

# Risk Assessments, Governance Risk and Compliance Program Buildout

SCCE – Scottsdale Regional Virtual  
Compliance & Ethics Conference  
April 10, 2020



1

## Presenters

- James Rose,  
Managing Director, SunHawk Consulting LLC
- Steve James,  
Director of Internal Audit, Cavco Industries Inc



2

2



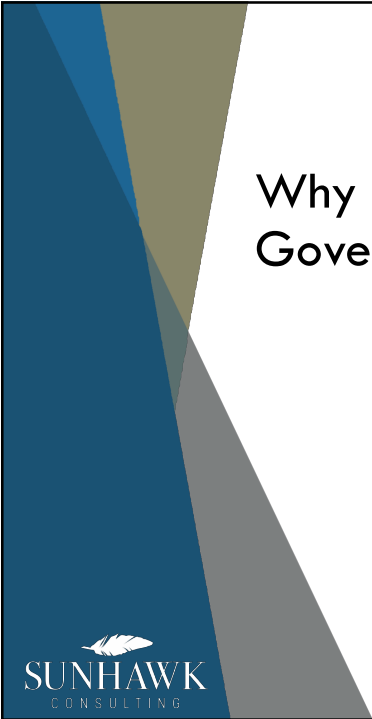
## Presentation Overview

- Why do we pursue excellence in Governance, Risk and Compliance?
- Compliance Risk Assessment for Your Organization
- Evaluating Your Compliance Program
- Governance, Risk and Compliance (GRC) Program Management



3

3




## Why do we pursue excellence in Governance, Risk and Compliance?



4

4



5

## Strategy Alignment:

### The Business Case for an Effective Compliance Program

As the global regulatory and enforcement focus on financial and corporate fraud, corruption, and national security crimes intensifies, a compliance and ethics program has never provided more value to companies. An effective compliance program demonstrates a company's commitment to responsible conduct and can result in substantial and direct benefits to a company's bottom line.

**What are the bottom line benefits of an effective corporate compliance and ethics program?**

**Prevention of violations:** A compliance plan tailored and implemented to address the real risks faced by a company should prevent most violations. In preventing violations, a compliance program can more than justify associated costs and investments. The cost of non-compliance

to financing may be constrained during the pendency of an investigation, regardless of its final resolution, Fitch Ratings reported recently<sup>1</sup>.

In order to be effective, a program needs to have a demonstrated commitment to compliance at the highest levels, Board of Directors' oversight, an empowered compliance infrastructure, relevant training, regular auditing and monitoring, reporting procedures, remediation, discipline, and recordkeeping.

**Competitive advantage:** A compliant company "will have a more resilient business, be an employer of choice for recruiting and can gain a competitive advantage as a preferred choice of ethically concerned customers, investors, suppliers and other stakeholders."<sup>2</sup> Compliant companies also offer the stability derived from avoidance of the


**Key is**

What are an effective and ethical Conclusion

**Competitive advantage:** A compliant company "will have a more resilient business, be an employer of choice for recruiting and can gain a competitive advantage as a preferred choice of ethically concerned customers, investors, suppliers and other stakeholders."<sup>2</sup> Compliant companies also offer the stability derived from avoidance of the delays and disruptions caused by investigations, interim suspension orders, intensive licensing reviews, or other, more stark, penalties. By implementing an effective compliance program, a company can highlight its commitment to stable and enduring business relationships, putting to rest anxieties about global trading and risk management pitfalls.

Clifford Chance (Global Law Firm) – Briefing Note August 2011

5



6

## Strategy Alignment:


ETHICS

### We Shouldn't Always Need a "Business Case" to Do the Right Thing

by Alison Taylor  
September 19, 2017

“...arguments for ethical business tend to focus heavily on the upside of risk prevention: avoiding the possibility of regulatory investigation or reputational scandal. While the argument for risk prevention can be compelling, it ignores the culture of most private sector organizations. Human beings are goal-oriented, competitive, and highly social, with limited memories and attention spans. People are generally overconfident when they assess risk, more comfortable focusing on its probabilities than on potential impacts. Given that senior decision makers in organizations often attained leadership precisely because they are keenly competitive, audacious people, they are particularly unlikely to be swayed by calls for caution . . .

