Internal Controls over Financial Reporting (ICFR)

Are Your ICFR Initiatives Keeping Up with Business Transformation?

February 6, 2019

Speakers

James Rice

- VP, Customer Solutions at Greenlight Technologies
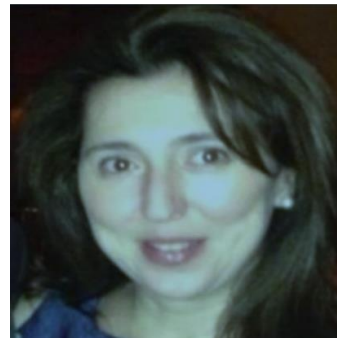- PwC
- Accenture

Mark Kissman

- CFO, Greenlight Technologies
- CFO of multiple public and private technology companies
- KPMG

Rich Adduci

- Advisor, Esito LLC
- CIO, National Grid
- CIO, Boston Scientific
- CIO Advisory Board Member

Hania Abrous-McCarthy

- Managing Director, Gladclif LLC
- CAE, American Stock Transfer & Trust
- SVP Internal Audit, Citco Fund Services
- KPMG

About Greenlight

Company

- ✓ Founded 2007; Headquarters Flemington NJ

Partnerships

- ✓ SAP Solution Extension

SAP® Certified

- ✓ Oracle Platinum Partner

ORACLE® Platinum Partner

- ✓ Cisco Security

CISCO

- ✓ FEI Strategic Partner

fei

Awards & Recognition

BIG DATA AWARD

- ✓ Best Big Data Solution for SAP HANA

- ✓ Highest Possible Rating in Gartner Marketscope

Gartner®

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

Millions of Users & Billions of Transactions Monitored

Enterprise Business Risk Challenges

Regulatory pressures

- Increasing requirements
  - Financial reporting regulations (SOX, MAR, CA-52 313, LSF, Turnbull)
  - Privacy mandates (PCI, PIPEDA, HIPAA/HITECH, EU Data Privacy)
  - Industry mandates (FERC/NERC, CFR21, Basel, GLBA)
  - Corporate governance mandates (ITAR, OFAC, FCPA, UK Bribery)
- Increased enforcement actions / fines

Pace of business

- Complex & changing business models
  (outsourcing, divestitures, M&A activity)
- Complex & changing technology infrastructure
  (cloud, mobile, social networking)
- Change to user functional roles with the organization
- Reduce cost of compliance & control, enable the business
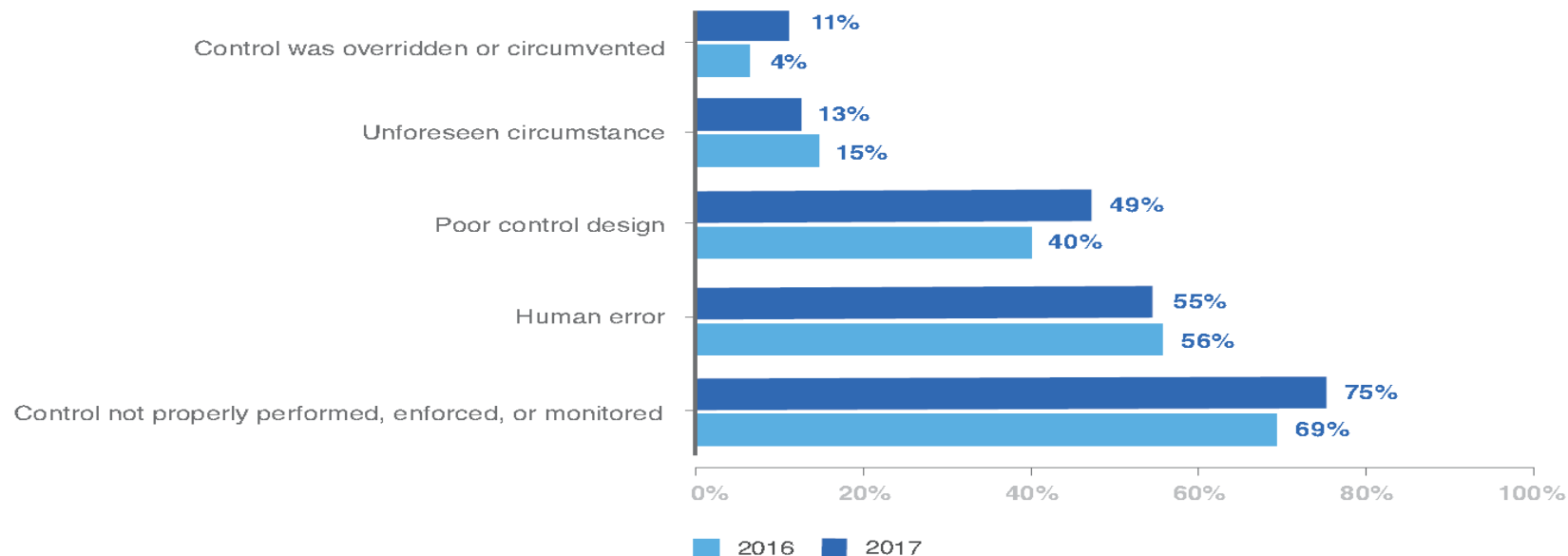
Increased risk exposure

