Analyzing First Quarter Material Weakness Disclosures

April 2019

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

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 ✉

REUTERS

"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. **A Deeper Dive into the FERF / Greenlight ICFR Tracker**

2. **A Deeper Dive into Internal Controls over Financial Reporting (ICFR)**

3. **"Material Weakness" vs. "Significant Deficiency"**

4. **Technology & Automation – Potential Risks vs. Actual Violations**

5. **Business & Financial Impact**

6. **Customer Use Cases Examples**

About Greenlight

Company
- ✓ Founded 2007; Headquarters Flemington NJ

Partnerships
- ✓ SAP Solution Extension

SAP® Certified

- ✓ Oracle Platinum Partner

ORACLE® Platinum Partner

- ✓ FEI Strategic Partner **fei.**

Awards & Recognition
- ✓ Best Big Data Solution using SAP HANA

BIG DATA AWARD

- ✓ Highest Possible Rating in Gartner Marketscope

Gartner®

Greenlight enables businesses to assess, manage and reduce risk for Financial Controls, Regulatory Compliance, and Application Security

FERF / Greenlight ICFR Tracker

As part of the Financial Education & Research Foundation and Greenlight Technologies' ongoing research into ICFR, we have created a program to automatically review all quarterly public filings and highlight those companies that have reported a material weakness.

After each quarter, we will provide you with this analysis as we look for trends over time, key issues that companies face and best practices to help with your reporting efforts.

Key takeaway: An effective system of ICFR can significantly reduce the risk of misstatements and inaccuracies in your company's financial statements.
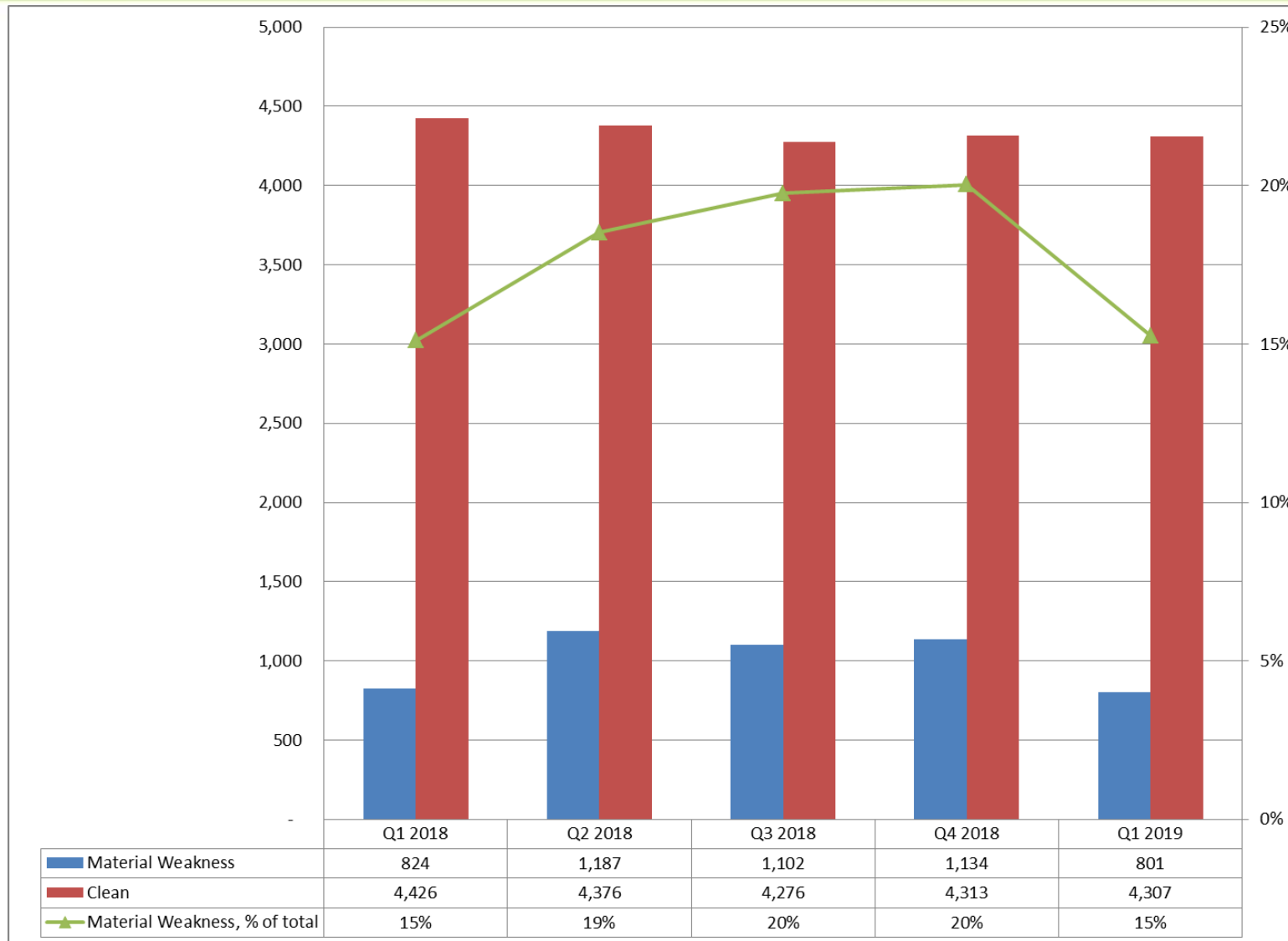
Greenlight consolidates information from publicly available authoritative data sources reasonably believed by Greenlight to be reliable and accurate at the time of providing the information.
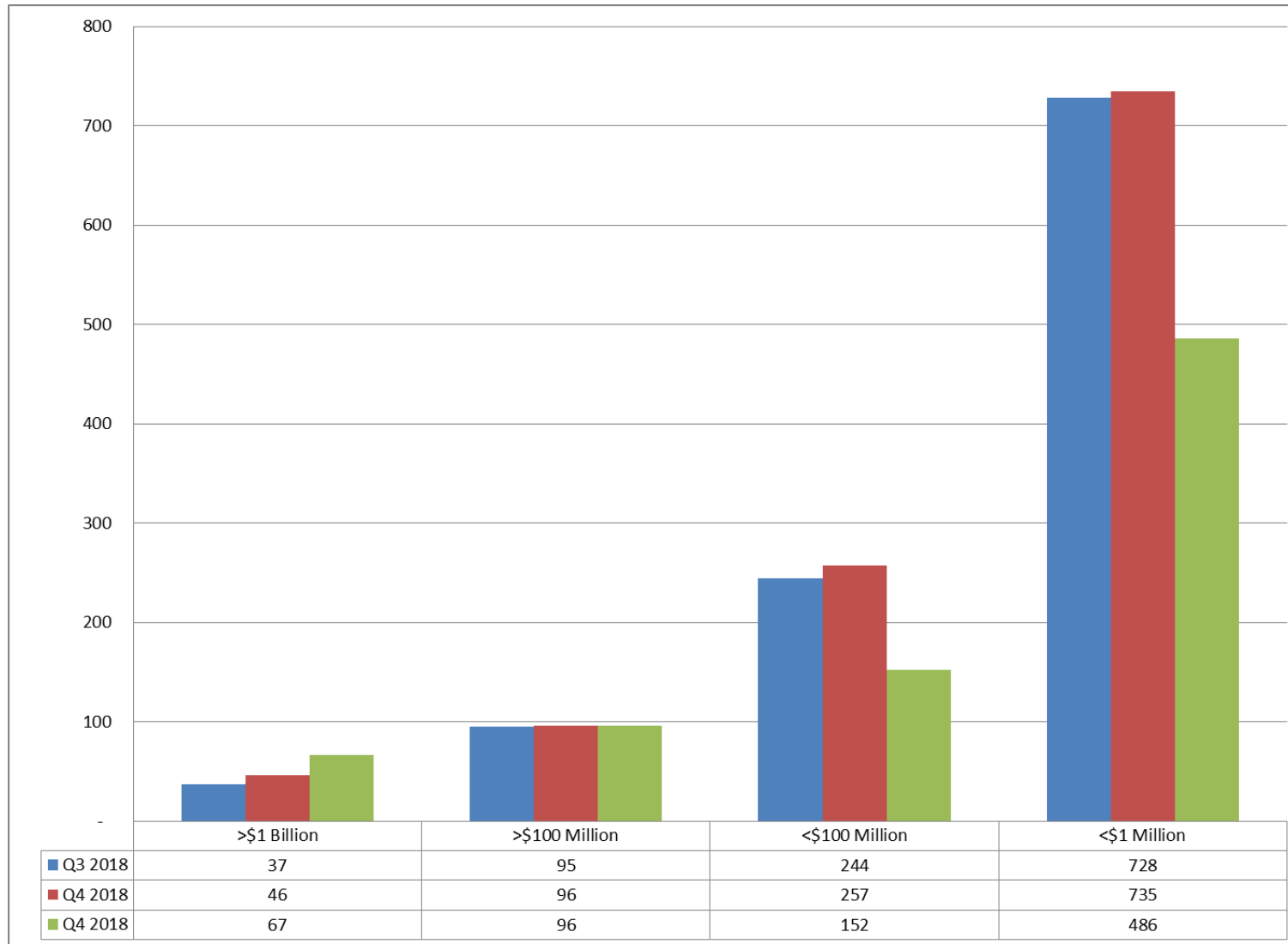
ICFR Tracker Overview