“On the other hand, senior executives often respond enthusiastically to the potential of business integrity to provide an inspirational narrative. Amid the world's faltering political will to tackle long-term social and environmental challenges, business is well-placed to assume a leadership role. Most corporate leaders know this. They understand the power of reputation and relationships. They think often and hard about their personal legacy at the company and their opportunity to change the world for the better. They are less subject to short-term operational pressures, and accordingly less risk-averse.”



6

## Compliance Program Effectiveness – Select Regulatory Enforcement Perspectives

- Federal Sentencing Guidelines
- Justice Manual FCPA Corporate Enforcement Policy (March 2018 and November 2019)
- Benczkowski Memorandum (October 2018)
- Policy on Evaluation of Corporate Compliance Programs (April 2019)
- Justice Manual, Cooperation Guidelines (May 2019)
- Justice Manual, Corporate Compliance Program Guidance (July 2019)



7

7

## Polling Question 1:

How hard is it to make the case for an effective compliance program within your organization?

- A. Everyone is onboard!
- B. We have support from the top – but difficult to implement.
- C. Episodic support – we have difficulty being consistent.
- D. Uphill daily struggle but at least the topic is alive.
- E. What is compliance? Never discussed.



8

8



## Compliance Risk Assessment for Your Organization



9

9



## Expectations for an Effective Compliance Risk Assessment

- Identify Authoritative Sources
  - Law and regulations related to your organization
- Identify Relevant Compliance Frameworks
  - SOX, COBIT, HITECH, COSO, ISO
- Prioritize Risks
  - Develop enterprise prioritization framework
- Assign Accountability
  - Take a process-based approach (versus departmental)



10

10

## Researching Your Organization

- Organization's website and internal portal
- Marketing materials
- Organizational charts
  - Segments
  - Legal Entities
  - Departments
- Articles of incorporation, operating agreements
- Board and senior leadership meeting minutes
- Professional and contracted services agreements
- Exchanges finlines



11

11

## Operations and Key Personnel

- Start by identifying key personnel who can provide institutional knowledge
- Meet with key stakeholders at the senior management level, VP's, Directors, Managers
- Meet with selected frontline staff
- Meet with all members of the executive compliance committee



12

12

## Areas of Potential Risk

- Depending on the size of your organization and services offered some potential risk areas include:
  - Federal Reserve / Banking
  - Local Licensing
  - Taxing Jurisdictions / Intercompany Pricing
  - Conflict of Interest Management
  - Sanction Checking – LEIE
  - HIPAA Privacy and Security
  - Any open investigations
  - Hotline calls
  - Vendor Management
  - OSHA
  - Department of Insurance