- Demand for more operational transparency
- Insider threat (corporate IP theft, loss due to fraud, misuse of authorization, human error or omission)
- Manual controls – can't prevent risk, error prone
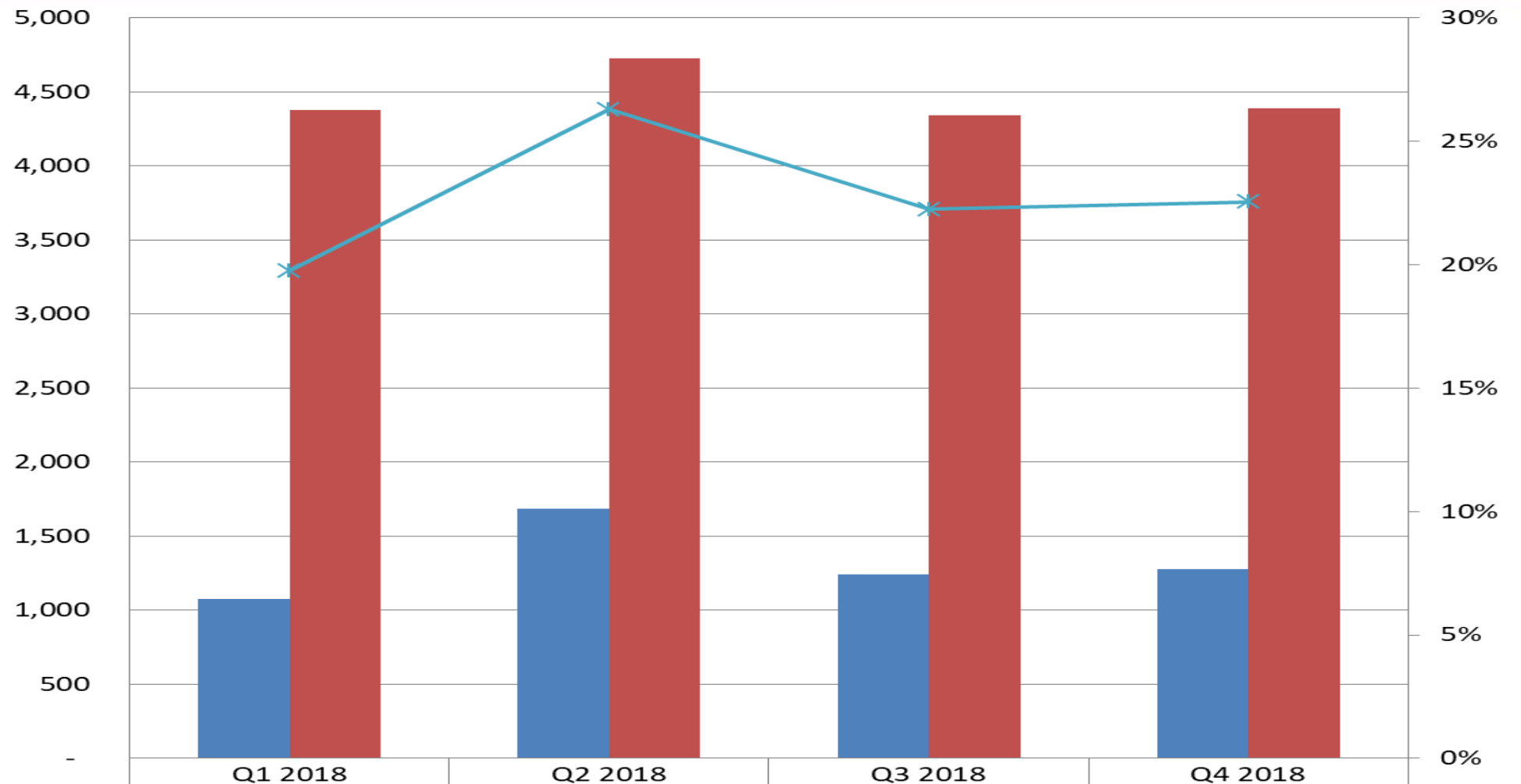
Internal Control Failures on the Rise

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

Disclosures of Material Weakness to SEC

	Q1 2018	Q2 2018	Q3 2018	Q4 2018
Material Weakness	1,078	1,685	1,241	1,276
Clean	4,376	4,724	4,339	4,386
Material Weakness, % of total	20%	26%	22%	23%

Poll Question #1

Has your organization had a material weakness or significant deficiency from audit?