- All SEC filings in EDGAR were analyzed for terms related to 'Material Weakness', 'Remediation', 'Significant Deficiency', etc. in relevant sections of 10-K and 10-Q filings

- Selected filings indicates high probability of Material Weakness (>95% confidence)

- Some Companies filed more than once during the quarter – e.g. 10-K then 10-KA; 10-K then 10-Q. These 'Duplicate' names are tracked to see number of unique Companies filing each quarter.

- Revenue values were correlated when available to stratify the filings to focus on large companies

- Companies are the tracked to see, new filings, how long the disclosure continues, type of weakness (RevRec, Leases, Taxes, IT Controls, SOX/SOD, etc.)

Disclosures of Material Weakness to SEC

	Q1 2018	Q2 2018	Q3 2018	Q4 2018	Q1 2019
Material Weakness	824	1,187	1,102	1,134	801
Clean	4,426	4,376	4,276	4,313	4,307
Material Weakness, % of total	15%	19%	20%	20%	15%

Source: SEC EDGAR filings – Q1 2018 – Q1 2019

Increase in >$1 Billion Revenue Companies

	>$1 Billion	>$100 Million	<$100 Million	<$1 Million
Q3 2018	37	95	244	728
Q4 2018	46	96	257	735
Q4 2018	67	96	152	486

Source: SEC EDGAR filings – Q3 2018 – Q1 2019

Example – Top 20 by Revenue

Disclosure Text	Type	Date	Link	Estimated Revenue	Company Name	CIK
Item 4—Controls an	10-Q	3/13/2019	https://www.sec.gov/	$141,576,000,000	COSTCO WHOLESALE CORP /NEW	909832
Item. ITEM 4 CONTR	10-Q	2/13/2019	https://www.sec.gov/	$ 34,055,000,000	AIS Holdings Group, Inc.	1702015
ITEM 4. CONTROLS	10-Q	1/10/2019	https://www.sec.gov/	$ 32,037,426,000	CHS INC	823277
ITEM 9A. CONTROLS	10-K	3/11/2019	https://www.sec.gov/	$ 23,443,000,000	CENTURYLINK, INC	18926
Item 9A.Controls an	10-K	3/1/2019	https://www.sec.gov/	$ 20,758,000,000	MARRIOTT INTERNATIONAL INC /MD/	1048286
ITEM 9A. CONTROLS	10-K	2/25/2019	https://www.sec.gov/	$ 18,735,073,000	GENUINE PARTS CO	40987
Item 9A. Controls ar	10-K	2/28/2019	https://www.sec.gov/	$ 14,070,000,000	Qurate Retail, Inc.	1355096
Item 9A. Controls ar	10-K	2/28/2019	https://www.sec.gov/	$ 14,070,000,000	QVC INC	1254699
ITEM 9A. CONTROLS	10-K	3/11/2019	https://www.sec.gov/	$ 12,552,900,000	TechnipFMC plc	1681459
Item 9A CONTROLS	10-K	3/8/2019	https://www.sec.gov/	$ 12,078,000,000	AXA Equitable Holdings, Inc.	1333986
Item 9A CONTROLS	10-K	3/28/2019	https://www.sec.gov/	$ 12,078,000,000	AXA EQUITABLE LIFE INSURANCE CO	727920
ITEM 9A. CONTROLS	10-K	2/12/2019	https://www.sec.gov/	$ 10,769,600,000	MOLSON COORS BREWING CO	24545
ITEM 9A. CONTROLS	10-K	3/4/2019	https://www.sec.gov/	$ 8,630,900,000	NEWELL BRANDS INC	814453
Item 4. Controls and	10-Q	2/7/2019	https://www.sec.gov/	$ 7,110,130,000	SANMINA CORP	897723
Item 9A. Controls ar	10-K	2/27/2019	https://www.sec.gov/	$ 6,543,000,000	Athene Holding Ltd	1527469
ITEM 9A. CONTROLS	10-K	2/13/2019	https://www.sec.gov/	$ 6,023,000,000	GRAPHIC PACKAGING HOLDING CO	1408075
ITEM 9A. CONTROLS	10-K	3/18/2019	https://www.sec.gov/	$ 5,492,524,000	Diplomat Pharmacy, Inc.	1610092
ITEM 9A. Controls a	10-K	3/15/2019	https://www.sec.gov/	$ 4,792,017,000	Camping World Holdings, Inc.	1669779
ITEM 9A: CONTROLS	10-K	3/1/2019	https://www.sec.gov/	$ 4,578,600,000	DIEBOLD NIXDORF, Inc	28823
Item 9A. Controls ar	10-K	3/18/2019	https://www.sec.gov/	$ 4,390,116,000	Syneos Health, Inc.	1610950
Item 9A - Controls a	10-K	3/1/2019	https://www.sec.gov/	$ 4,346,703,000	JELD-WEN Holding, Inc.	1674335
Item 9A.CONTROLS	10-K	2/21/2019	https://www.sec.gov/	$ 3,590,000,000	Liberty Latin America Ltd.	1712184