## Compliance Risk Management – Compliance Risk Categories

General Compliance Risks	Mortgage Compliance Risks	Corporate Compliance Risks
<b>Planning Risks:</b> <ul style="list-style-type: none"> <li>• Compliance Leadership &amp; Succession Planning</li> <li>• Regulatory Forecasting               <ul style="list-style-type: none"> <li>• State Regulators</li> <li>• Federal Regulatory</li> <li>• Non-US Regulatory</li> </ul> </li> </ul> <b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Compliance Staffing</li> <li>• Compliance Organizational Design and Accountability Assignment</li> <li>• Compliance Reporting</li> <li>• Compliance Risk Assessment</li> <li>• Fraud, Waste &amp; Abuse Assessment</li> <li>• Ethical Conduct</li> </ul>	<b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Anti-Money Laundering</li> <li>• Equal Credit Opportunity Act</li> <li>• Fair Credit Reporting Act</li> <li>• Fair Debt Collection Practice Act</li> <li>• Fair Housing Act</li> <li>• Privacy of Consumer Financial Information</li> <li>• Truth In Lending Act</li> <li>• Real Estate Settlement Procedures Act (RESPA)</li> <li>• Secure and Fair Enforcement for Mortgage Licensing</li> <li>• Unfair, Deceptive, or Abusive Acts or Practices</li> <li>• Telephone Consumers Protection Act</li> <li>• Homeowner Protection Act</li> <li>• Service Members Civil Relief Act</li> <li>• Fair and Accurate Credit Transactions Act</li> <li>• EFT</li> <li>• Loan Originator Compensation Rule</li> <li>• FTC Advertising Rules</li> <li>• E-sign Act</li> <li>• OFAC Compliance</li> <li>• IRS 1098 requirements</li> <li>• PCI – Debit/Credit Card Security</li> <li>• Foreclosure requirements—state statutes</li> <li>• Bankruptcy Code(?)</li> <li>• Government Loan Annual Renewal (FHA, VA, RHS)</li> <li>• Loan file retention policy</li> <li>• CFPB               <ul style="list-style-type: none"> <li>• Vendor management</li> <li>• Customer Complaint Process</li> </ul> </li> </ul>	<b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Securities Regulations &amp; Filings               <ul style="list-style-type: none"> <li>• 10K / 10Q</li> <li>• Form 4</li> <li>• Section 16 filers</li> <li>• Disclosures</li> </ul> </li> <li>• NASDAQ regulatory guidelines</li> <li>• Investor Communication / Fair Disclosure</li> <li>• Tax filings (Federal and state)               <ul style="list-style-type: none"> <li>• Income tax (fed / state)</li> <li>• Sales tax (state)</li> <li>• Heavy weight use tax (fed)</li> <li>• Contractor 1099s</li> </ul> </li> <li>• Conflict Minerals (Form SD)</li> <li>• Dodd-Frank reporting</li> <li>• Census reporting</li> <li>• Information Security</li> <li>• Privacy Regulations               <ul style="list-style-type: none"> <li>• HIPAA</li> <li>• GDPR</li> </ul> </li> <li>• Contract Adherence</li> <li>• Contract management</li> <li>• Intellectual Property</li> <li>• Litigation Management</li> <li>• Government Procurement</li> <li>• Advertising Laws</li> <li>• Human Resources               <ul style="list-style-type: none"> <li>• DOL Requirements</li> <li>• FLSA</li> <li>• Minimum Wage</li> <li>• Hiring Discrimination</li> </ul> </li> </ul>
<b>Manufacturing Compliance Risks</b>		
<b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• HUD</li> <li>• OSHA</li> <li>• EPA</li> <li>• State code compliance (modular)</li> <li>• Reporting of shipped homes to states</li> <li>• Licensing               <ul style="list-style-type: none"> <li>• Plant</li> <li>• Retailers</li> <li>• Salespeople</li> <li>• Contractor licenses (e.g., installation)</li> <li>• Validate Retailer Licenses</li> </ul> </li> </ul>		

## Inquiries to Understand Risk Culture

- Risks - Identification and Prioritization
  - Are risks understood at all impacted operational levels (role-appropriate)?
  - Proactive identification of current or prospective risks or reactive “check the box” approach (e.g., OIG work plan)?
  - Is there clarity regarding organizational risk tolerance or culture of magical thinking (make it so)?
  - Consideration of new risks when new business lines pursued?



15

15

## Inquiries to Understand Control Culture

- Controls to Manage Risks (e.g., policies and procedures, education and training and monitoring)
  - Are Controls designed to address greatest risks?
  - Actually implemented (not policy on a shelf or one slide of 100 in annual training)?
  - Understood by those responsible for implementing and overseeing?
  - What type of testing and monitoring of control effectiveness occurs?



