HCCA's 12th Annual COMPLIANCE INSTITUTE

APRIL 13–16, 2008 | NEW ORLEANS, LA | HILTON RIVERSIDE NEW ORLEANS

Enterprise Risk Management
A Practical Approach to Implementation

Kelly Nueske, LarsonAllen LLP

Steven LeFar, MediRegs – Wolters Kluwer Law & Business

Jenny O'Brien, Halleland Lewis Nilan & Johnson

HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

www.hcca-info.org | 888-580-8373

HCCA
2008
New Orleans
COMPLIANCE
INSTITUTE
April 13–16, 2008
www.compliance-institute.org
888-580-8373

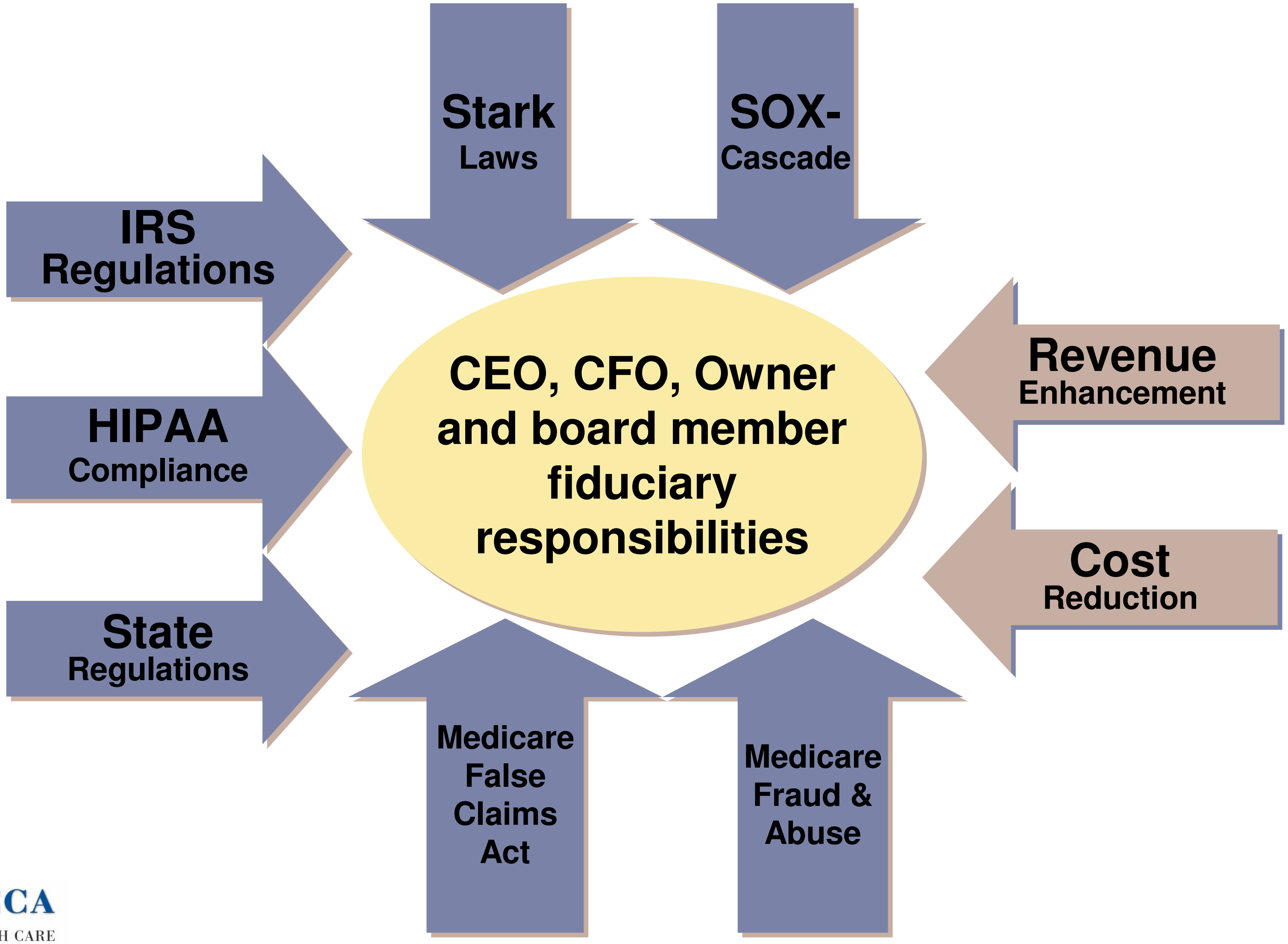
Presentation Outline

- Today's Healthcare Environment
- What and Why ERM
- COSO's ERM Framework
- Board Involvement
- Healthcare Risks
- Process
  - Phase I: Governance & Structure
  - Phase II: Assessment Tools
  - Phase III: Deliverables

Today’s Healthcare Environment

- Healthcare organizations are complex
- New challenges and emerging risks
- Financial and operational well being at risk
- Continually changing reimbursement rules and increasing state and federal regulations
- Educated consumers asking for more
- IRS scrutiny of tax exempt status
- New accounting standards
- Technology improvements
- “Expectation gap” between producers of information and users of information

Healthcare Regulatory Environment



CEO, CFO, Owner and board member fiduciary responsibilities

Leading Providers

- Understand the risks most pertinent to their organization
- Manage the risks in an integrated fashion
- Prioritize risk management efforts around
  - Risks having the biggest potential impact
  - Risks most likely to occur

Enterprise Risk Management Concepts

Managing today's healthcare risks can be a competitive advantage

.

What is Enterprise Risk Management?

- Holistic approach to identifying risk – more than regulatory compliance, financial, medical liability, patient safety, general liability or SOX