Source: SEC EDGAR filings – Q1 2019; other sources for revenue estimates

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)

Polling Question #1

Who owns the ICFR process in your organization?

A. CEO

B. CFO

C. Controller

D. Compliance Officer

E. Head of Internal Audit

F. Other/ N/A

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

What is a "deficiency" in ICFR?

A **"deficiency in design"** exists when:

- a control necessary to meet the control objective is missing

- an existing control is not properly designed so that, even if the control operates as designed, the control objective would not be met

A **"deficiency in operation"** exists when

- a properly designed control does not operate as designed

- when the person performing the control does not possess the necessary authority or qualifications to perform the control effectively
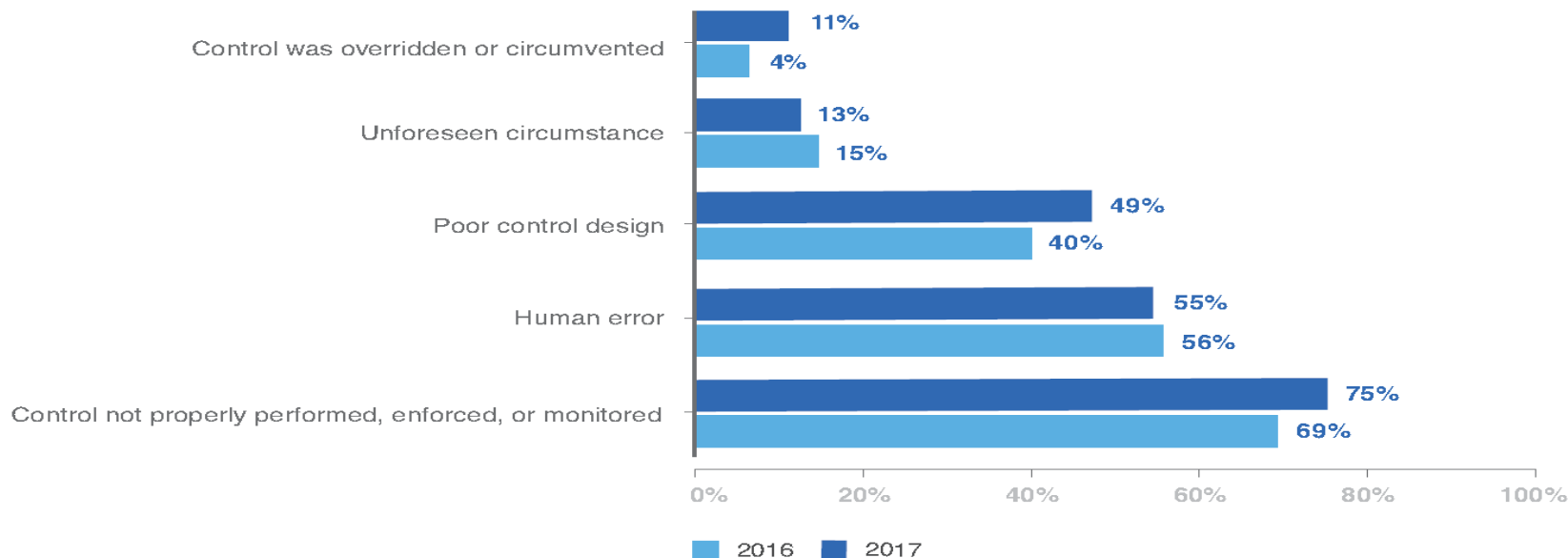
A **"significant deficiency"** is a deficiency that is less severe than a material weakness yet important enough to merit attention by those responsible for oversight of the company's financial reporting

Internal Control Failures on the Rise

Per the *2017 State of the SOX/Internal Controls Market Survey*, there was a 9 percent increase in the number of respondents that reported internal control failures compared to the previous year.

The most cited cause was "Control not properly performed, enforced, or monitored" (increased by 6%)

Cause	2016	2017
Control was overridden or circumvented	4%	11%
Unforeseen circumstance	15%	13%
Poor control design	40%	49%
Human error	56%	55%
Control not properly performed, enforced, or monitored	69%	75%

Legend: 2016, 2017

Source: SOX & Internal Controls Professionals Group, Moss Adams LLP, and Workiva

How can you have a "clean" audit of financial statements, but disclose one or more material weaknesses in ICFR?

While the audit of financial statements may be "clean," this provides little information to those outside the company as to whether other financial information is reliability

One of the key purposes of SOX 404 is to provide this additional information to market participants. Specifically, the ICFR audit report provides the public with a barometer against which to evaluate the reliability of a company's disclosed financial information

Polling Question #2

Is your organization subject to SOX?

A. Yes, large accelerated filer

B. Yes, accelerated filer

C. Yes, non-accelerated filer

D. No, privately held company

E. No, Other

Recent Example

<u>Costco Warns of Material Weakness in Controls</u>
The warning related to IT systems that "support the company's financial reporting processes" drove Costco's stock down 2.4%.

October 5, 2018 | CFO.com

"The weakness relates to **general information technology controls** in the areas of user access and program change-management over certain information technology systems that support the company's financial reporting processes," Costco said. "The access issues relate to the extent of **privileges afforded users authorized to access company systems**."

Remediation efforts have begun, according to Costco, but the material weakness will **not be considered remediated** until "management has concluded, **through testing**, that [the applicable] controls are operating effectively."