16

16



## Risk Analysis

- Risk Ranking Methodology
  - Attempt first to develop or use an enterprise ranking methodology.
  - CAUTION – The purpose of the risk ranking is to be “directionally correct” about which risks are most important. Risk ranking should not become its own exercise – there is no “perfect” ranking

17

## Risk Ranking Methodology – 4x4 Heat Map

Risk Categorization Matrix					
Impact	Significant				<b>Immediately Address</b> Risk Beyond Acceptable Tolerance
	Moderate				<b>Consider Improvement</b> Risk/Compliance Expectations Require Improvement
	Minor				<b>Maintain Focused Investment</b> Seize Opportunities to Improve As Available
	Negligible				<b>Optimize &amp; Maintain</b> Optimize Processes To Shift Resources to Higher Risk Areas
		Highly Predictable	Unlikely	Likely	Unpredictable / Unknown
		Ability to Predict (Likelihood)			

18

## Example Risk Ranking Methodology

Likelihood Model	Weighting	Rating Score	Predictable Risk - 1	Lower Risk - 2	Moderate Risk - 3	Unpredictable Risk - 4
<b>Risk and Control Framework In Place</b>	35%	3	1.05	Process Owner Defined; Controls in Place; Limited Risk Analysis to Validate Comprehensive Nature of Controls	Limited Controls in Place, Lack of Clarity Regarding Process Owner and Accountability	No Process Documentation nor Preventative Risk Analysis or Controls in Place
<b>Audit of Effectiveness Results</b>	35%	4	1.4	While Independent Audit Have Occurred in the Last 12 Months, Remediation of Issues is Not in Place, Audits are Limited	No Comprehensive Independent Audits or Validation of Risks/Controls has Occurred in Last 12 Months	No Independent Audits and Validation has Occurred in Last 2 Years, Past Issues/Root Cause Unresolved
<b>Ability to Anticipate Risk</b>	30%	4	1.2	Risk can be Anticipated and Foreseen; Ability to Mitigate Before Risk Gets Out of Control	Patterns of Risk are Predictable if Not Foreseen; Risk Can Be Mitigated Before Getting Out of Control	Risks are Unforeseen but Can be Partially Mitigated Before Getting Out of Control
<b>Total:</b>	<b>100%</b>		<b>3.65</b>			

Likelihood Ratings are guesses and should be used with caution. The question to consider is whether you can handle the risk incident if it occurs and to what degree have you mitigated the risk in terms of identifying, reducing the impact.

Impact Model	Weighting	Rating Score	Negligible - 1	Minor - 2	Moderate - 3	Significant - 4
<b>Safety</b>	40%	1	0.4	Limited to No Safety Risk Concerns or Incidents; Minor Treatable Injuries	Inherent Safety Risk Not Believed to Involve Life or Limb Even if Instructions / Warnings / Manuals Are Not Followed	Limited Risk to Life or Limb Exists for Associate or Customer if Instructions / Manuals / Warnings Not Followed
<b>Product Quality / Customer Impact</b>	15%	3	0.45	More Likely That Product Consistently Exceeds Customer and Regulatory / Industry Guidelines; High Level of Customer Satisfaction is Achieved	More Likely That Product Generally Meets Customer Expectations While Achieving Regulatory/Industry Guideline; Risk of Episodic Failures for Specific Units	Inherent Risk That Product Does Not Meet Customer Expectations and Periodically Fails Regulatory/Industry Expectations
<b>Reputational</b>	10%	3	0.3	Limited Brand Damage Risk, Limited to Individual Clients or Circumstances	Brand Damage Risk Impacting Sales That Can Be Easily Mitigated	Brand Damage Risk That Can Be Mitigated with Deliberate Effort and Resource Expenditure Over the Course of a Year; Sales Impacted
<b>Financial Results / Valuation</b>	35%	4	1.4	Inherent Risk of Loss Less Than \$50,000	Inherent Risk of Loss >\$50,000 but <\$500,000	Inherent Risk of Loss >\$500,000 but <\$1 Million
<b>Total:</b>	<b>100%</b>		<b>2.55</b>			