- Creates a portfolio view of risks
- Identifies interrelationships and interdependencies among risks
- Offers ability to manage risks within and across business units
- Improves organization’s ability to identify and seize opportunities – competitive edge

What is Enterprise Risk Management?

- Considers risk in the formulation of business strategy
- Method to achieve business objectives
- Involves all levels of management
- Process to identify, analyze, mitigate/manage, measure and communicate risks across organization
- Measurement of risks includes severity and magnitude of impact
- Can eliminate duplicates efforts [Internal Audit, Compliance, Risk Management]

Benefits of Enterprise Risk Management

- Successful risk identification & mitigation become key elements of a strategic plan
  - Competitive advantage for those with ERM capability & discipline
  - Mitigate downside exposure and capitalize on upside opportunities
- Reduced financial losses
- Improve business performance
- Enhanced risk identification and assessment processes
- Improved awareness and collaboration
- Improved decision making and accountability
- Improved regulatory compliance

Risk of No Enterprise Risk Management

- All risks are a threat if ignored
- Bankruptcies
- Fraud
- Restatement of earnings
- Decrease business valuation
- Loss of customers
- Careers destroyed
- Lack credibility in market

COSO’s ERM – Integrated Framework

- COSO [Committee of Sponsoring Organizations of the Treadway Commission] is a voluntary private sector organization that encompasses five professions
  - American Accounting Association
  - American Institute of CPAs
  - Financial Executives International
  - Institute of Internal Auditors
  - Institute of Management Accountants

COSO ERM – Integrated Framework

- States “ERM is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.”

