Control Systems That Fit Company Culture

Martin Espinosa

Polycom

VP, Chief Audit Executive & Chief Compliance Officer

Polycom™

Profile (Industry and Role)

Companies (High Tech & Semi-conductor - Reinvention):

- Polycom (CAE, CCO - $1.4B, 3,747 employees, $10.49 Stock)
- Electronic Arts (CAE - $4.1B, 9,200 employees, $17.13 Stock)
- Avago Technologies (CAE - $2.4B, 3,600 employees, $31.38 Stock)
- Yahoo! (SOX Director (IT & process) - $5B, 11,700 employees, $23.75 Stock)

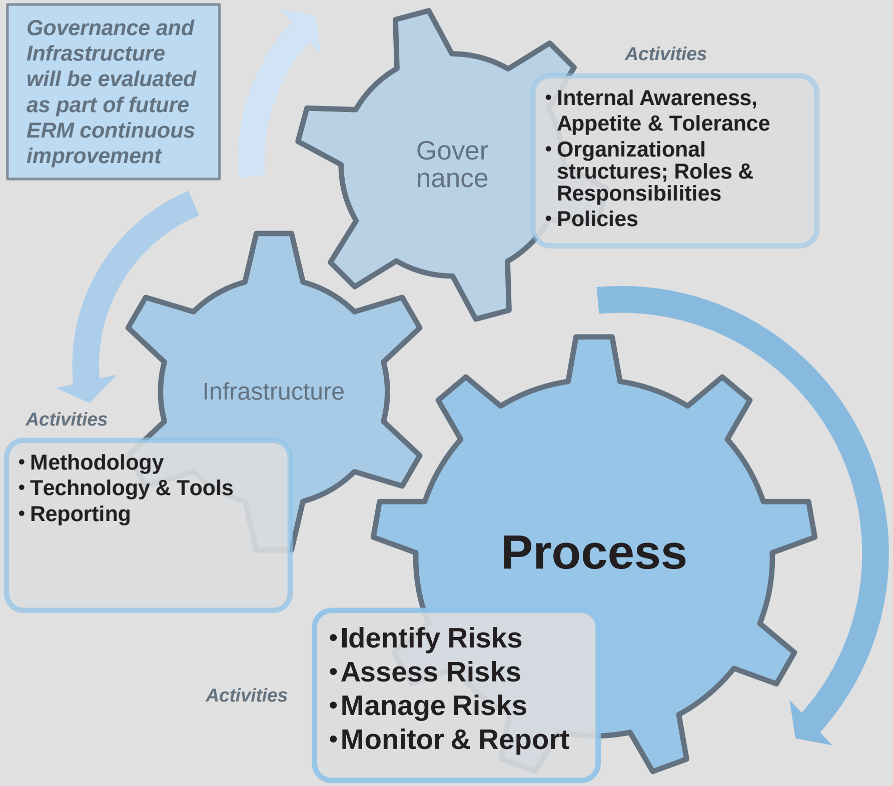
Characteristics:

- Rapid growth companies (Revenue, Customers, M&A, Life Cycle)
- Rapidly changing products/technologies (Widgets to SW to Cloud)
- High Wall Street expectations (Hot Topics, Products, Reporting, etc.)
- Transformation environments (skills, controls – finance and operations, systems, training, experience (age) and operational/financial reporting)

Keep in Mind (All relative to your Organization)

Behavior	**Considerations** (Where we spend more time)			
Maturity (Organization, Processes, etc.)	**Fewer is more** (Focus on important items)	**Evolution not Revolution** (Pace & Acceptance)	**Execute in the framework of your company** (Language, processes, etc.)	• Understand companies ***maturity and complexity*** (Be Agile) • ***Link to objectives and processes*** (Make it real) • ***Right skill sets for the right job*** (May require new skill sets)
Necessity				• ***Education*** at all levels (Consequences and impact) • ***Mandate*** ("Use the Audit Committee Mandate don't abuse it") • ***Simplify*** for the audience (Complicated = misunderstanding or fear)
Prioritization				• ***Sponsorship and partnering*** (Shared benefits and accountability) • ***Build Credibility*** (Act, listen and do) • ***Achievable*** – Risk based approach (Don't overreach)
Complexity				• ***Leverage existing frameworks*** (COSO, etc.) • ***Actions are executable and have owners*** (Accountability) • ***Simplify*** for the audience (Complicated = misunderstanding or fear)
Details				• ***Simplify*** for the audience (Complicated = misunderstanding or fear) • ***Deliverables that are usable*** (Not shelf ware) • ***Leverage/integrate into existing processes*** (They exist)