- Yes

- No

Recent Example

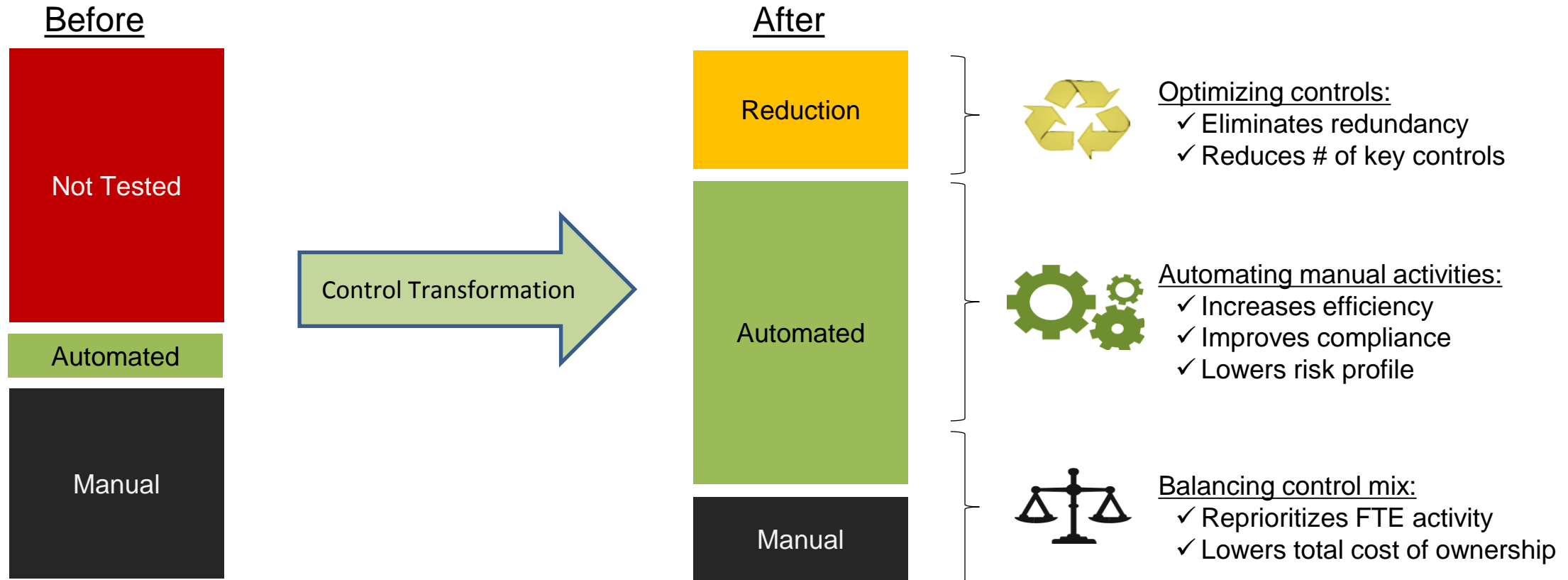**Costco Warns of Material Weakness in Controls**
The warning related to IT systems that "support the company's financial reporting processes" drove Costco's stock down 2.4%.

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."

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:
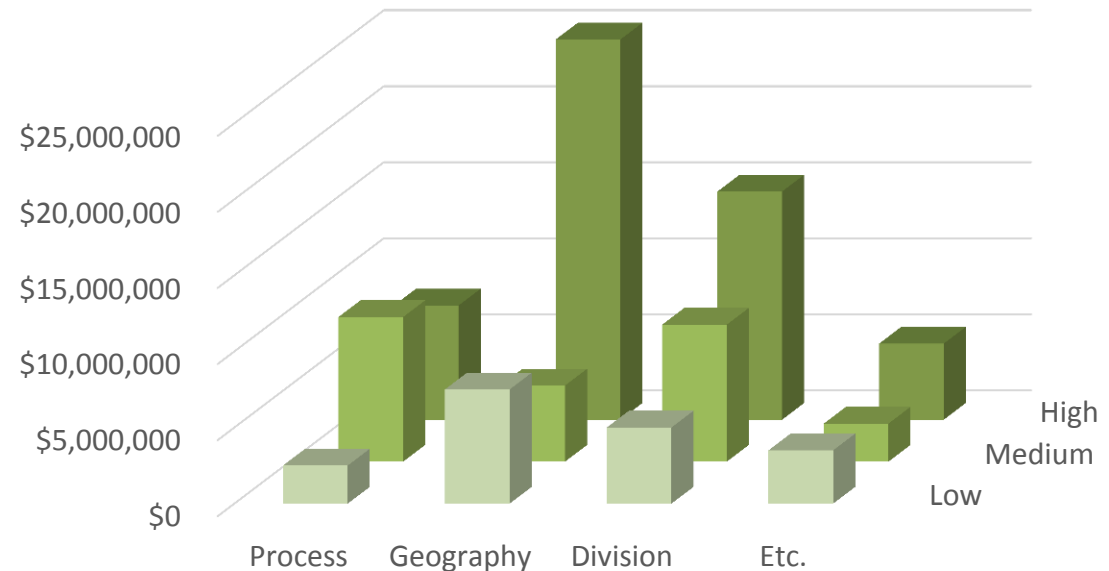- ✓ Reprioritizes FTE activity
- ✓ Lowers total cost of ownership

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

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?

Chart axis values: $0, $5,000,000, $10,000,000, $15,000,000, $20,000,000, $25,000,000

Categories: Process, Geography, Division, Etc.