COSO ERM Components

- Internal Environment – entity’s risk culture and risk appetite
- Objective Setting – risk appetite is considered during objective setting
- Event Identification – internal & external events are identified that present risk or opportunity & are included in strategy & objective setting process
- Risk Assessment – likelihood & impact of risks on established objectives

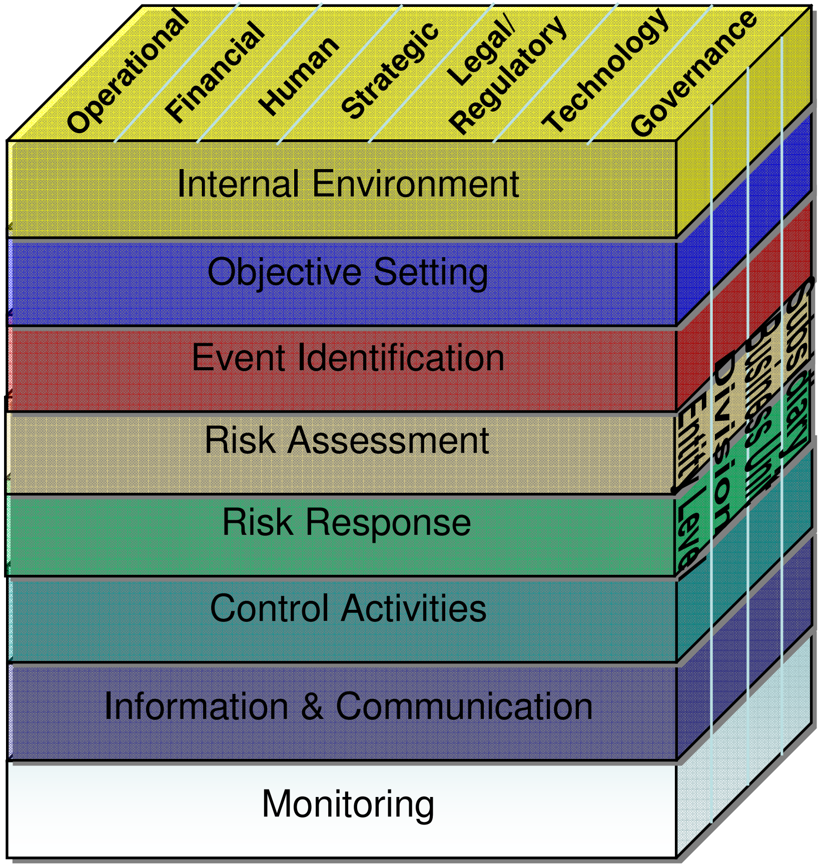
COSO ERM Components

- Risk Response – decision whether to avoid, accept, reduce or share risk
- Control Activities – policies are established to ensure management’s risk responses are carried out
- Information & Communication – thorough & timely communication to support effective execution of roles & responsibilities
- Monitoring – ongoing with modifications made as necessary