Challenges

"Getting Clean" can be a challenge

- Focus typically based on highest number of violations vs. impact to the business
- Not all SoD's will be removed due to business requirements

Internal controls typically requires a lot of manual effort to mitigate violations and to manage audit reporting requirements:

- Mostly manual controls
- No ability to manage by exception and identify fraud
- Lack of visibility to true financial exposure

Business processes increasingly moving outside of ERP

- Non-ERP applications such as Business Planning & Consolidation, Master Data Management, etc.
- Cloud based applications such as Ariba, SuccessFactors, Salesforce, Workday, etc.
- Legacy, custom and homegrown applications

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

Customer Example #1

Customer Example:

- Fortune 500 company
  - \>15,000 employees worldwide
  - ERP Instance: SAP ECC

- Reported Material Weaknesses in 10-K

- Audit Issue: Not able to identify SoD conflicts for mitigation and document where conflicts originated and how they were resolved.

Mark Kissman

CFO, Greenlight Technologies
(Former CFO of multiple public & private technology companies)

mkissman@greenlightcorp.com

Customer Example #2

Customer Example:

- Fortune Global 100 company
  - \>50,000 employees worldwide
  - ERP Instances: SAP (5) and JDE (28)

- Project Objectives include moving from SAP/JDE to SAP S4 in the Cloud
  - Also includes moving Procurement from SAP/JDE to SAP Ariba in the Cloud

- Audit Issue: How to monitor and test internal controls across SAP/JDE/Ariba processes

Control Automation Project (CAP) Opportunity

- There is an opportunity to simplify the process used to validate activity. The current process, while not broken, is inefficient with a lot of manual control reporting.

- The project will evaluate control monitoring and reporting software.

  – This software extends the capability of the SAP GRC Access Control currently used today for SAP and JDE User Access Reviews and SOD Conflict reporting.

  – Through control automation, it can reduce the need for organizations to manually run compensating control reports for individuals with SOD conflicts and may provide additional fraud protection.

CAP Fit with Overall System Transformation Initiative

CAP will allow process simplification now and provide uninterrupted transition to S4

Opportunity statement:

Develop an Information Technology strategy, determine the target architecture framework, and define the company's digital core to position Company to fully leverage technology advances and guide the replacement of soon-to-be obsolete systems.

Success vision:

- No business interruption from obsolescence of current systems or during transition to new systems

- Create competitive advantage through quick and easy access to critical information via improved systems of record. This will enable more informed business decisions and streamlined processes to meet changing business information needs.

- Serve as a foundation for Company to capitalize on the fourth industrial revolution; leverage rapidly transforming technologies like cloud, mobile, analytics and artificial intelligence (e.g., machine learning).

Transformation Initiatives Guiding Principles

CAP will allow end to end processes across Compliance, Procurement and ERP

Simplify now to drive global compliance and financial risk processes

Quantifying Value of Risk has 12 month or less payback

Use a business-driven, enterprise approach

- Company's business strategy will drive the strategy.
- Focus first on complete value streams / end-to end-processes (vs. focusing on opcos or functions).
- Govern the program as an enterprise initiative.

Eliminate, simplify, standardize and automate

- Emphasize elimination and simplification before standardization. Standardize to drive efficiency and compliance with the digital core. Functions will own global processes and drive standardization for core business processes and data.
- Validate localization to address legal, fiscal or regulatory requirements and allow localization where necessary. Understand the risk and exposure to make informed decisions.

Plan for the long-term

- Leverage internal employees both for program leadership and for opportunities to build organizational capability. Use third-party consulting for key advisory roles and program continuity.
- Build solution to be scalable and to allow for agility & innovation.
- Maintain control of our destiny (i.e., not dictated by software providers).
- Protect our business interest by implementing a value-driven solution.

Transformation Initiative Benefits

Listed below are the current items in scope and the expected program benefits.

In-scope value streams:

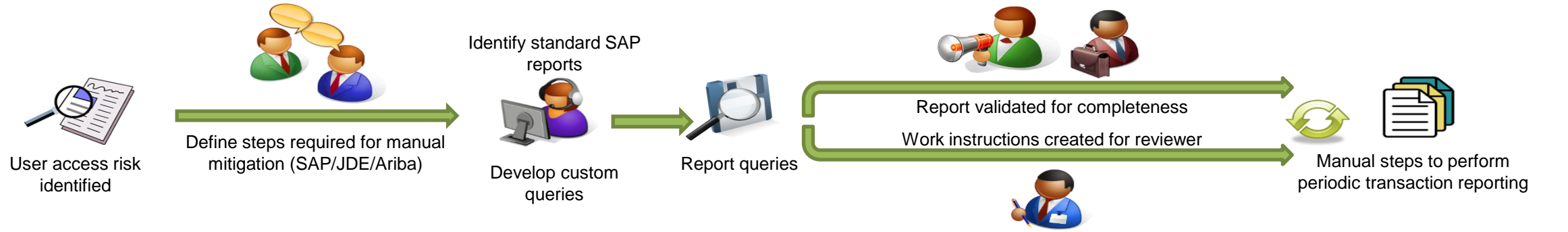|		
• Asset lifecycle	• Customer lifecycle	• Source to Pay
• Commodity to market	• Liquidity and risk management	• Recruitment to retirement
• Product lifecycle	• Financial booking to reporting	• Integrated business planning

Expected program benefits:

- Greater agility and flexibility – respond rapidly to internal and external needs to maximize value for the organization

- Powerful analytics – make timely decisions and develop insights to enjoy first-move advantage

- Process simplification and data foundation – streamlined enterprise processes and common systems of record

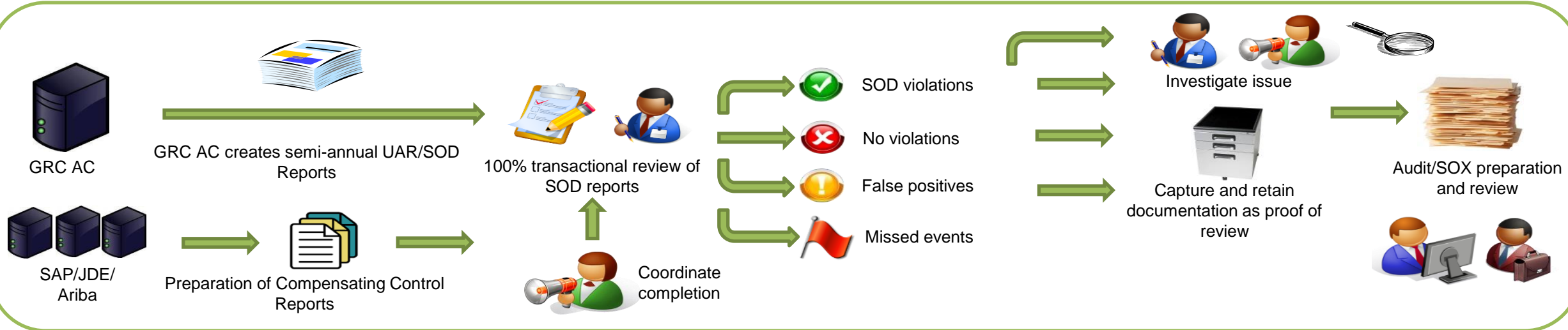- New and improved capabilities for financial information