Depth axis: High, Medium, Low

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

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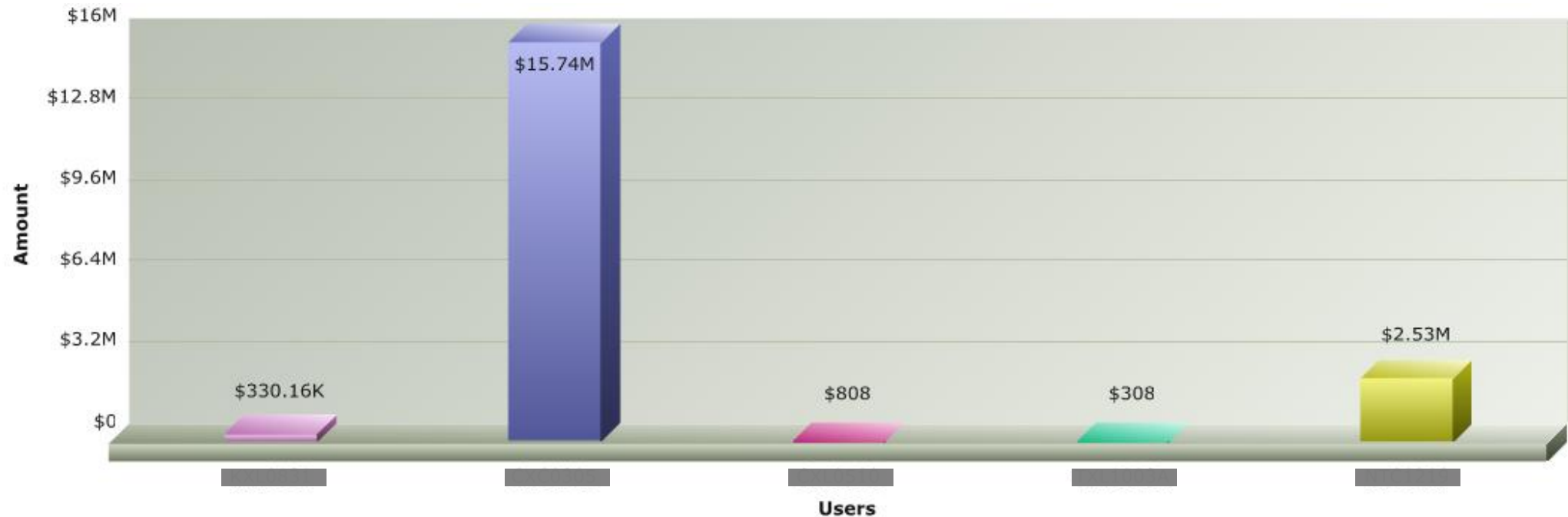
140 users are reported by a GRC solution to have the authorizations to perform the risk

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

ICFR Survey – Maturity Model

1. **Initial**
   - Unpredictable environment, no or few control activities designed or in place

2. **Repeatable**
   - Control activities in place, but not adequately documented.
   - Little or no formal training or communication of expected minimum control activities

3. **Capable**
   - Control activities designed and adequately documented but not standardized.
   - Deviations may not be detected on a timely basis

4. **Defined**
   - Standardized controls with periodic testing.
   - Automation and tools may be used to support ICFR

5. **Efficient**
   - Integrated internal controls with real time monitoring.
   - Automation and tools are used to support control activities
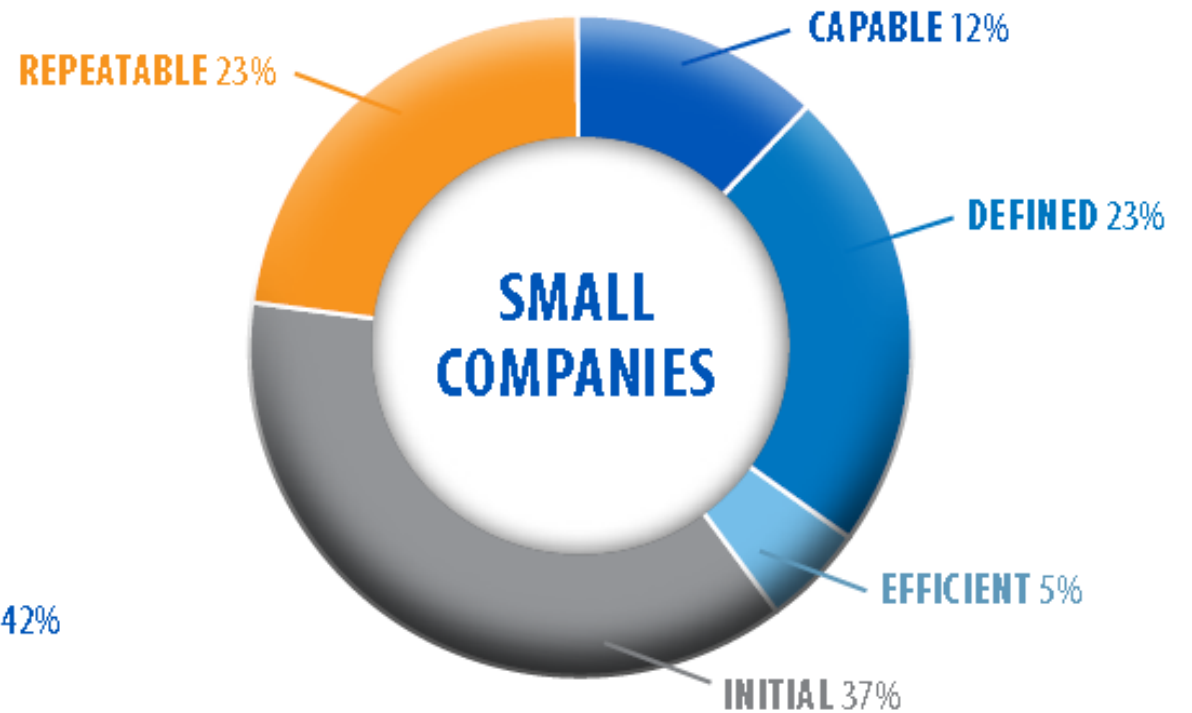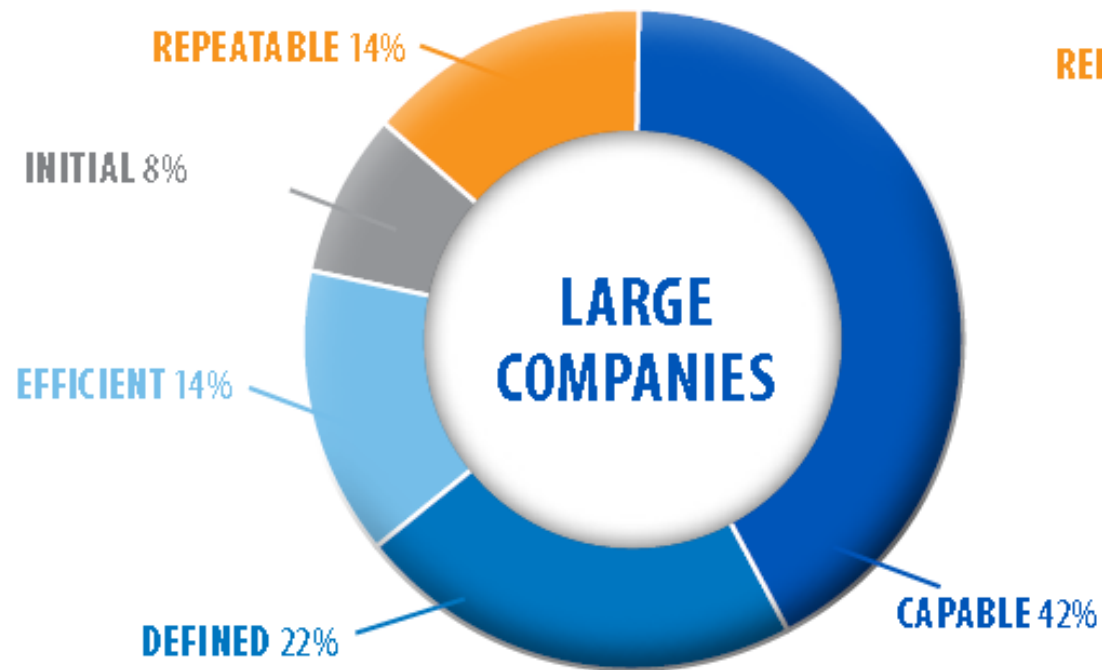
Poll Question #2