19

19

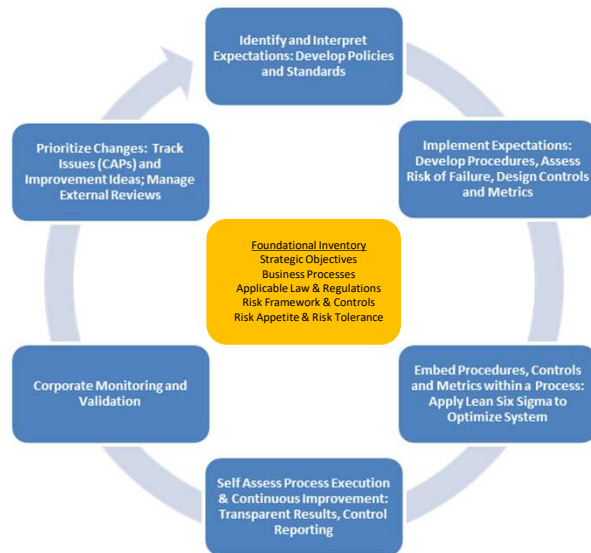
## A Process View Helps Identify the Accountable Risk

- Understanding Process Accountability
  - Department / Organization Hierarchy VS
  - Process
    - Supply Chain
    - Manufacturing Chain
    - Sales
  - Any risks or requirements (strategic, operational, financial, compliance) should be seen and managed across the business process.

20

20

## Process Accountability



Process Accountability is an Organizational Design Discussion

- What should line management be doing?
- What should corporate be doing?
- What centralized / aligned processes should we have?

21

## Polling Question 2:

- Who is primarily responsible for your compliance program?
- We have a dedicated Chief Compliance / Ethics Officer.
- Our General Counsel also services at the Chief Compliance Officer.
- Internal Audit primarily oversees the Compliance effort.
- The Compliance Program is a side item for selected leaders – no one is focused on the effort.
- We do not have a compliance program.

22

## Evaluating Your Compliance Program



23

23

## Federal Sentencing Guidelines

Federal Sentencing Guideline Element
Risk Assessment Process
Policies and Procedures
Training and Communications
Confidential Reporting & Investigations
Third Party Management
Mergers and Acquisitions
Commitment by Management
Compliance Resources
Incentives and Disciplinary Measures
Continuous Improvement and Periodic Testing
Investigations & Root Cause Analysis



24

24

## Review Your Organization's Documentation

- Measure your program's documentation against the Federal Sentencing Guidelines (FSG) elements.
- List of documents may include:
  - Compliance plan
  - Code of conduct
  - Compliance policies and procedure
  - Compliance personnel job descriptions
  - Compliance committee charter
  - Compliance department reports to management and the board
  - Compliance department work plans
  - Prior risk assessments conducted
  - Reports related to hotline calls
  - Documents related to any past government agency investigations or audits



25

25

## Evaluate Program Structure

- Ensure that each of the FSG elements are addressed.
- In an established program assess personnel responsible for administering the program:
  - Identifying personnel responsibilities
  - Background and experience of personnel
  - Appropriate staffing levels
  - Workflow
  - Challenges staff encounter in performing their duties



26

26

## Evaluate Program Structure

- In a **new program** focus on identifying and fulfilling staffing needs. Some areas to include:
  - What staffing is needed to meet each element?
  - Has any staffing been approved in the budget?
  - What resources are available for recruiting?
  - What does the recruitment process to attract solid candidates look like?
  - Is there a software tool available that may mitigate the need to hire another full-time employee?



27

27

## How Does the DOJ Evaluate Effectiveness?

- Three Areas of Focus:
  - Design - Is the compliance program well-designed?
  - Implementation – Is it applied earnestly and in good faith?
  - Operation – Does it work in practice?