Financial Value will enable more accurate risk profile
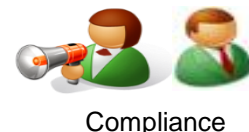
Current Internal Controls Process

Manual Mitigating Controls – Defining

User access risk identified → Define steps required for manual mitigation (SAP/JDE/Ariba) → Identify standard SAP reports / Develop custom queries → Report queries →

Report validated for completeness
Work instructions created for reviewer

→ Manual steps to perform periodic transaction reporting

Manual Mitigating Controls – Monitoring

GRC AC → GRC AC creates semi-annual UAR/SOD Reports → 100% transactional review of SOD reports

SAP/JDE/Ariba → Preparation of Compensating Control Reports →

Coordinate completion

- SOD violations
- No violations
- False positives
- Missed events

→ Investigate issue

→ Capture and retain documentation as proof of review

→ Audit/SOX preparation and review

Legend:

Assessor   IT Support   Compliance   Audit   Reviewer

Moving to Greenlight: What Changes?

GRC AC

SAP/JDE/Ariba

AVM creates with GRC AC SOD Reports
GRC AC creates semi-annual UAR/SOD Reports

AVM queries target systems to identify SOD transactions
Preparation of Compensating Control Reports

100% transactional review of SOD reports
100% transactional review of transaction logging and data correlation across SOD events

Coordinate completion

SOD violations

No violations

False positives

Missed events

Email notification

Investigate issue

Proof maintained in AVM
Capture and retain documentation as proof of review

Findings stored for Audit/SOX preparation and review
Audit/SOX preparation and review

Goes away	Manual preparation of SOD reports	False positives or missed events	Retain proof of review	Compliance oversight	Audit preparation effort
Replace with AVM	AVM syncs w/ GRC Access Control Automated controls check for exceptions by Risk	AVM controls are configured to review all transactions and capture only actual violations	Record of control execution is maintained online in AVM	Real-time notifications delivered to Supervisor to initiate review	Evidence of review (e.g., comments, attachments) available online

Legend:

Assessor

IT Support

Compliance

Audit
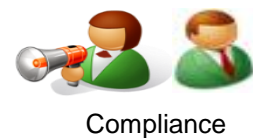
Reviewer

Project results: key takeaways

AVM Process: Supervisor SOD Review UAT

→ *Standardize and gain visibility to the SOD Review process*

- SOD review process in AVM requires the same or less effort than the current process, and allows for a more thorough review process, while reducing the number of tools used.
- Estimated total of 46-57 hours spent per year performing current SOD reviews (15 supervisors / 5 in-scope risks). Estimated time savings using AVM between 30%-50%.

Reviewer

Current Process: Preparing System Reports for Compensating Controls:

→ *Automate and centralize SOD risk exception reporting*

- Estimated total of 18 hours/year preparing reports for the five in-scope risk IDs across in-scope BUs Americas/Downstream, Brazil/Upstream, and FSS (4 report preparers).

Report Creation

Current Process: Internal Controls Activities

→ *Reduce Internal Controls time commitment to SOD activities*

- Internal Controls SOD SME committed ~80% of their time supporting X control processes and acting as liaison between PWC during the annual audit. With AVM, time spent managing the external audit of control could be reduced from estimated 3.5 months to 1 month.
- PWC estimates approximately 187 hours auditing control X per year today. With AVM, PWC expects less ongoing audit hours. However, there would be initial cost in auditing the setup of AVM.
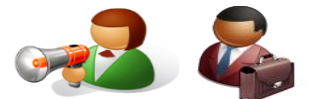
Compliance / Audit
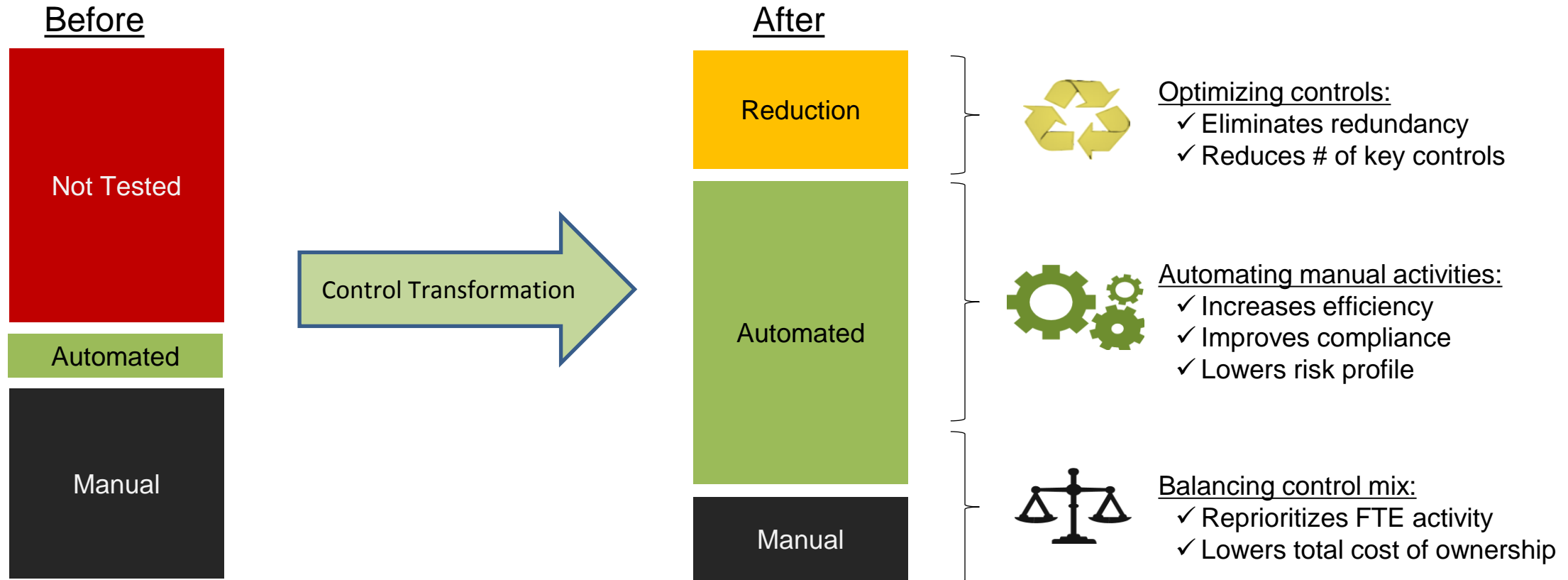
Scope of Deployment

