Greenlight TECHNOLOGIES

A Financial Executive's Guide to ICFR Changes, Trends & Best Practices

May 2018

A Financial Executive's Guide to ICFR Changes, Trends & Best Practices

Ponemon Institute found that 57% of organizations in its survey lack the confidence to know whether their user access practices are compliant because they don't have enterprise-wide visibility of that user access.

An effective system of internal control over financial reporting (ICFR) can significantly reduce the risk of misstatements and inaccuracies in your company's financial statements.

3 major learning points:

- What it means for a company to have a "clean" audit of its financial statements, but disclose one or more material weaknesses in ICFR
- Examples of what used to earn companies like yours a free pass on SOX
- Insight into what's changing this year and what auditors are asking your peers for today

Speakers

James Rice

Vice President of Customer Solutions

Greenlight Technologies

Mark Kissman

CFO

Greenlight Technologies

Agenda

1. What is ICFR? – COSO Framework Overview
2. “Material Weakness” and “Deficiency”
3. Challenges and Changes
4. Technology & Automation – Potential Risks vs. Actual Violations
5. Business & Financial Impact
6. Customer Use Cases Examples

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

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**

1. Control Environment

The company's top-level environment with respect to control. This includes elements such as the ethical "tone at the top," and the effectiveness of the board's audit committee in its high-level oversight of financial reporting.

- Integrity and Ethical Values
- Commitment to Competence
- Board of Directors and Audit Committee
- Management's Philosophy and Operating Style
- Organizational Structure
- Assignment of Authority and Responsibility
- Human Resource Policies and Procedures

2. Risk Assessment

The assessment of risks of the various processes and data points that feed into the company's financial reports. For example, a process that is highly susceptible to fraud would be considered to be a high-risk area.

- Company-wide Objectives
- Process-level Objectives
- Risk Identification and Analysis
- Managing Change

3. Control Activities

The way in which controls are actually designed and implemented within the company, so as to address the identified risks.

- Policies and Procedures
- Security (Application and Network)
- Application Change Management
- Business Continuity/Backups
- Outsourcing

4. Information & Communication

The way in which information within the company is gathered and shared, both to people within the company responsible for financial reporting, and to external users of financial reports.

- Quality of Information
- Effectiveness of Communication

5. Monitoring Activities

The way in which the effectiveness of these controls are monitored by company management.

- Ongoing Monitoring
- Separate Evaluations
- Reporting Deficiencies

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

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

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

“Staying Clean” 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:

