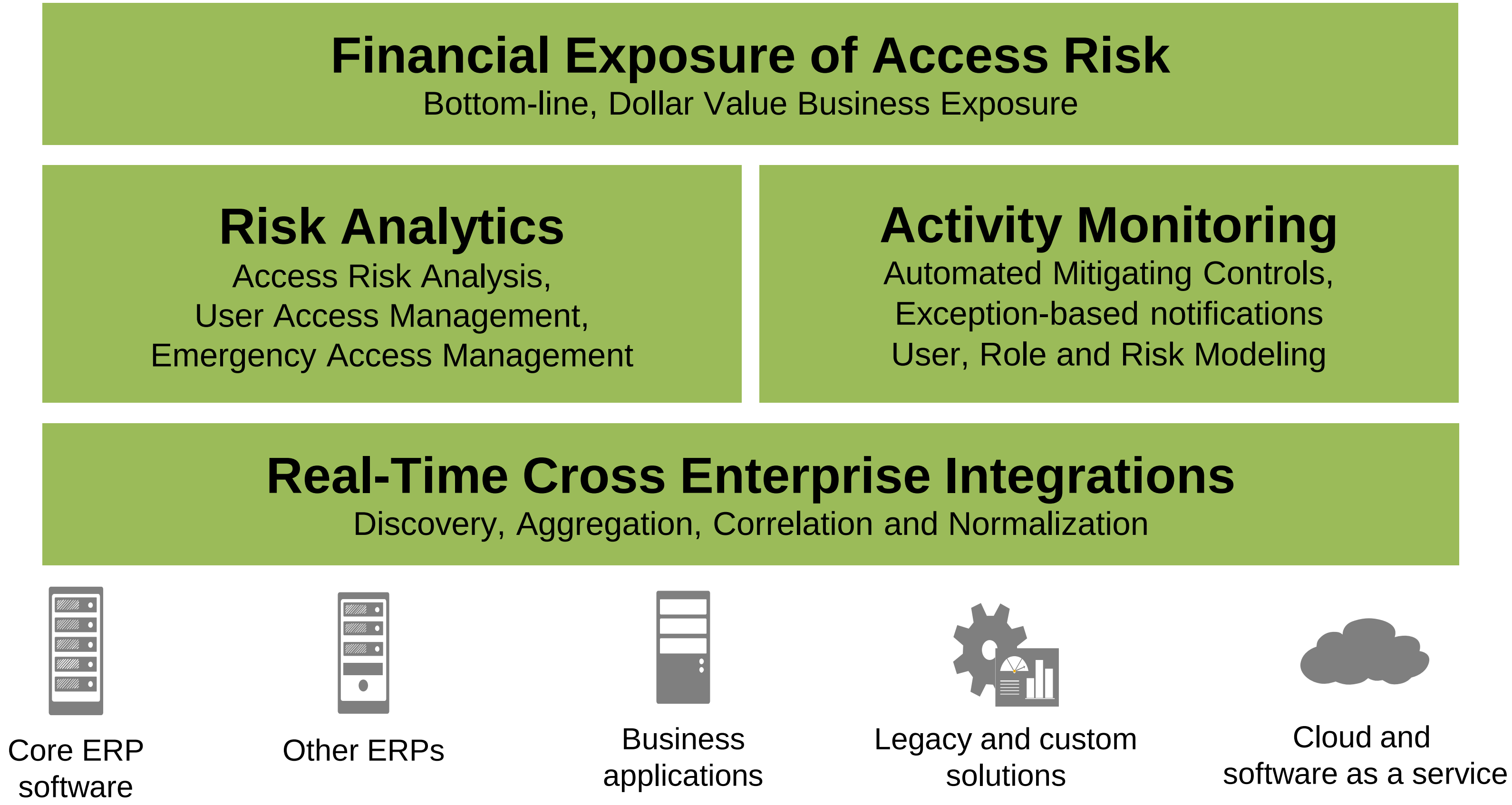


All numbers in percetages.

Chart: Financial Executives Research Foundation • Get the data • Created with Datawrapper

Enterprise Business Controls

Enterprise access governance based on business impact



Financial Exposure of Access Risk
Bottom-line, Dollar Value Business Exposure

Risk Analytics
Access Risk Analysis,
User Access Management,
Emergency Access Management

Activity Monitoring
Automated Mitigating Controls,
Exception-based notifications
User, Role and Risk Modeling

Real-Time Cross Enterprise Integrations
Discovery, Aggregation, Correlation and Normalization

Core ERP software

Other ERPs

Business applications

Legacy and custom solutions

Cloud and software as a service

SAP SAP HANA ARIBA An SAP Company successfactors™ An SAP Company **CRM**

ORACLE® PeopleSoft JDEdwards® Enterprise Software infor Microsoft

Implement Comprehensive Controls Around User Risks

- Manual processes are resource intensive and difficult to monitor and enforce
- Auditors are expecting an end to end control process for SOD mitigation
  - Key business process controls are not effective in managing user access risks
  - Business owners should be monitoring business transactions that are risky based on company policy (SODs / critical access)
- Finance Transformation → Controls & Compliance Transformation
- Focus on value added activities by automating manual controls
- If using manual controls, introduce automation to transform the control process
- Eliminate the need to redesign manual controls

Benefits of Automation & Focus

Out of the box SOD risks

- Benefit by using controls that have been thoroughly tested
- Updates to risks are done via configuration, technical resources are not required

Ability to scale by company, location, system, other

- Ability to apply common rules globally, while allowing localized changes
- Enforces standardized processes by performing controls consistently

Speed up the time of discovery

- Run controls more timely due to ease of use – identify fraudulent activity faster

Compliance scope can extend to other financially relevant business applications

- New business critical applications which are to be included in SOD scope can be included in automated controls
- Additional controls, including cross application monitoring, can be implemented when needed

POLL QUESTION

What percentage of your internal controls testing is automated today?