28

28



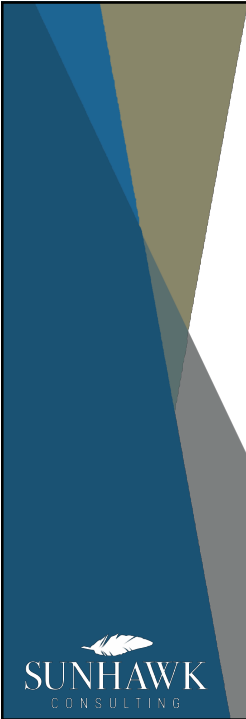
## DOJ and Program Effectiveness - Design

- Is there a risk assessment? Formal or informal?
- Do effectiveness metrics tie to the key risks?
- Are resources prioritized toward high-risk areas?
- Are policies, procedures and expectations well communicated?
- Are compliance failures responded to appropriately?
- Are investigations appropriately conducted, scoped and results addressed?



29

29



## DOJ and Program Effectiveness - Implementation

- Autonomy of compliance personnel (versus management obstruction)
- Adequate resources for compliance program
- Increased risk tolerance for pursuit of new business or revenues?
- Publication of discipline (and causes) and consistent treatment of similar instances of misconduct
- Incentives for compliance performance
- Is the Board and C-Suite engaged?



30

30

## DOJ and Program Effectiveness - Operation

- Are investigations focused on root causes and identifying accountability lapses among supervisory managers and senior executives?
- Is the volume, frequency and scope of audits appropriate?
- Gap analysis for compliance program?
- Organization-wide polling of all employees to determine impression of management's commitment to compliance?



31

31

## Polling Question 3:

Do you use the Federal Sentencing Guidelines (FSG) elements to organize your compliance program?


- A. Yes and we assess how we adhere to the FSG elements, periodically with independent external review.
- B. Yes and we assess how we adhere to the FSG elements, using internal resources.
- C. Yes but we have not assessed how well we adhere to the FSG elements.
- D. No, we have a compliance program but do not align to the FSG elements.
- E. What is compliance? We do not have a compliance program.



32

32





## Governance, Risk and Compliance (GRC) Program Management



33

33



## GRC – Look Beyond Just Compliance

- All compliance programs – whether for small entities or global Fortune 50 organizations – require the same components.
  - Each component needs to be addressed at a level consistent with the risk.
- Focus on building **great business processes that are compliant**, not separate compliance programs that are difficult to sustain.



34

34



## Shift to Embedding Compliance Into the Business

- Create a unified corporate culture across subsidiaries
- Ensure clarity on how compliance is part of corporate strategy
- Ensure clarity on corporate values
- Develop a common risk language
- Engage leaders in proactive consideration of all risks that may impact corporate strategy and values
  - Strategic
  - Operational
  - Financial
  - Compliance



## Incorporating Compliance Into the Business

### Enterprise Risk Management

- Business leaders should be discussing risk holistically.
- Compliance matters should have their distinct place within that discussion.

### Governance, Risk and Control Methodologies

- Controls and monitoring should give compliance risks the appropriate weighting.
- When using GRC software systems, compliance matters should be embedded in overall operations dashboards – not separate modules / systems.

# What Does Success Looks Like.....

## Enterprise Risk Management

- Conversations about risk happen normally throughout the day.
- We have clarity on current corporate level risks.
- We have clarity on each department / plant key risks.
- Risk tolerance is understood.
- We have driven long term value creation by appropriately managing all categories of risk.

## Compliance Program

- We demonstrate in word and deed how we align with expectations for a corporate compliance program.
- The compliance program supports and reinforces our shared values toward our employees, customers and shareholders.

## Employee Engagement

- We track and understand the level of employee engagement.
- We have a high level of employee engagement based on clear expectations, trust and shared purpose.



37

37

## Enterprise Risk Management – Risk Framework Categories

A risk framework is used by leadership teams, departments, process owners, and division leaders to proactively brainstorm specific risks to the achievement of objectives. Resources and time should then be prioritized to appropriately mitigate those specific risks.