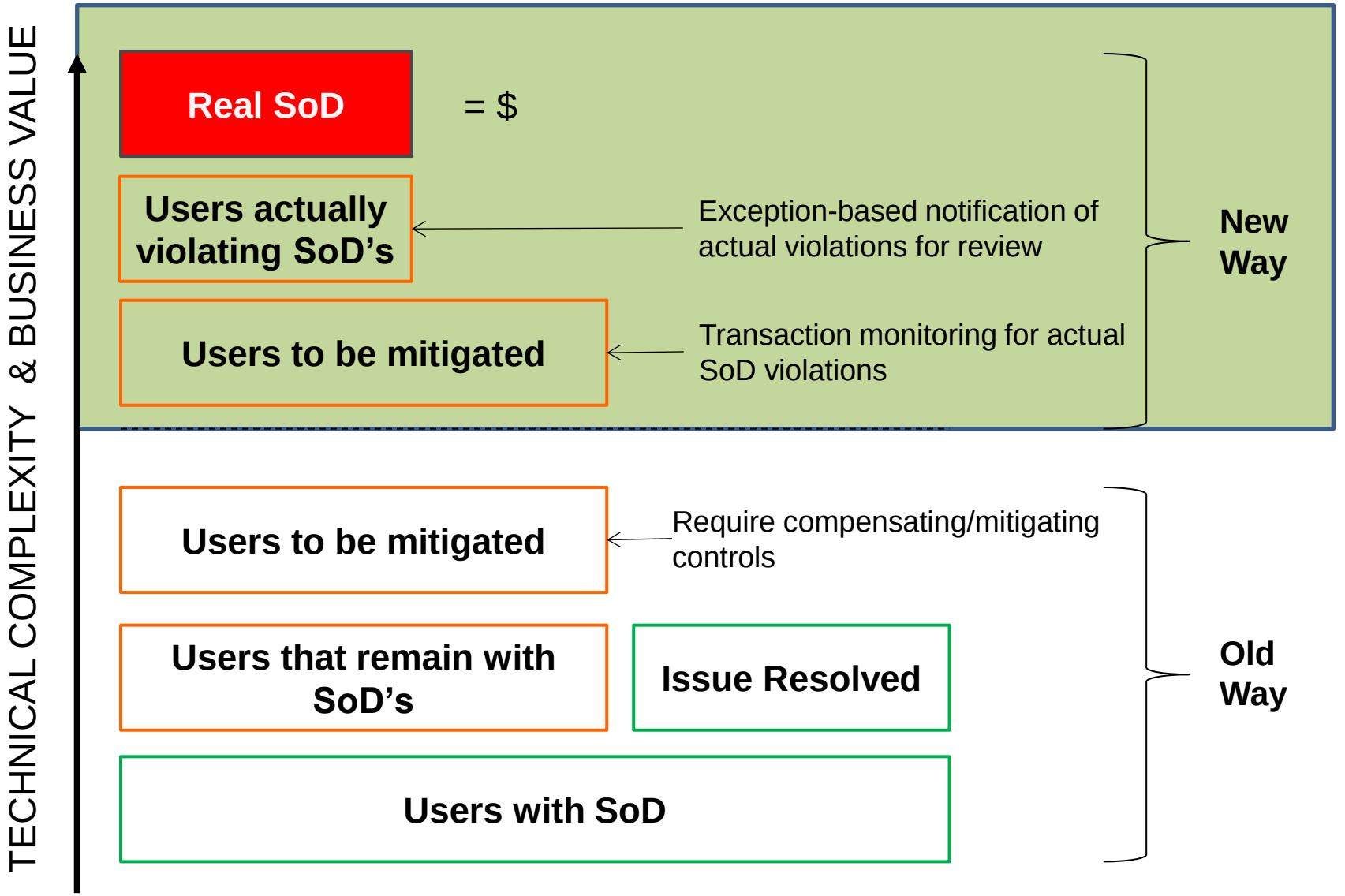
- No controls are defined – companies stop at the point of which users have risky access
- 'Dummy' controls are in place to mask risks from being reported as uncontrolled
- A business process control is identified and assigned that does not adequately monitor user risk
- Controls are defined, haphazardly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

Potential Risk vs. Actual Violations

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	

Prioritize Controls Based on Business Impact



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 #3

What are your plans to automate your internal controls testing?