- 51 ERP Systems
  - 5 SAP
  - 28 JDE
  - 14 Ariba-JDE cross-over
  - 4 Ariba-SAP crossover

- 47 SoD Risk Conflicts
  - 34 SAP
  - 8 JDE
  - 3 Ariba-JDE cross-over
  - 2 Ariba-SAP crossover

RISKID	RISKID description	ERP
FI01	Adjust owner interest calculation and Create/change PRA manual journal entries	SAP
FI02	Create/change PRA manual journal entries and Approve PRA manual journal entries	SAP
FI03	Generate manual royalty check and Create/change PRA manual journal entries	SAP
OC01	Maintain customer master data and Maintain customer credit master data	SAP
OC02	Maintain customer master data and Process sales order	SAP
OC03	Maintain customer master data and Asset posting to a vendor/customer account	SAP
OC04	Maintain customer master data and Post customer cash call	SAP
OC05	Maintain customer master data and Process customer invoice/credit	SAP
OC06	Maintain customer master data and Post customer down-payment	SAP
OC07	Maintain customer master data and Clear customer down-payment	SAP
OC08	Maintain customer master data and Process incoming payments	SAP
OC09	Maintain sales deal and Process sales order	SAP
OC10	Maintain SD pricing condition records and Process sales order	SAP
PP01	Maintain vendor master data and Release requisition	SAP
PP02	Maintain vendor master data and Release PO	SAP
PP03	Maintain vendor master data and Process PO no release (DT)	SAP
PP04	Maintain vendor master data and Process PO no release (DT/POrg)	SAP
PP05	Maintain vendor master data and Asset posting to a vendor/customer account	SAP
PP06	Maintain vendor master data and Process vendor invoice/credit	SAP
PP07	Maintain vendor master data and Create vendor down-payment request	SAP
PP08	Maintain vendor master data and Create vendor cash call advance request	SAP
PP09	Maintain vendor master data and Post vendor down-payment	SAP
PP10	Maintain vendor master data and Clear vendor down-payment	SAP
PP11	Release requisition and Process goods/service receipt	SAP

RISKID	RISKID description	ERP
PP11	Release requisition and Process goods/service receipt	SAP
PP12	Release PO and Process goods/service receipt	SAP
PP13	Process PO no release (DT) and Process goods/service receipt	SAP
PP14	Process PO no release (DT/POrg) and Process goods/service receipt	SAP
PP15	Process a PM External Order and Requisition and Process goods/service receipt	SAP
PP16	Release requisition and Process vendor invoice/credit	SAP
PP17	Release PO and Process vendor invoice/credit	SAP
PP18	Process PO no release (DT) and Process vendor invoice/credit	SAP
PP19	Process PO no release (DT/POrg) and Process vendor invoice/credit	SAP
PP20	Process a PM External Order and Requisition and Process vendor invoice/credit	SAP
PP21	Maintain customer master data, Maintain vendor master data and Post JV/FI documents	SAP
X001	Maintain vendor master data and Release requisition	SAP/Ariba
X002	Release requisition and Process goods/service receipt	SAP/Ariba
JR01	Maintain vendor master data and Approve Expenditure	JDE
JR02	Maintain vendor master data and Process vendor invoice/credit	JDE
JR03	Approve Expenditure and Process vendor invoice/credit	JDE
JR04	Approve Expenditure and Acknowledge receipt of goods/services	JDE
JR05	Approve Expenditure and Maintain approvals	JDE
JR07	Maintain customer master data and Process sales order	JDE
JR08	Maintain customer master data and Process customer invoice/credit	JDE
JR09	Maintain sales deal/pricing and Process sales order	JDE
JX01	Maintain vendor master data (JMVD) and Release requisition(ARIBA)	JDE/Ariba
JX02	Acknowledge receipt of goods/services (JPGR) and Release requisition(ARIBA)	JDE/Ariba
JX03	Process vendor invoice/credit (JPVI) and Release requisition(ARIBA)	JDE/Ariba

Control Automation and Monitoring

Before

After

Not Tested

Automated

Manual

Control Transformation

Reduction

Automated

Manual

Optimizing controls:
- ✓ Eliminates redundancy
- ✓ Reduces # of key controls

Automating manual activities:
- ✓ Increases efficiency
- ✓ Improves compliance
- ✓ Lowers risk profile

Balancing control mix:
- ✓ Reprioritizes FTE activity
- ✓ Lowers total cost of ownership

Incorporating continuous control monitoring helps companies increase audit coverage and standardize review process while reducing compliance and operational cost.

Polling Question #3

What are your plans to automate your internal controls testing?