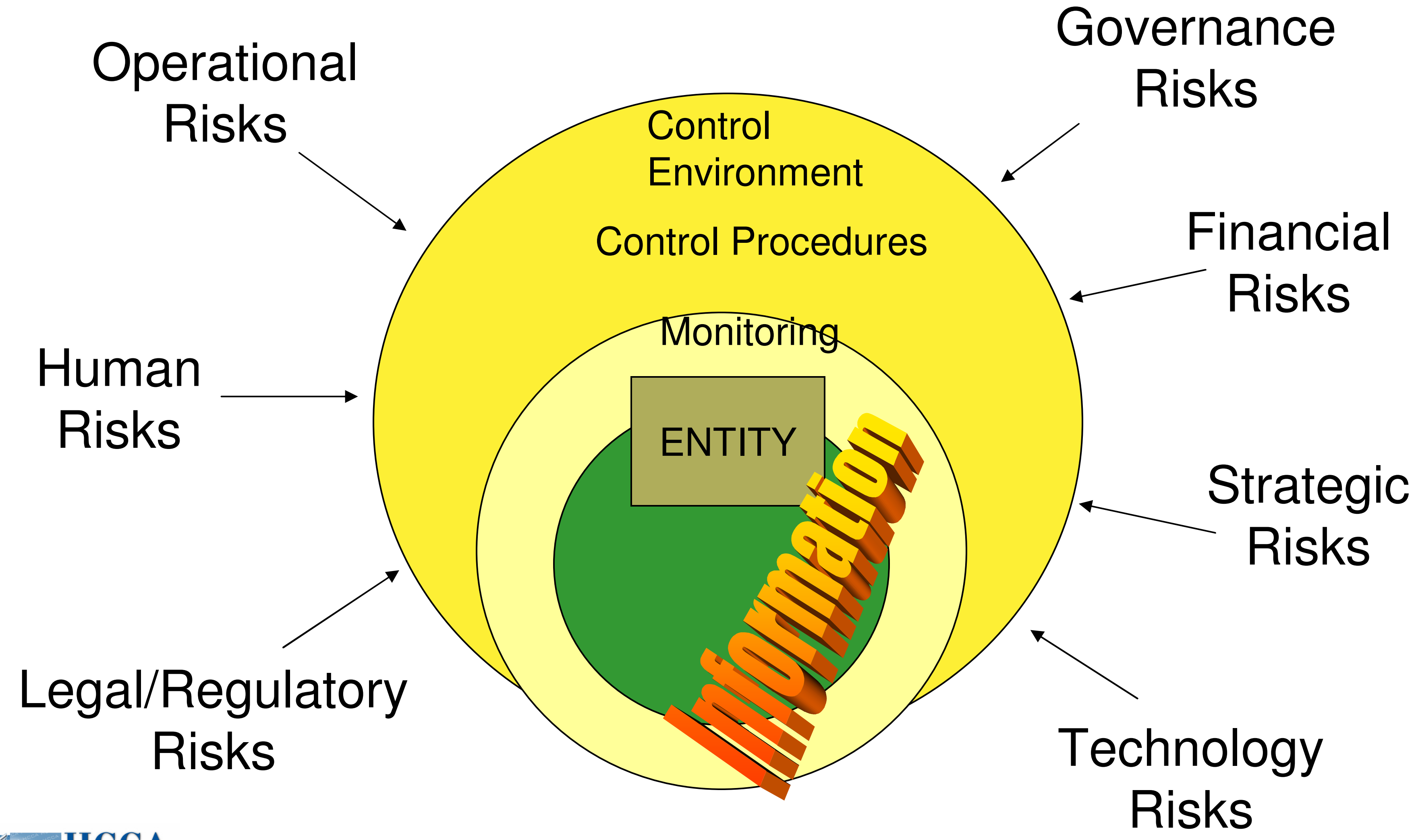
COS Risk Domains - Expanded

- Operational – core business including systems and processes. Example: outpatient care
- Financial – ability to earn, raise or access capital. Example: bonds
- Human – recruiting, retention and managing workforce. Example: worker's compensation
- Strategic – ability to grow and expand. Example: joint ventures
- Legal/Regulatory – statutory, regulatory compliance, licensure, accreditation. Example: HIPAA, OSHA, JC
- Technology – biomedical & information technologies. Example: CPOE
- Governance – board and committee structure, and roles and responsibilities. Example: Audit Committee Charter

ERM Components & Expanded Risk Domains



Risks and Control



Who is responsible for ERM?

- Everyone!
- Board of directors provide guidance, direction and monitoring
- Audit Committee, Risk Committee or full board receive “dashboard” on risk and establish risk tolerance
- CEO has ultimate ownership and sets tone for ERM process
- Each level of management stays informed and takes ownership of risks at their level
- Chief Risk Officer, if one exists, is facilitator and challenger of process
- Risk Management Team comprised of CEO, CFO, COO, CRO, CIO, CNO, CMO, etc to oversee and support process

Board Involvement

There are growing pressures for boards to be smarter, more transparent and more rigorous in their pursuit of great governance.