Where does your organization fall on the maturity curve?

1. Initial

2. Repeatable

3. Capable

4. Defined

5. Efficient

ICFR 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.

LARGE COMPANIES
- REPEATABLE 14%
- INITIAL 8%
- EFFICIENT 14%
- DEFINED 22%
- CAPABLE 42%

SMALL COMPANIES
- CAPABLE 12%
- DEFINED 23%
- EFFICIENT 5%
- INITIAL 37%
- REPEATABLE 23%

FINANCIAL EXECUTIVES INTERNATIONAL | www.financialexecutives.org

ICFR Survey Results

Big Companies Plan to Automate ICFR While Smaller Companies On The Technology Sidelines
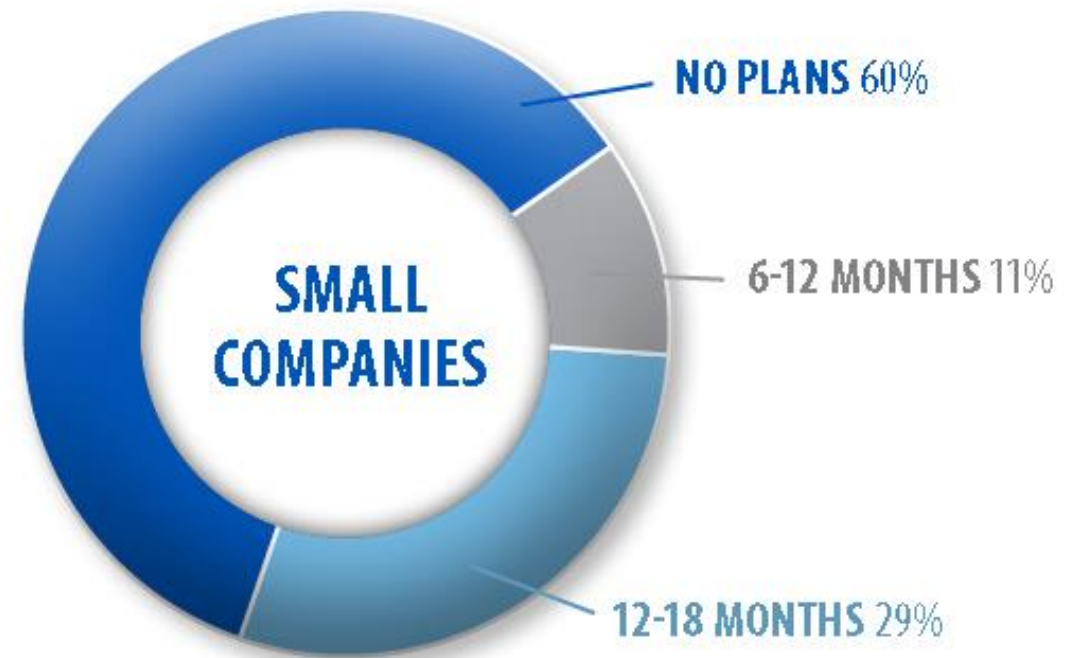
LARGE COMPANIES