Strategic Risks	Operational Risks	Financial Risks	Compliance Risks
<b>Planning Risks:</b> <ul style="list-style-type: none"> <li>• Strategic Planning &amp; Forecasting</li> <li>• Business Portfolio Change</li> <li>• Competitor Actions</li> <li>• Economic Conditions</li> <li>• Industry Consolidation</li> <li>• Industry Disruption</li> <li>• Global, Macro &amp; Micro Trends                             <ul style="list-style-type: none"> <li>• Social</li> <li>• Technological</li> <li>• Economic</li> <li>• Environmental</li> <li>• Political</li> </ul> </li> </ul> <b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Leadership &amp; Succession Planning</li> <li>• Organizational Design</li> <li>• Authority &amp; Limits</li> <li>• Product Development Lifecycle</li> <li>• Stakeholder Relations</li> <li>• Brand &amp; Reputation Management</li> <li>• Social Responsibility</li> </ul>	<b>Planning Risks:</b> <ul style="list-style-type: none"> <li>• Operational Planning &amp; Forecasting</li> <li>• Innovation, Continuous Improvement, &amp; Learning</li> <li>• Insights, Data Analytics, &amp; Consumer Research</li> <li>• Client Satisfaction, Provider Satisfaction &amp; Perfect Service</li> <li>• Product Safety &amp; Liability</li> </ul> <b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Perfect Service Culture</li> <li>• Account Management</li> <li>• Intellectual Property</li> <li>• Process Management</li> <li>• Technology Management</li> <li>• Vendor Management</li> <li>• Facilities Management</li> <li>• Human Resources Management</li> <li>• Supply Chain Management</li> <li>• Sales Inventory Management</li> <li>• Sales Channel Prospecting &amp; Sales Execution</li> <li>• Associate Health &amp; Safety</li> <li>• Product Safety</li> <li>• Business Interruption</li> <li>• Fraud, Waste &amp; Abuse</li> <li>• Acquisition Integration</li> </ul>	<b>Planning Risks:</b> <ul style="list-style-type: none"> <li>• Financial Planning &amp; Forecasting</li> <li>• Working Capital Forecasting &amp; Management</li> <li>• Sales Pipeline Forecasting</li> <li>• Capital Availability</li> <li>• Lending Covenants</li> <li>• Investor Goals</li> </ul> <b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Capital Allocation &amp; Resource Prioritization</li> <li>• Pricing and Underwriting</li> <li>• Administrative Cost Containment</li> <li>• Financial Reporting Accuracy</li> <li>• Accounts Receivable and Payable Management</li> </ul>	<b>Planning Risks:</b> <ul style="list-style-type: none"> <li>• Regulatory Forecasting</li> </ul> <b>Execution Risks:</b> <ul style="list-style-type: none"> <li>• Ethical Conduct</li> <li>• Securities Regulations</li> <li>• Regulatory Filings – Financial</li> <li>• Construction Regulations</li> <li>• Information Security</li> <li>• Privacy Regulations</li> <li>• Contract Adherence</li> <li>• Litigation</li> <li>• Advertising Laws</li> <li>• OSHA / Employee Regulations</li> <li>• Fraud Prevention</li> </ul>

38



38

## Polling Question 4:

Do you have an Enterprise Risk Management Program in Place?

- A. Yes – We have a well-established ERM program.
- B. Yes – but the ERM program is focused on non-compliance risks.
- C. Yes – but the ERM program is new / immature.
- D. No – but we plan on starting an ERM program.
- E. No – and there is no plan to start an ERM program.



39

39

## Is There Alignment on Metrics to Monitor?

Governance Area	Financial Metrics	Operational Metrics	Satisfaction Metrics	Compliance Metrics
Audit	✓	✓	✓	✓
Compliance	✓	✓	✓	✓
Business Operations	✓		✓	?
Quality		✓	✓	?
Safety		✓		?
Risk Management	✓		✓	?
Executive Committee	✓		✓	?
Board	✓		✓	?

How is compliance monitoring embedded into all oversight groups?  
How is compliance serving its role as the second line of defense?