ERM Program Elements/Activities


Governance and Infrastructure will be evaluated as part of future ERM continuous improvement
Gover nance
Activities
• Internal Awareness, Appetite & Tolerance
• Organizational structures; Roles & Responsibilities
• Policies
Infrastructure
Activities
• Methodology
• Technology & Tools
• Reporting
Process
Activities
•Identify Risks
•Assess Risks
•Manage Risks
•Monitor & Report

- An effective ERM Program includes a risk management framework consisting of **Governance**, **Infrastructure** and **Process**, subject to monitoring and oversight, and matures based on continuous improvement
- Current year enhancements to **Process** activities (Governance and Infrastructure have activities in place)

Objective is to optimize existing ERM Process to increase the efficiency of effort required by the Risk Owners and provide the Risk Committee with an increased level of assurance that committed actions to manage risks are progressing according to plan.

ERM: Example – Less Mature

Model Criteria	Current	Desired State	Traditional ERM
Internal Risk Factors	✓ (Broad, 10K) 🟩	• (Risk Categories)	✓ (Very specific)
External/Environmental Risk Factors	✓ 10K identifies external risk factors 🟩	• 10K identifies external risk factors, ratings & industry trends	✓ (Very Broad and Analytical Process)
Risk Management Reporting	✓ (CFO) 🟥	✓ (Audit Committee & Risk Committee)	✓ (Board, Board Risk Committee & Risk Committee)
High Level Gross Risk	✓	✓	✓
Detailed Risk (business process level)	– 🟨	✓ (Partial)	✓ (Full)
Focus on Awareness	✓	✓	✓
Focus on Detail Management (Sub committees)	– 🟥	✓ (Risk Owners)	✓ (Full Committees)
Business Objectives/Strategies	– 🟩	✓ (Partial)	✓ (Full Alignment)
Leverage Existing Processes	✓ (Financial processes) 🟨	✓ (Financial Processes, QBR and IA Risk Assessment)	✓ (Additional Processes)
Qualitative Measures	✓ (Partial)	✓	✓ (Detailed)
Quantitative Measures	– 🟩	✓ (Leverage Existing Where Applicable)	✓ (Broader More Detailed)

ERM: Example – More Mature

Criteria		Company X	Traditional ERM *
Risk Identification	√	Process ensures risk portfolio is complete	Identified in the objective setting process
	√	10K process makes transparent external risk factors & general industry trends	Considers both internal/external events
	√	Categorized using COSO categories	Organized by categories (type)
Assessment Criteria	√ +	Implicit in “Impact” rating Make impact and likelihood explicit in risk template	Considers impact and likelihood
Assess Risk	√ +	Implicit in existing risk template (“Impact”) Use basic qualitative measures for impact and likelihood (e.g. H, M, L)	Uses quantitative and qualitative measures
	√	Implicit in existing risk template (“Assessment”)	Assessed on gross risk and residual risk basis
	√ +	Implicit in current risk committee & audit committee reporting Leverage explicit qualitative measures to illustrate risk relationships via dashboards	Presents risk interactions
Respond to Risks	√ +	Included in existing risk template Clarify existing controls from risk response action items and simplify	Ownership, action items, timelines
	√	Included in existing risk template (streamline for ease of use)	Activity level metrics to monitor risks
Monitoring	√	Risk Committee consisting of key players (executives)	Risk committee oversight
	√ +	Part of IA Audit Plan Prioritize/categorize risk response actions; enhance IA quarterly oversight	Internal Audit oversight

**** Not necessarily a required minimum as an ERM program should be tailored based on size and structure of the entity; also, criteria activities can be more advanced towards “leading” ERM practices***

✓ Aligned with Traditional + Optimization opportunity

What's the path? (Execution & Removing Excuses)

- ***Agree/Align with key clients on desired state*** (Alignment and Mandate)
- ***Understand cost if desired state*** ($, time, effort & executive commitment)
- Use ***consistent standard measurements*** (Maturity index, Standard ERM language, COSO language, or rating criteria = Not having to explain yourself)
- ***Leverage other industry trends*** (Lines of defense, Assurance language, etc.)
- ***Strike the balance of substantive review and risk coverage*** (make sure you are doing enough to make it real)
- ***Make it repeatable and flexible*** (document, evolve, etc.)
- ***Ensure you have a close loop process*** (Can it be monitored, is there accountability, follow up process, etc.)
- ***Consultants:*** Don't let them tell you what you need – know what you need! (Manage It)

Lesson’s learned?