A. Already automated

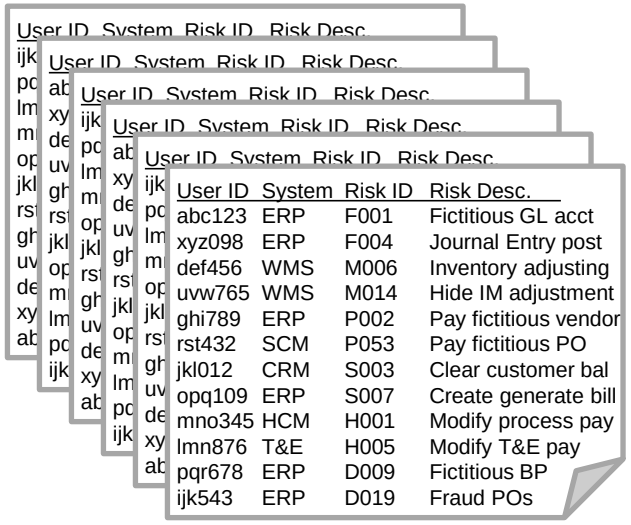
B. Significant plans

C. Moderate plans

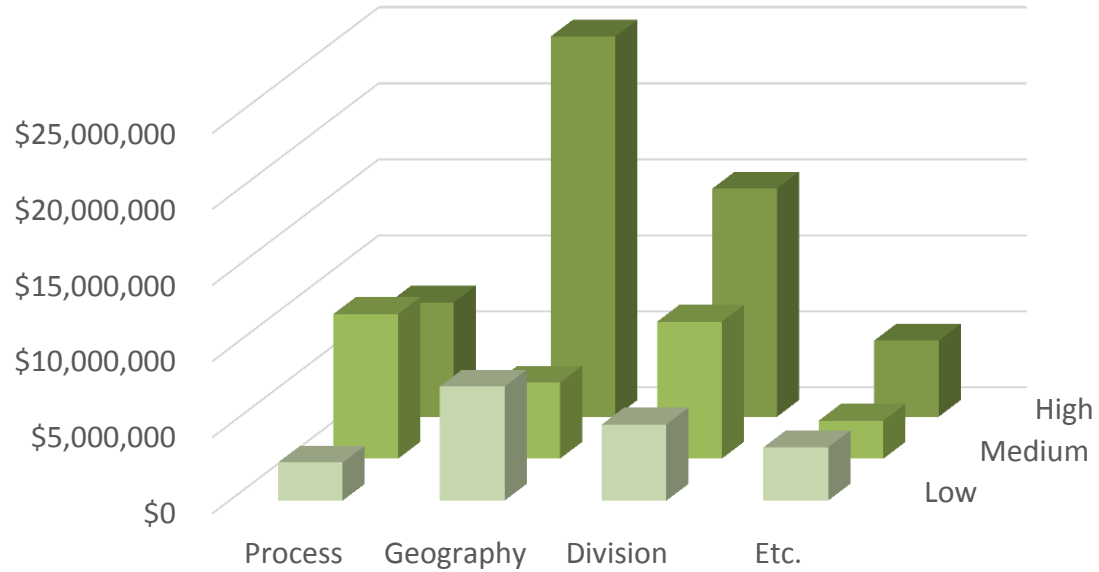
D. No plans

Drive Financially Based Business Decisions that Ensure Significant Return on Investment

Would you rather review potential risks that might occur…



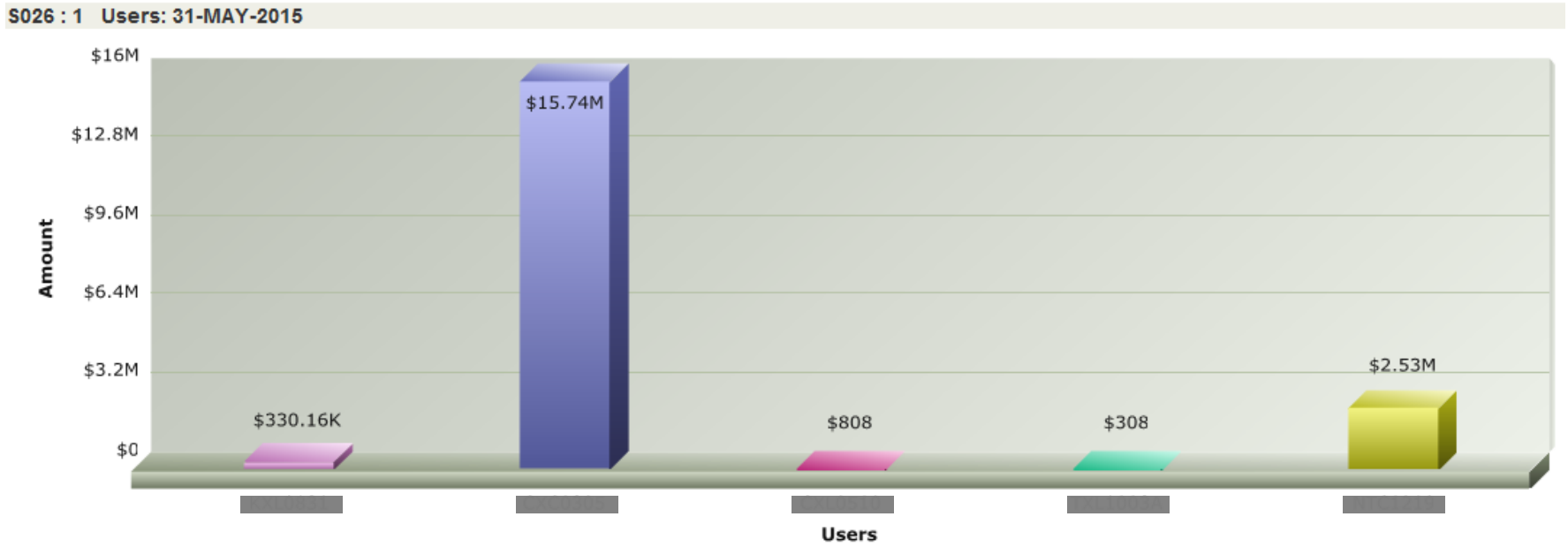
Or review the impact actual material violations are having on your business?