1. 100%
2. 75%-99%
3. 50%-74%
4. 25%-49%
5. 1%-24%
6. 0%

Implementation Considerations

- Reduce or eliminate the requirement to develop and implement manual control processes to monitor risks
  - Automated controls are executed on a periodic basis (weekly, monthly, quarterly, yearly)
    - Control jobs produce SOD exceptions and there are options for reviews
      - The business owner is notified via email
      - Compliance reviews output
      - Combination can be used to support phased roll out
- All transactional detail is on-line providing audit and management confidence that data is accurate and proves
  - How data was captured
  - Data was not manipulated in spreadsheets
  - Review was completed in a consistent approach across business
  - Reviewers are performing the control
- Reduced time for SOD audits - by both internal and external audit

Automated Controls

> “We were able to reduce the time it took to review our segregation of duties by 94%. Our cycle could run every day if we wanted to.”
>
> *- Head of Information Security*

Company
Global Energy Company

Headquarters (Region)
EMEA

Industry
Energy

Number of Employees
50,000+

Objectives

- Eliminate manual processes required to facilitate monthly reporting across 14 countries
- Improve efficiency that jeopardized financial systems’ performance and consumed a lot of labor resources
- Eliminate audit issues proving to external auditors that risk and compliance reporting was under control

Solution

- Automate legacy SOD processes
- Eliminate highly manual mitigating controls

Benefits

- Reduced business involvement in compliance
- More coverage and visibility of historical data
- Labor savings and reduced auditor fees

1-2 days

New monthly audit cycle time (down 94% from 4-6 weeks)

$1.8M

3 year adjusted cost savings

90%

More coverage in historical data and transactional activity

96%

ROI in first year (12.9 month payback)

Forrester Total Economic Impact Study™ – May 2017

Beyond ERP

> “The synergy frees companies to focus on core business functions. Leveraging innovative solutions like Greenlight allows Sharp to do more and maximize resources.”
>
> *- Wyatt MacManus, Associate Director, Information Security*

Company
Sharp Electronics Corporation

Headquarters (US)
Montvale, New Jersey

Industry
Information Technology & Services

Products & Services
Home electronics, appliances, mobile devices, and business solutions

Number of Employees
15,000+

Website
www.sharpusa.com

Objectives

- Leverage technology to streamline access governance across enterprise applications
- Use automation to standardize GRC processes for all financially relevant business applications
- Contextualize the segregation of duty risk in terms of financial exposure to the business

Solution

- Extend GRC and centralize access governance solution
- Automate SOD controls
- Provide insight into financial exposure of SOD violations

Benefits

- Reduction in manual efforts
- Reduction in external audit costs
- Reallocation of resources in the IT security team

80%

Reduction in IT personnel time required to manage access governance and SOD controls

300 hours

Reduction in time spent per month on SOD control monitoring

33%

Increase in the number of systems managed by GRC

Other Key Business Processes

Procure to Pay

- Configuration
- Master Data
- Procurement
- Goods Receipt Invoice
- Vendor Invoice
- Vendor Payment

General Accounting

- Master Data
- Fixed Asset
- General Ledger Reconciliation
- Journal Entry Processing
- Financial Close

Order to Cash

- Customer Master
- Order Processing
- Sales Invoice Processing
- Account Receivables
- Credit Management

Inventory Management

- Item Master
- Physical Inventory
- Inventory Transactions

Human Resource

- Master Data
- Employee Management
- Benefit Administration
- Payroll

Time & Expenses

- Expense Reports
- Duplicate Expenses
- Expense Approvals
- Cash Advances
- Receipts

Greenlight Monitors Millions of Users & Billions of Transactions

smiths medical
AXA
Pfizer
POLO RALPH LAUREN
HEINEKEN
NBCUniversal
Santander
SANOFI
CITRIX
SHARP
Olin
SOUTHERN CALIFORNIA EDISON
Microsoft
bp
Loblaws
BBVA Compass
PG&E
Pacific Gas and Electric Company
Chevron
GM
Microsoft
Aflac
JABIL
Johnson Controls
IBM
TATA
nationalgrid
COACH NEW YORK
U.S. DEPARTMENT OF THE INTERIOR
Hanes
NewellRubbermaid
Joburg
ca technologies
eDF
MAPLE LEAF
ARKEMA
PHILIPS
Unilever
SPIRIT AEROSYSTEMS
MAERSK LINE
RELIANCE Capital
DEFENSE LOGISTICS AGENCY
WARNACO
Shell
BBC
Statoil
elster
AICL Where needs take us
BRIDGESTONE
FPL
AMGEN
PEARSON
UNISYS

Thank You

Learn more at www.greenlightcorp.com