- ***There is no one right answer***
- *It has to fit* ***yours and organizations priorities***
- **Communicate** (over and over again – assume they have other priorities)
- **Benchmark** when possible (confidence to position or create urgency)
- ***Are the bare minimums in place*** (Build foundation along with a path)
- ***Make sure there is ‘buy in’*** (Educate/Communicate to everyone – formal & Informal)
- ***Form over function – make sure it makes sense?***
- ***Always question and evolve*** (Continuous/Incremental improvement)
- ***Mix/blend of methods or standards*** (Standard yet unique)
- Trust others input – ***validate, validate, validate!!!***
- You/they are ***managing a portfolio*** (Time, attention & cost – Pick your battles)

Control Systems That Fit Company Culture

Bavan Holloway Vice President, Corporate Audit

The Boeing Company

BOEING

COMPLIANCE WEEK 2013

POWERFUL INSIGHTS, PRACTICAL IDEAS, REAL SOLUTIONS

#CW2013

Overview

About Boeing

- World's leading aerospace company and largest manufacturer of commercial jetliners and military aircraft
- Design and manufacture rotorcraft, electronic and defense systems, missiles, satellites, launch vehicles and advanced information and communication systems
- Customer support in 150 countries with more than 170,000 Boeing employees in 50 states and 70 countries

About the Environment

- Increasingly complex and punitive regulations
- Emerging global requirements and enforcement
- Growing customer expectations
  - Compliance as a core competency
  - Early and effective business partner engagement
  - Compliance embedded into the businesses processes

BOEING

Boeing Leadership Attributes

A Boeing Leader:

- Charts the course
- Sets high expectations
- Inspires others
- Finds a way
- Lives the Boeing values
- Delivers results

Boeing Leadership Attributes

A Boeing Leader

Lives the Boeing Values

- Models, leads, and is committed to the Boeing values, principles and business conduct policies
- Earns the trust and respect of all Boeing stakeholders
- Ensures effective business, compliance and financial controls
- Promotes integrity in all that we do
- Demonstrates commitment to and takes advantage of diversity
- Creates an environment of respect and inclusion
- Does not use abusive or intimidating behavior
- Bounds vigorous pursuit of individual and business objectives with overall interest and reputation of the company

BOEING

Boeing Leaders Leading

- Enhance performance by enabling an open workplace culture
- Align business performance expectations with behaviors
- *The same principles that drive performance also drive an ethical and compliant work environment*

BOEING
Speak Up
Done the right way, at the right time, speaking up can help shape a positive work environment.
Ethics@Boeing

Posters

Videos

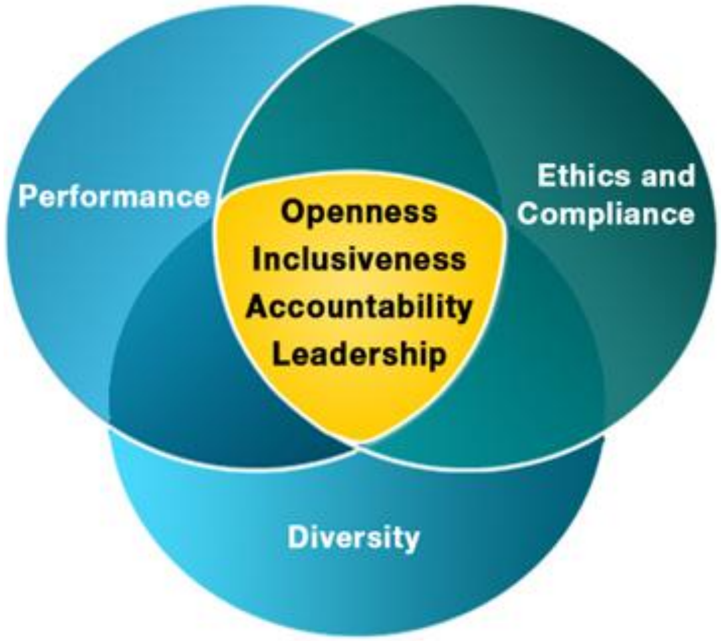
Employee Perspectives

The Ethics Report: Is this manager holding a grudge?