- NO PLANS 19%
- 6-12 MONTHS 25%
- 12-18 MONTHS 56%

SMALL COMPANIES

- NO PLANS 60%
- 6-12 MONTHS 11%
- 12-18 MONTHS 29%
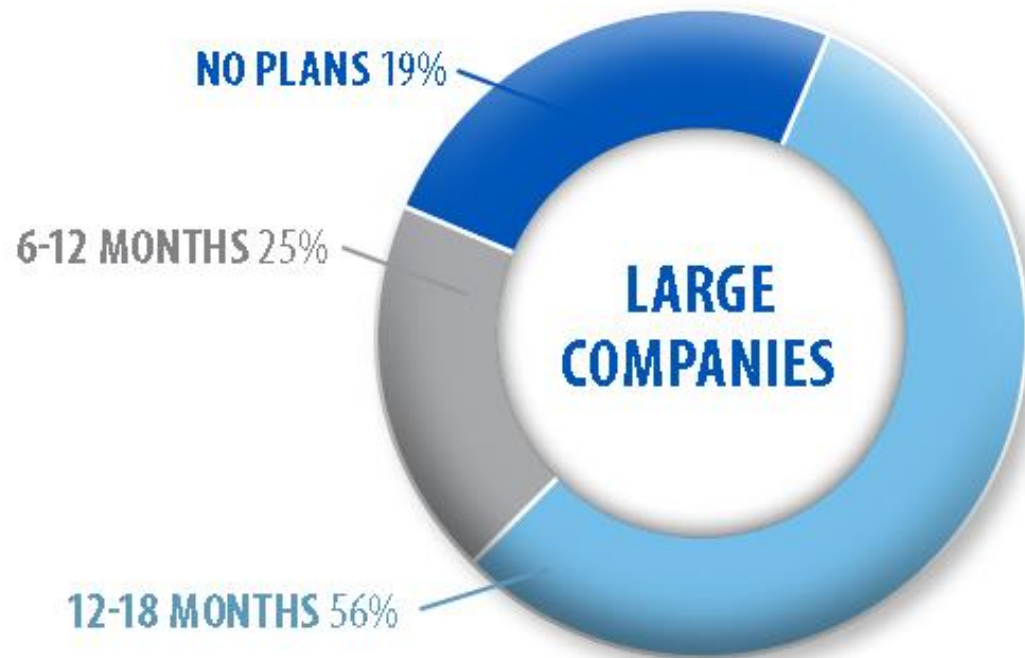
Nearly 80% of respondents with 10,000 or more employees said they plan to increase investment in ICFR automation in the next 6-18 months.

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.

Poll Question #3

Does your organization have plans to automate testing of internal controls over financial reporting?

- No plans

- 6-12 months

- 12-18 months

ICFR Survey Results

Who Owns ICFR?

Large company Controllers lead the ICFR charge, while CFOs are small companies focus controls

LARGE COMPANIES
- CEO: 0%
- COMPLIANCE OFFICER: 8%
- HEAD OF INTERNAL AUDIT: 11%
- CONTROLLER: 61%
- CFO: 19%

SMALL COMPANIES
- CEO: 2.1%
- COMPLIANCE OFFICER: 1.6%
- HEAD OF INTERNAL AUDIT: 5.3%
- CONTROLLER: 34.9%
- CFO: 56.1%
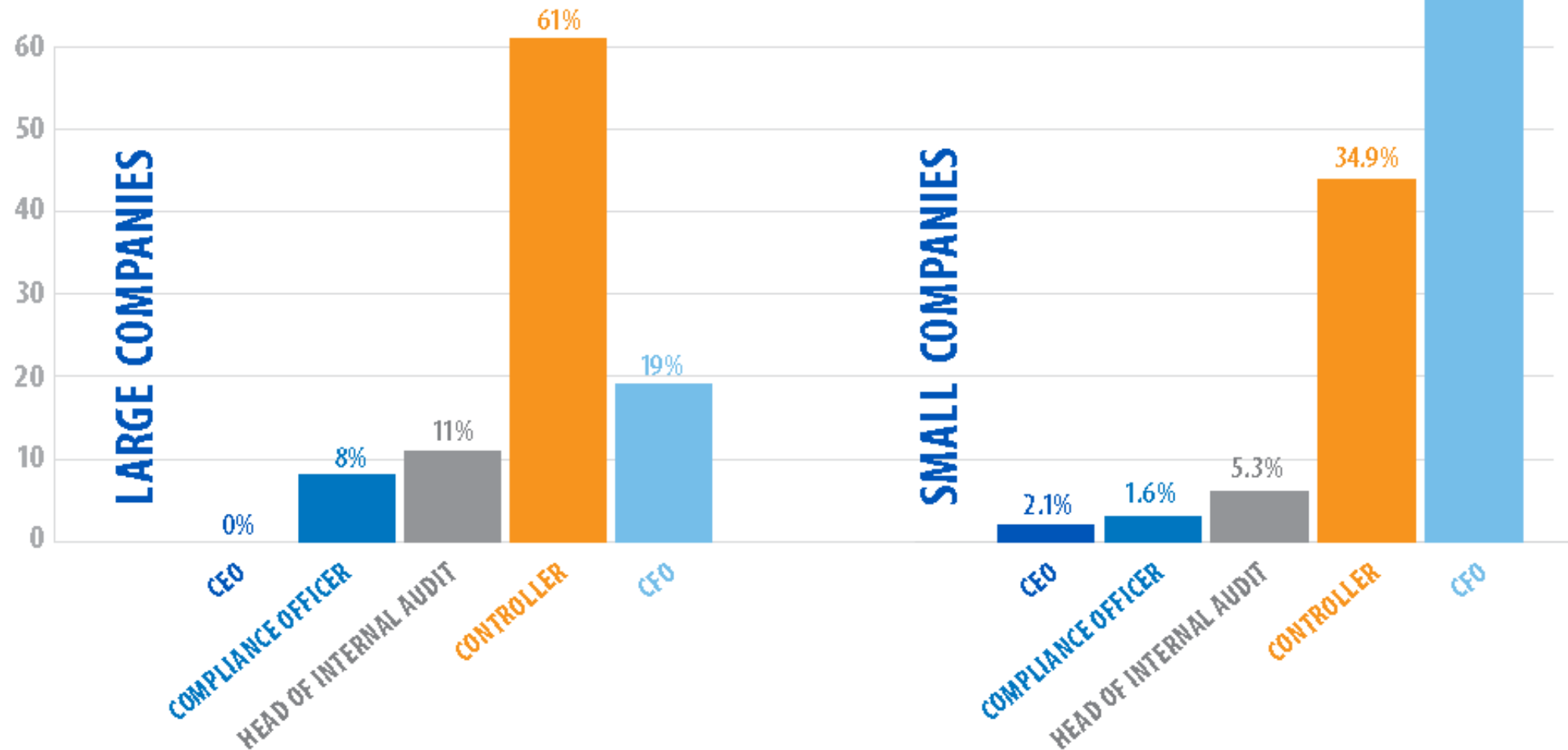
Poll Question #4