Organizational Readiness for ERM

- Success depends on organization’s readiness
  - Is the Board requesting a risk management strategy for organization?
  - Is CEO and executive team willing to lead & take ownership for the process? [not an Internal Audit responsibility]
  - Is risk approach proactive or reactive?
  - What is the risk tolerance?
    - Profitable organizations are willing to tolerate more volatility
    - Expressed in level of self-insurance

Boards of Directors Fiduciary Role Questions

- What do we hold in trust, and for whom?
- What are the fiduciary, but non-financial roles of our boards and committees?
- How do we know the organization is fulfilling its mission?
- Does a proposed initiative effectively advance our mission?
- What safeguards do we have in place to avoid well publicized fiduciary failures?
- If we held an annual stakeholders meeting, what would we say about the fiduciary performance and the board’s effectiveness as a steward?
- What is the evidence that we are a trustworthy organization? What are some examples of times in which we earned the title “trustworthy”?
- What are our major financial vulnerabilities? What are we doing as an organization and a board to address them?
- Even though we are not bound by Sarbanes-Oxley, are there some provisions we should adopt?

Governance Challenges: Which Fit?

Many decision makers

Complex regulatory compliance issues

Competition for stakeholders’ loyalty

Geographic distance and demographic diversity

Large capital requirements

Calls for faster, smarter, and more ethical, more transparent and cost-effective governance

Tough fiscal pressures

Need stability with growth

Press to deliver on economies of scale

Growing government, media, and bond holder interest in performance

Need to deliver on promise of mission for caring and curing

Press for diversity of experiences & views of our staff and board

Calls for enhanced quality and safety

Six Core Board Responsibilities

- Determine the future of the organization
- Ensure the quality of clinical care and customer service
- Protect the financial health of the organization
- Ensure effective executive leadership and management
- Develop, improve, and perpetuate an effective governance function
- Reflect the community served and strengthen relationships with key stakeholders

HCCA's 12th Annual COMPLIANCE INSTITUTE

April 13–16, 2008 | New Orleans, LA | Hilton Riverside New Orleans

Building an Enterprise Risk Management Program

A Practical Approach for Leading Providers

HCCA
HEALTH CARE
COMPLIANCE
ASSOCIATION

www.hcca-info.org | 888-580-8373

HCCA
2008
New Orleans
COMPLIANCE
INSTITUTE
April 13–16, 2008
www.compliance-institute.org
888-580-8373

Nature of the Risk

- Risk is universal
- Risk is not properly identified and managed by most organizations, including governments
- Need a common risk vocabulary
- Need improved risk management methodologies
- Risks are diverse & inherent to the business operations
- If non-clinical risks are not managed they are just as hazardous as clinical risks