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

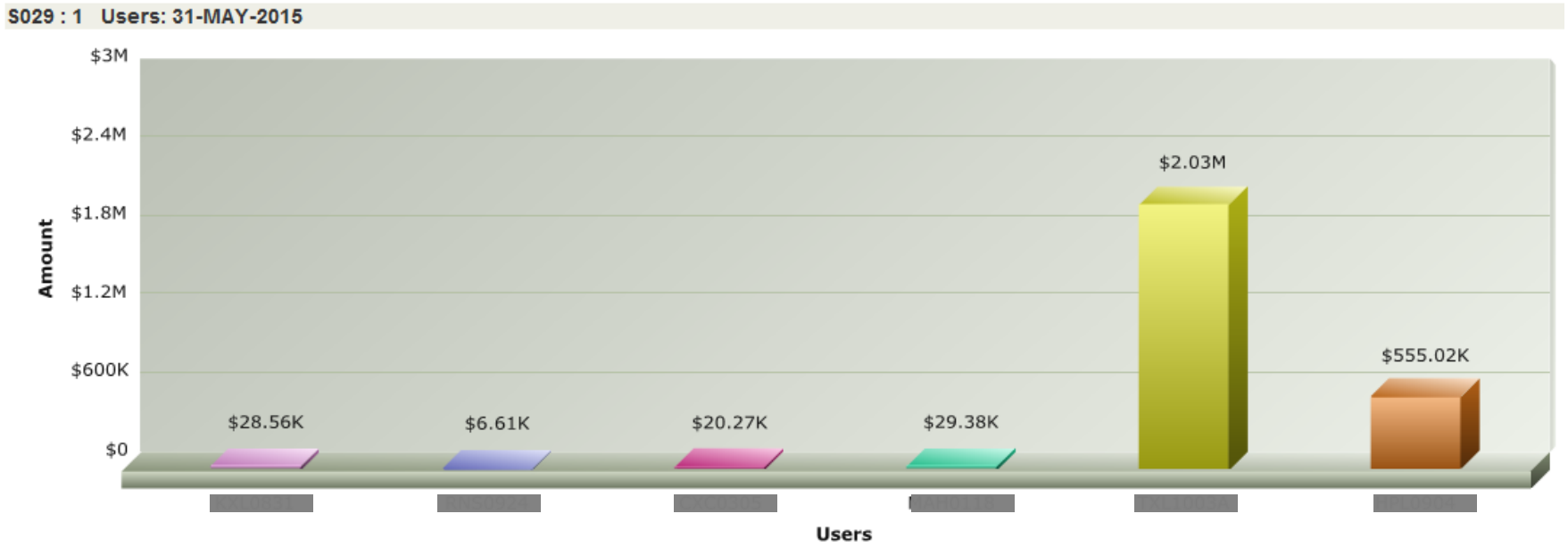
Customer Example: Invoicing & Processing Payments