Ethics Report

Boeing Corporate Audit

- Focusing on functional excellence
  - Right people, right skills
  - Coverage of key risks
  - High assurance of compliance
- Delivering better service to our customers
- Supporting strong operational performance



Functional Excellence Journey

2009 | 2010 | 2011 | 2012 | 2013 | -------> Ongoing

2009
- Tools/process benchmarking
- Core Data Analytics Team
- Standard client surveys

2010
- GRC workflow tool
- Continuous monitoring projects
- Advisory services

2011
- Flexible model
- Competency assessments
- Unannounced audits

2012
- Rolling risk assessment
- Professional certifications
- Operational metrics

2013
- Project Mgmt. tools
- Standard work
- Integrated resource management

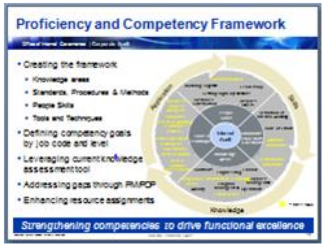
Ongoing
- Enhanced processes/tools
- Improved capabilities & competencies
- Integrated Assurance
- Employee engagement

BOEING

Control Self Assessment
Open House

BCA Tanker Proposal
March 15, 2010
Location: 45-801 11D14
Time: 8:00 – 4:00

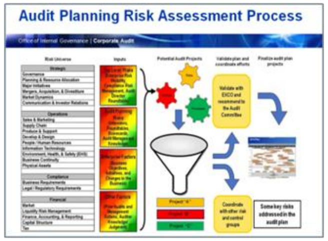
Hosted by Corporate Audit


Proficiency and Competency Framework

Office of Internal Governance | Corporate Audit

- Creating the framework
  - Knowledge areas
  - Standards, Procedures & Methods
  - People Skills
  - Tools and Techniques
- Defining competency goals by job code and level
- Leveraging current knowledge assessment tool
- Addressing gaps through PM/PDP
- Enhancing resource assignments

Strengthening competencies to drive functional excellence


Audit Planning Risk Assessment Process

Office of Internal Governance | Corporate Audit

Risk Universe
Strategic
Governance
Planning & Resource Allocation
Major Initiatives
Mergers, Acquisition, & Divestiture
Market Dynamics
Communication & Investor Relations
Operations
Sales & Marketing
Supply Chain
Produce & Support
Develop & Design
People / Human Resources
Information Technology
Environment, Health, & Safety (EHS)
Business Continuity
Physical Assets
Compliance
Business Requirements
Legal / Regulatory Requirements
Financial
Market
Liquidity Risk Management
Finance, Accounting, & Reporting
Capital Structure
Tax

Inputs
Top Level Risks
Audit Planning
Enterprise Factors
Business Objectives, Initiatives, and Changes in the Business
Other Factors
Potential Audit Projects
Validate plan and coordinate efforts
Finalize audit plan projects
Validate with EXCO and recommend to the Audit Committee
Project "A"
Project "B"
Project "C"
Coordinate with other risk and control groups
Some key risks addressed in the audit plan

Making progress to be a valued integrator

BOEING

Control Systems That Fit Company Culture

Jose Tabuena

Orion Health

Chief Compliance Counsel | *CW* Columnist

ORION HEALTH™

Control Systems That Fit Company Culture

Technology *culture* – what does that mean?

“You can find it on the Woki (our Wiki)”

“It’s already been installed”

“Isn’t there an app for that?”

“I thought we were a technology company?”

Control Systems That Fit Company Culture

Need for Controls –

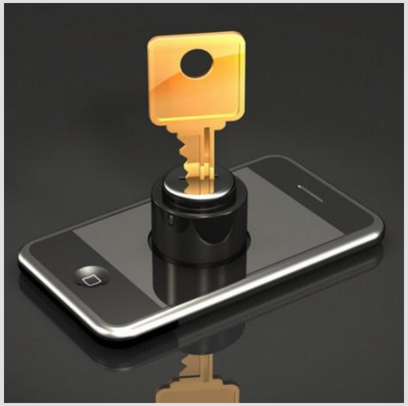
- Assist customers in implementing software products that support the protection of patient health information
- Security and privacy laws vary within each country and most U.S. states have specific requirements, in addition to federal laws and regulation
- Services have evolved to include maintaining sensitive health information as a SaaS vendor (a 3rd party risk our customers need to manage)

Control Systems That Fit Company Culture

Initial Approach

Access controls alone should protect

Thou must not access | use | disclose PHI



Control Systems That Fit Company Culture

Reality Check

- Recognize realities of environment (customer interaction) makes it challenging to limit access
- Without access to certain health data employee effectiveness is inhibited and customer satisfaction impacted
- Technology not the total panacea

Control Systems That Fit Company Culture

Uh... Sam, when they say we're supposed to eat our own 'dog food'... oh, never mind.
Pirillo & Fitz
ALPO

© BLAUGH.COM · FITZ & PIRILLO · SAVE 10% AT GODADDY BY USING THE COUPON CODE "BLAUGH"

Control Systems That Fit Company Culture

Information Security Workgroup

- Mapping data; risk analysis – *When* does PHI need to be accessed? *How* is it accessed?
- Role-based access protocols
- Need-to-know access supported through policy and education
- If technology controls limited, more stringent compensating controls and monitoring instituted