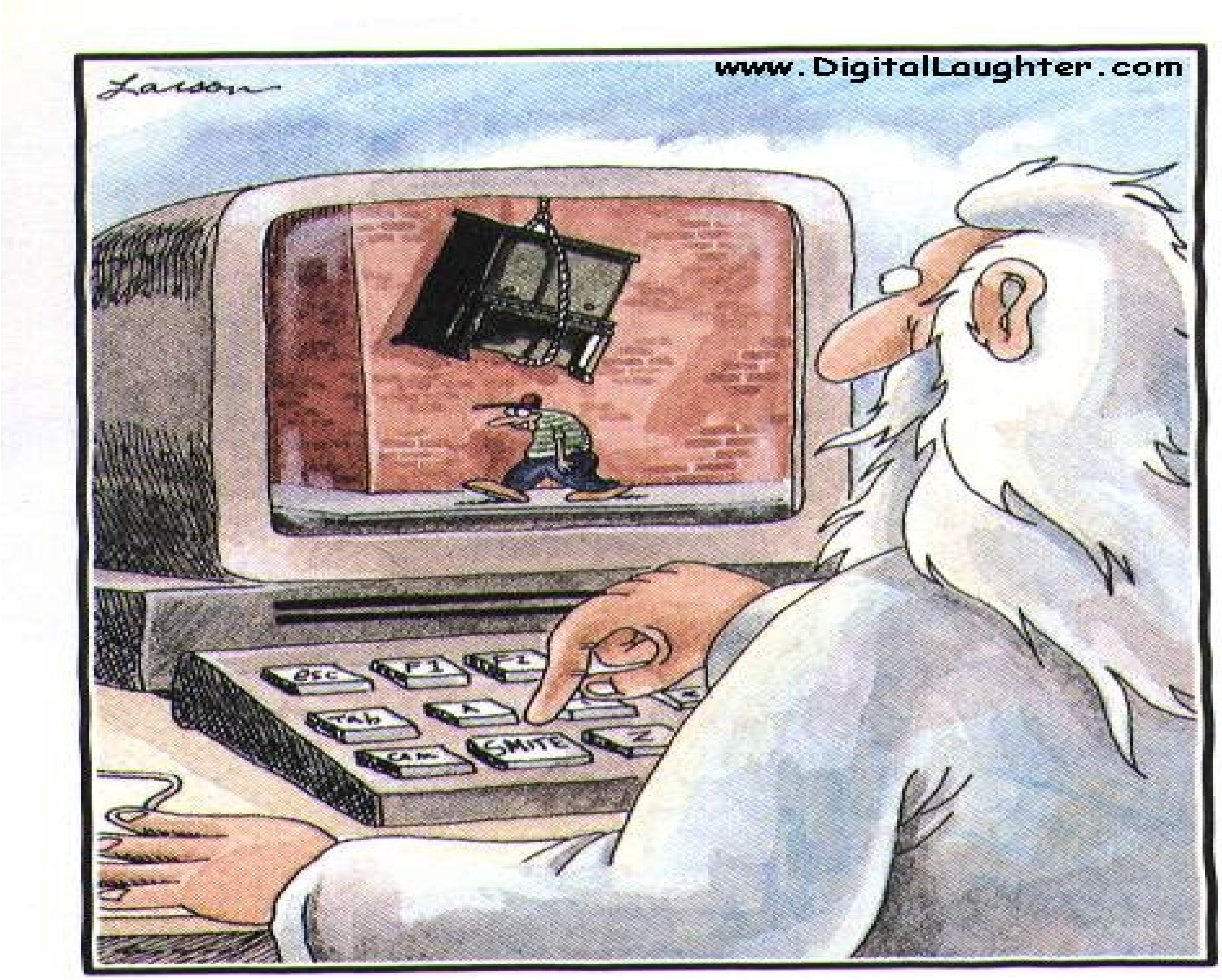
Internal Risks

- Policies and Procedures
  - Internal controls
- Contracting
  - Vendor Relationships
  - Physician Relationships
- Financial Reporting
  - Financial Statements
  - Tax Returns
  - Cost Reports
  - Investor Reporting
  - Credit Risk
  - Liquidity Risk
- Crisis Management Program
  - Business Continuity Plan
- Human Resource Management
  - Hiring & Terminations
  - Employee Relations
- Governance
  - CEO Succession
- Clinical Practices
  - Quality
  - Core measures
  - Evidence Based
- Information Technology
  - Security
  - Disruptions
- Document Management

External Risks

- Office of the Inspector General
- CMS
- State Health Department
- OSHA
- EPA
- Investors
- CCAC
- Litigators
- Past Employees
- HIPAA
- IRS
- Auditors
- Competition