- 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

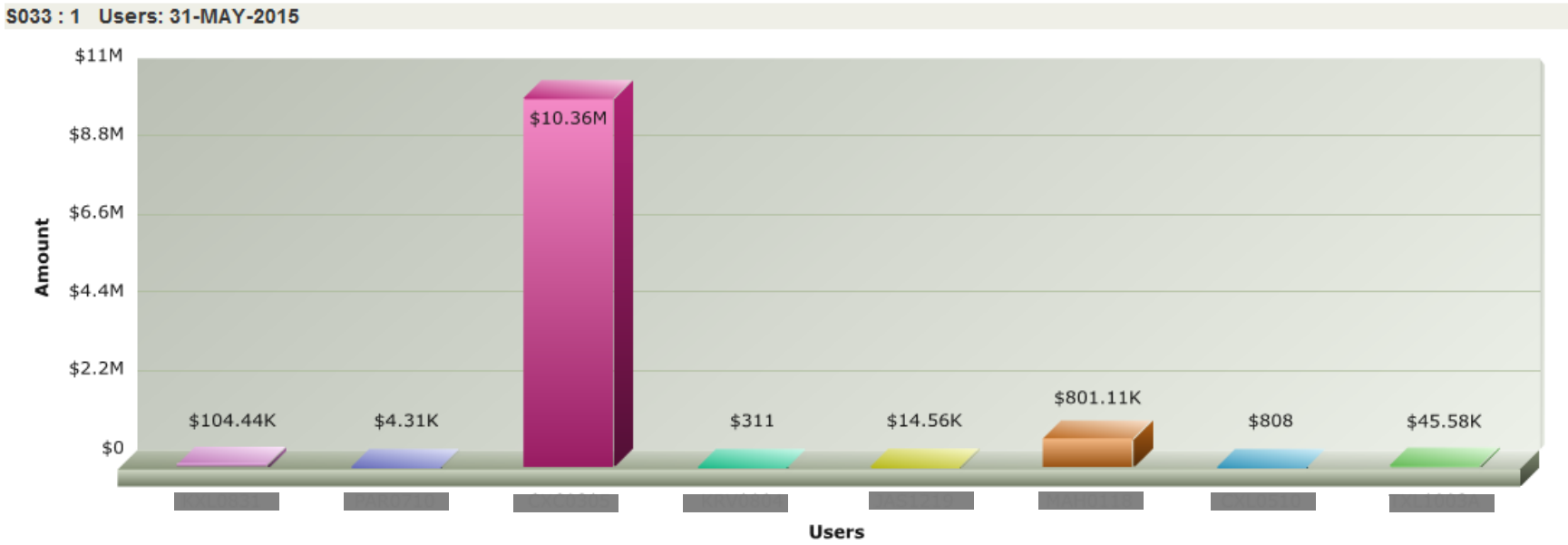
Find where the risk is materializing, have controls that are built into the business process and ensure transparency to the actual bottom-line business value ($) exposure allows senior management, compliance or audit to identify fraud much quicker than with typical manual monitoring

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

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 HANA

ARIBA An SAP Company

successfactors An SAP Company

CRM

ORACLE

PeopleSoft

JDEdwards Enterprise Software

infor

Microsoft

Benefits of Automation & Focus

Out of the box SOD risks ERP

- 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

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 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 managed by GRC