Who owns ICFR at your organization?

- CEO

- Compliance Officer

- Head of Internal Audit

- Controller

- CFO

Mark Kissman – CFO, Greenlight Technologies

Customer Example:

- Fortune Global 100 company
  - \>40,000 employees worldwide
  - ERP Instances: SAP (4) 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

Mark Kissman

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

mkissman@greenlightcorp.com

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 • Commodity to market • Product lifecycle	• Customer lifecycle • Liquidity and risk management • Financial booking to reporting	• Source to Pay • Recruitment to retirement • 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
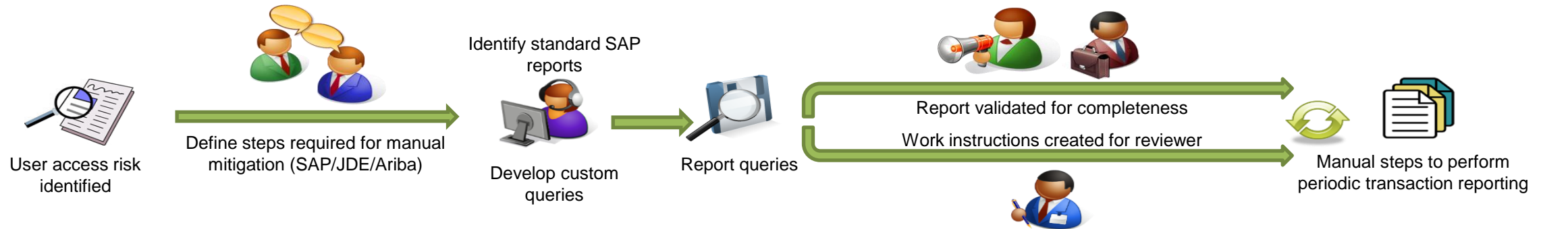
Manual Mitigating Controls – Monitoring

GRC AC — GRC AC creates semi-annual UAR/SOD Reports →

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

100% transactional review of SOD 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

GRC AC creates semi-annual UAR/SOD Reports

AVM syncs w/ GRC AC SOD Reports

AVM queries target systems to identify SOD transactions

Preparation of Compensating Control Reports

100% transactional review of SOD reports

Manage 100% transactional mapping and data correlation across SOD events

Coordinate completion

SOD violations

No violations

False positives

Missed events

Email notification

Investigate issue

Capture and retain documentation as proof of review

Proof maintained in AVM

Findings stored for Audit/SOX preparation and review

Audit/SOX preparation and review

	Manual preparation of SOD reports	False positives or missed events	Retain proof of review	Compliance oversight	Audit preparation effort
Goes away / **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

Rich Adduci – Advisor @ Esito & Former CIO @ National Grid

- **Architectures have become complex**
  - Was: On-prem, central, all in one ERP solution
  - IS: Cloud, modular, distributed
- **Increased Scrutiny from Auditors**
  - SOD / SOX Compliance
  - Audit Costs
- **Cybersecurity Risk Continues to Grow**
  - Whaling - impersonation of C-suite to trigger transfers
  - Insider threat
  - Compromise of Admin Credentials
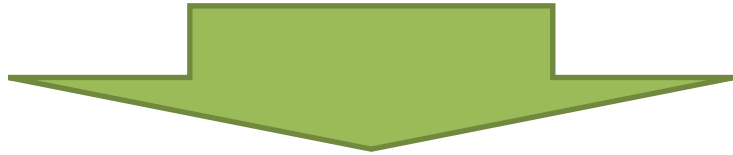
- **Software Solutions are Uniquely Capable of Helping You…**
  - Cross Platform
  - Real-time
  - Monitors & Can Restrict / Take Action
- **My Experience**
  - Reduces audit costs
  - Prevents bad things from happening
  - Outstanding Partner