A. Already automated

B. Significant plans

C. Moderate plans

D. No plans

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
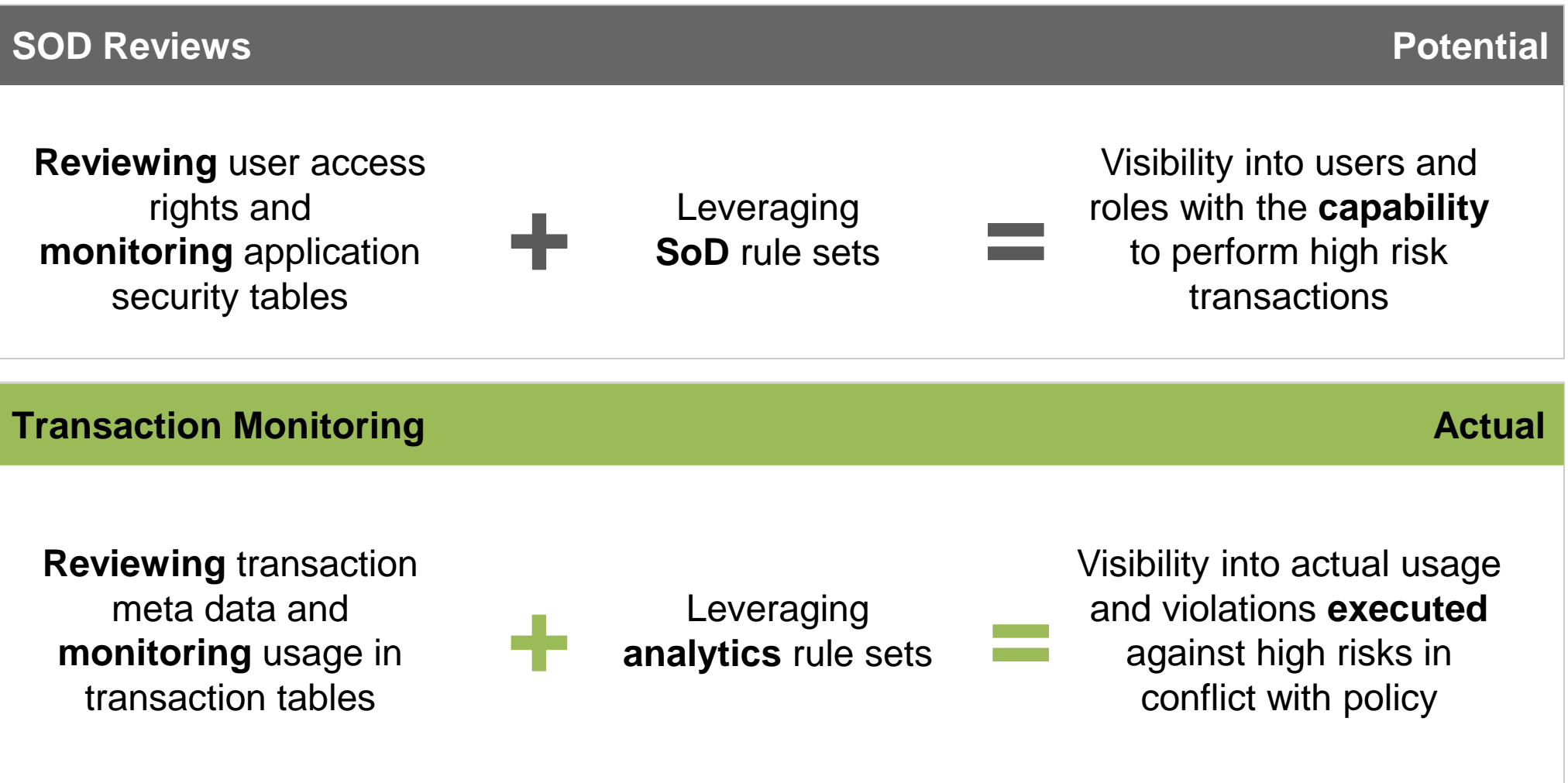- Duplicate Expenses
- Expense Approvals
- Cash Advances
- Receipts

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

Financial Impact & Risk Quantification

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

Potential to Perform

Risk	Risk Description	Business Process	Conflicts reported from User Access		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	24	2,916	0	0	$0
P001	Maintain a fictitious vendor and enter a vendor invoice for automatic payment	Purchasing and Payables	31	3,383	4	9	$493,108

Actually happened

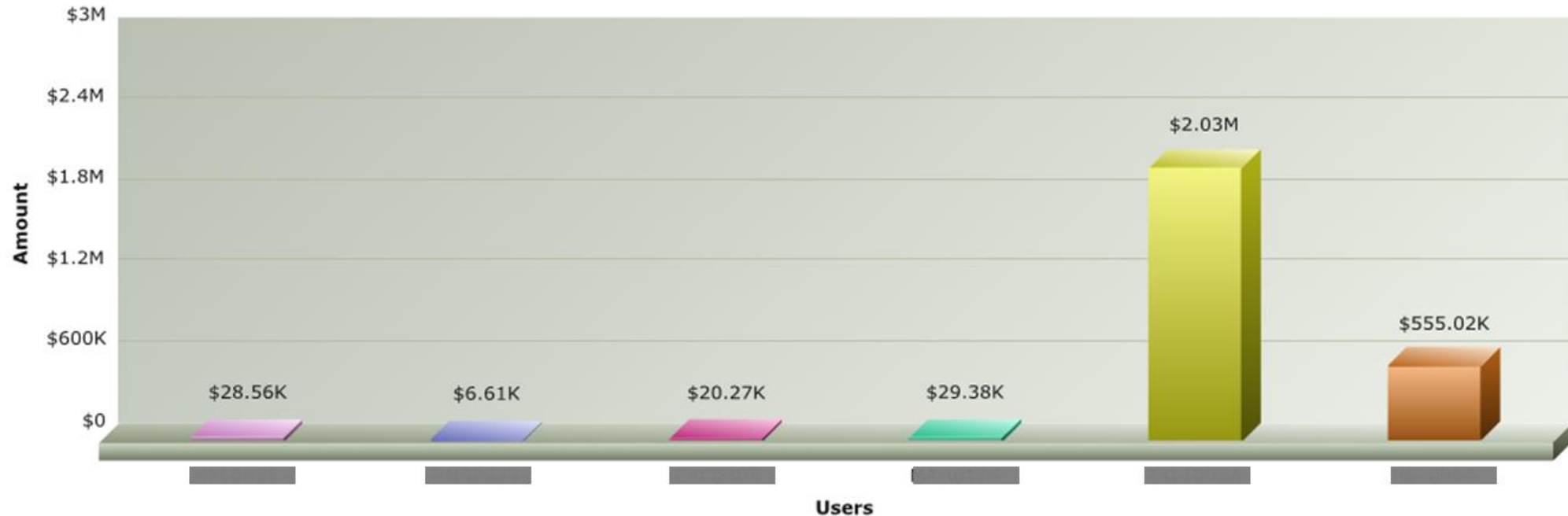# Customer Example: Invoicing & Processing Payments
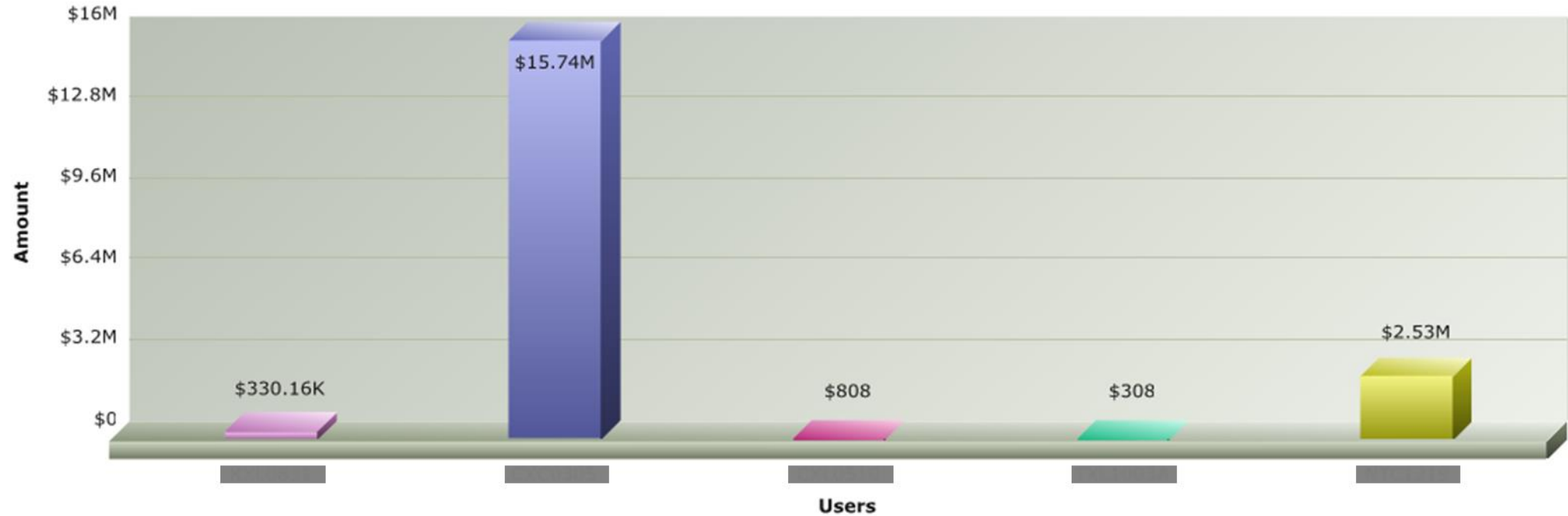
140 users are reported by a GRC solution to have the authorizations to perform the risk