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%

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

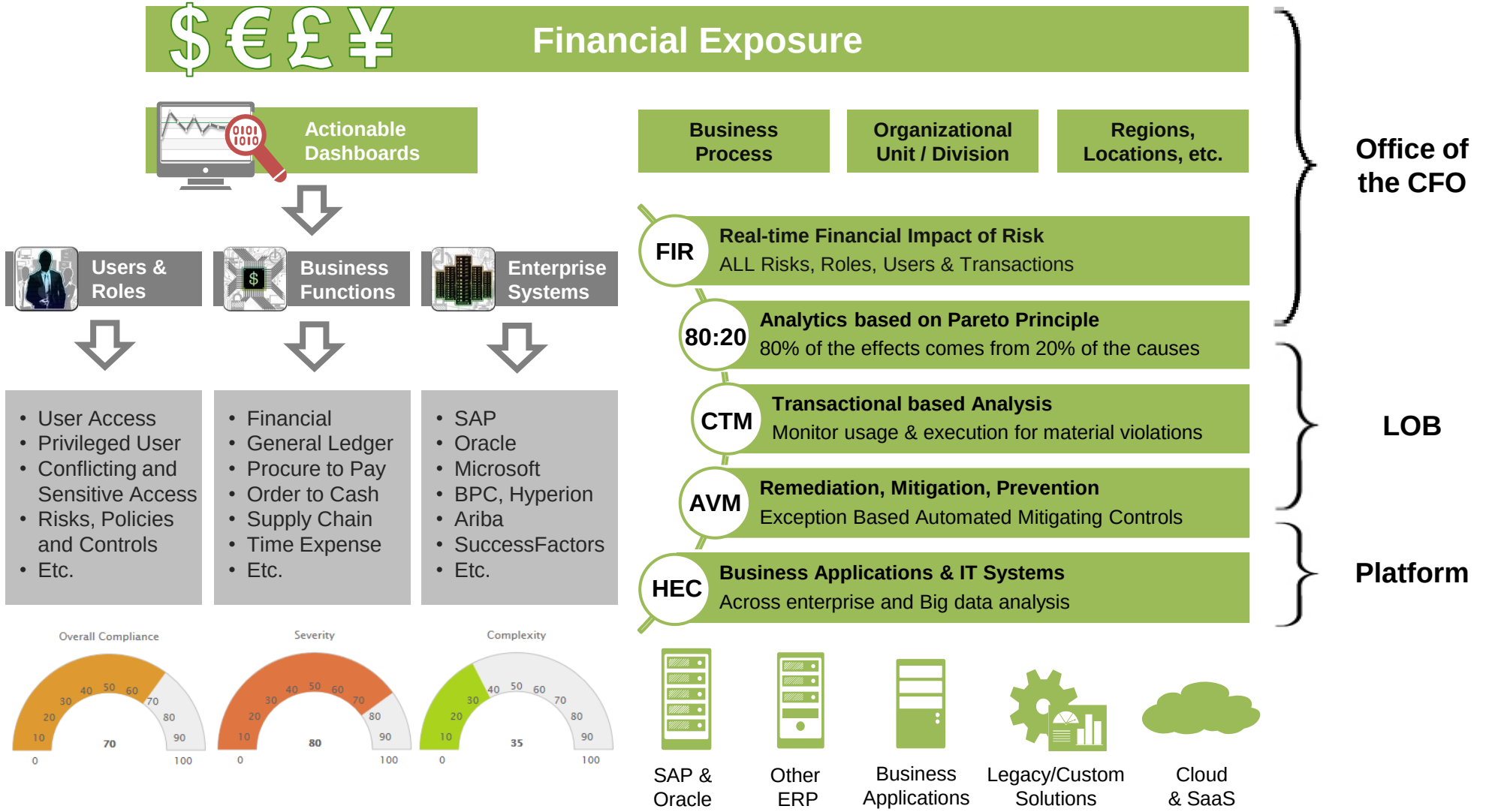
Human Resource

- Master Data
- Employee Management
- Benefit Administration
- Payroll

Time & Expenses

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

Financial Impact of Risk & Business Exposure



Greenlight Monitors Millions of Users & Billions of Transactions

Thank You

Learn more at www.greenlightcorp.com