Rich Adduci

Founder & Advisor, Esito LLC
(Former Global CIO @ National Grid)

Rich.Adduci@Esito.us
www.Esito.us

Esito LLC

Hania Abrous-McCarthy – Managing Director, Gladclif LLC

What?
- Technology enabled risk and controls assessments
- Different from Continuous Monitoring, which is performed by the first and second lines

Why?
- Move away from point in time assessments towards real time reviews
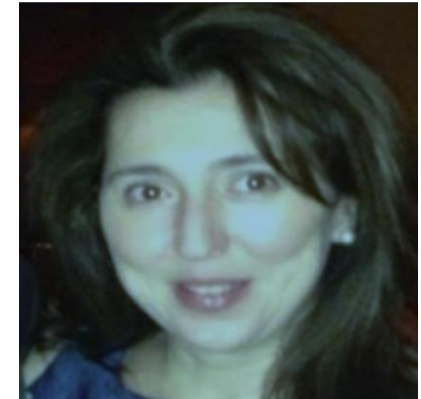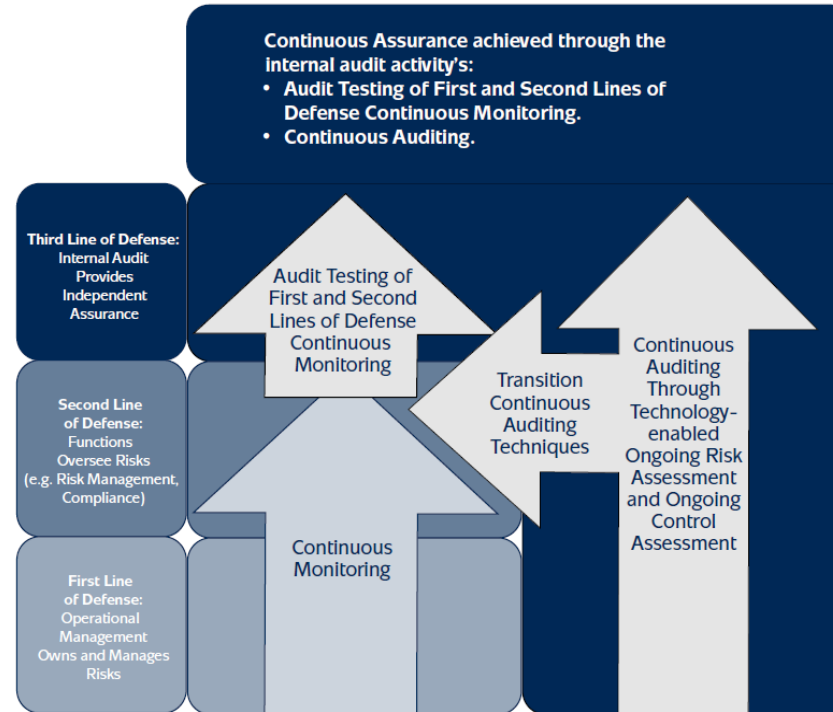- Move away from selecting limited number of items to testing 100% of the population

Challenges
- Data can be difficult to extract, in an 'auditable' format
- May require significant startup time, including staff training
- Marketing of approach to stakeholders

Benefits
- Enhanced communication with first and second lines
- Increased effectiveness and efficiency
- Better audit coverage and assurance, over time

Automation: Internal Audit Perspective Continuous Auditing

Continuous Assurance achieved through the internal audit activity's:
- Audit Testing of First and Second Lines of Defense Continuous Monitoring.
- Continuous Auditing.

Third Line of Defense: Internal Audit Provides Independent Assurance

Second Line of Defense: Functions Oversee Risks (e.g. Risk Management, Compliance)

First Line of Defense: Operational Management Owns and Manages Risks

Audit Testing of First and Second Lines of Defense Continuous Monitoring

Continuous Monitoring

Transition Continuous Auditing Techniques

Continuous Auditing Through Technology-enabled Ongoing Risk Assessment and Ongoing Control Assessment

My experience
- Development of end-to-end continuous auditing methodology is key
- Begin with the end in mind!

Hania Abrous-McCarthy

Managing Director, Gladclif LLC
(Former Chief Audit Executive @ American Stock Transfer & Trust)

hmccarthy@gladclif.com

Question & Answer

James Rice

- VP, Customer Solutions at Greenlight Technologies Inc.
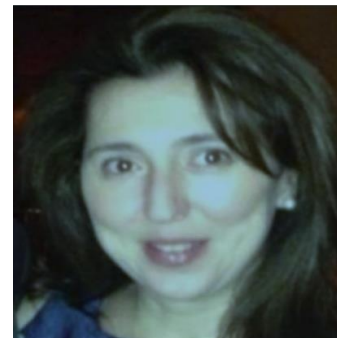- PwC
- Accenture

Mark Kissman

- CFO, Greenlight Technologies Inc.
- CFO of multiple public and private technology companies
- KPMG

Rich Adduci

- Advisor, Esito LLC
- CIO, National Grid
- CIO, Boston Scientific
- CIO Advisory Board Member

Hania Abrous-McCarthy

- Managing Director, Gladclif LLC
- CAE, American Stock Transfer & Trust
- SVP Internal Audit, Citco Fund Services
- KPMG

Internal Controls over Financial Reporting (ICFR)

Are Your ICFR Initiatives Keeping Up with Business Transformation?

February 6, 2019