40

40

## Tools and Templates Options

### Desktop Systems

- Risk Category Frameworks (PowerPoint)
- Compliance Risk Assessment (Excel Spreadsheet)
- Policy (& Standard) Template (Word Document)
- Process / Control Narrative (Word Document)
- Executive Team / Board Report Format (PowerPoint)

### Enterprise (GRC) Systems

- Centralized Data / Documentation Repository
- Company Wide Documentation Access
- Company Wide Tracking and Alerts



41

41

## Various System Tools for Compliance Functions

- Reporting mechanisms – hotline
- Repository for tracking reported issues
- Education and training materials
- Repository to manage policies
- Repository for documenting investigations
- HIPAA Risk Assessment Tool



42

42

## How Does an Integrated GRC Infrastructure Approach Support Our Risk Philosophy?

### Infrastructure Functional Goals

- Scalability
- Ease of Use
- Ease of Modification
- Ease of Reporting

### Infrastructure Total Cost of Ownership Considerations

- Reduce Number of Platforms
  - Reduce Upkeep Costs
  - Reduce Associate Fatigue / Learning
  - Reduce Silos of Knowledge
  - Create Shared Experience
- Reduce Data Entry
  - Enter once
  - Answer many (reporting templates for each constituent)



43

43

## Compliance Program Effectiveness - Board Governance Perspective

- When presenting to Board or Audit/Compliance Committee, does management team:
  - Identify highest risks? How often are these reassessed?
  - Clearly articulate organization's risk tolerance?
  - Explain how these risks are being managed to the level of desired exposure (no such thing as zero risk)?
  - Describe process for evaluating effectiveness of controls?
  - Provide transparency around changes in risk profile or control failures?



44

44

## Keep In Mind....

- The Board is expected to know what a sound compliance program looks like
- The Board is expected to know how to infer from management's reports and answers to questions – the true extent of the compliance program's capabilities
- The Board is expected to know the organization's risk tolerance and how that risk tolerance aligns with stakeholder expectations
- Organizations with issues generally have Board's that missed having a deep discussion around the respective risk area



45

45

## Special Situations That “Test” Compliance Effectiveness and Board Oversight

- Mergers and Acquisitions
  - What compliance due diligence is performed? Scope?
  - Who performs it? Qualifications?
  - What is plan to address identified issues?
- Third Party Vendors (e.g., Revenue Cycle, Billing, information security, etc.)
  - Rationale for using?
  - What vetting process used? Does contract reflect this?
  - Monitoring and process for addressing red flags?



46

46

## Top Questions Board Members Should Ask

- What issues exist that we have not discussed?
- What is the biggest risk we believe we have well managed and why?
- If you had one more staff to monitor or audit an additional area or dive deeper into an area – what area would that be and why?
- How do you know your auditing and monitoring investment meets established criteria for conducting compliance efforts / audits / investigations?
  - What external peer review of your work is conducted?
  - What did the latest peer review report say about our organization?



47

47

## Today's Other Presentations:

9:45 AM MST: An FBI Perspective on the Current Cyber Landscape, Threats and Trends

11:00 AM MST: Ethics Reporting and Incident Management, Marketing, Benchmarking, and Best Practices

1:00 PM MST: Connecting Corporate Culture with the Bottom Line

2:15 PM MST: Anti-Corruption / Anti-Bribery

3:30 PM MST: Compliance Work Plan and the Board: a Compliance Committee Toolkit



48

48





## Recap and Questions

- Why do we pursue excellence in Governance, Risk and Compliance?
- Compliance Risk Assessment for Your Organization
- Evaluating Your Compliance Program
- Governance, Risk and Compliance (GRC) Program Management



49

49



## Available Educational and Operational Tools

- Compliance Program Assessment Tool – Cross Walk to DOJ Expectations
- Metrics That Matter – Metrics for Compliance Programs
- Enterprise Risk Management Category Examples



50

50

## Questions:

- James Rose,  
Managing Director, SunHawk Consulting LLC  
[James.Rose@SunHawkConsulting.com](mailto:James.Rose@SunHawkConsulting.com)
- Steve James,  
Director of Internal Audit, Cavco Industries Inc



51