5 users are flagged after 100% transaction monitoring

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

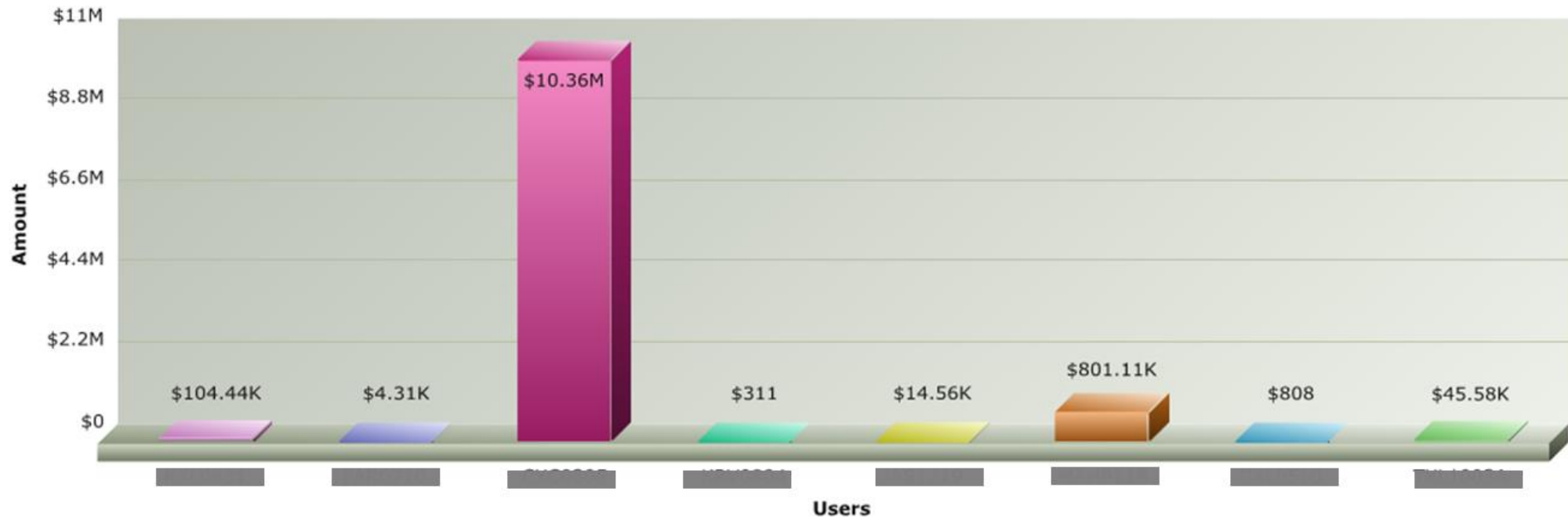# Customer Example: Credit Memo & Clear Balance

72 users are reported by a GRC solution to have the authorizations to perform the risk

6 users are flagged after 100% transaction monitoring

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: Invoicing & Clear Balances

76 users are reported by a GRC solution to have the authorizations to perform the risk

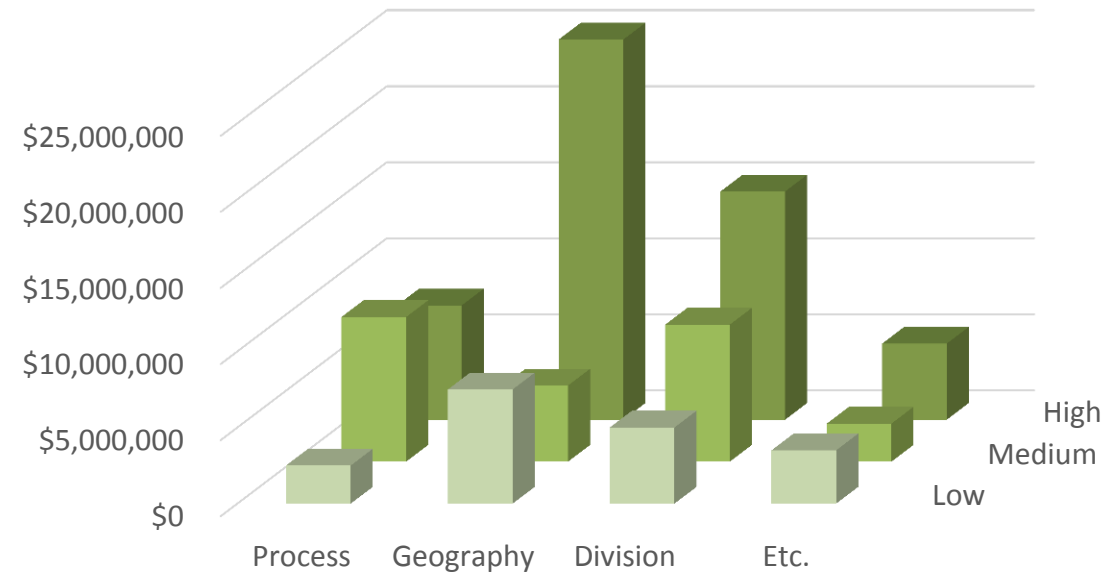**8 users** are flagged after 100% transaction monitoring

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

Would you rather review potential risks that might occur…

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

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

A financial impact assessment 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

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

Polling Question #4

What percentage of ICFR relevant business process applications are in the cloud?

A. 100%

B. 75%-99%

C. 50%-74%

D. 25%-49%

E. 1%-24%

F. 0%

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

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 it 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 in scope for Governance, Risk & Compliance

Greenlight Monitors Millions of Users & Billions of Transactions

Thank You

Learn more at www.greenlightcorp.com