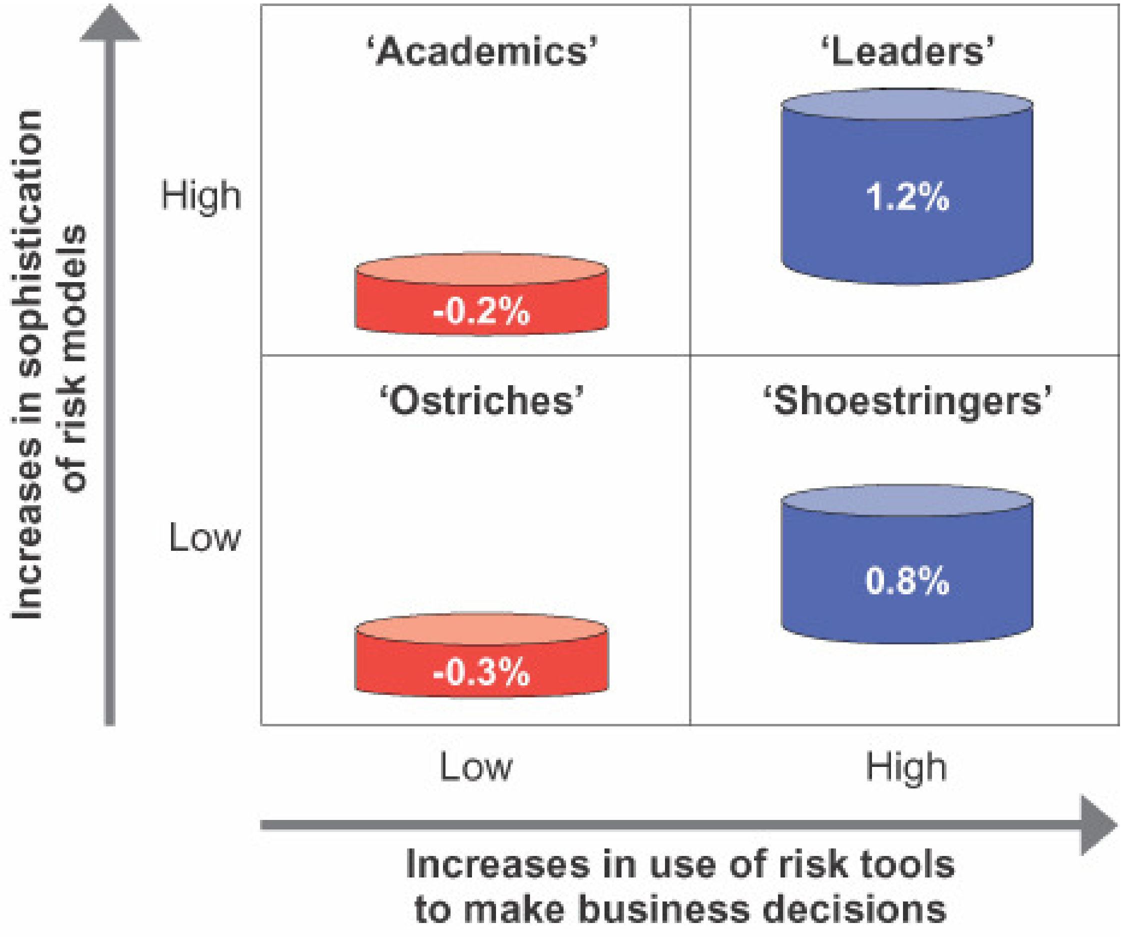
What About the Unknown?



God at His computer

Managing Risk Can Improve Results

Annualized total shareholder returns (1998-2003) for differing degrees of risk model sophistication and risk tool usage



Source: PA Consulting Survey of Global Banks

Misunderstanding Risk is Devastating

- Subprime Debacle– Some Win—Some Got Killed
  - Countrywide
  - Washington Mutual
  - Merrill Lynch
  - Goldman Sachs
- Black Swans
  - Beyond the unexpected
  - Exposure to positive and negative unknowns

Compliance Manages Risk

- Risk Assessment: Estimating the probability of an event occurring and the magnitude of effects if the event does occur. (Probability x Loss)
- Risk Management: Process of identifying, assessing, and controlling risks arising from operational factors and threats and making decisions that balance risks and costs with mission benefits. From the US Army

  - Compliance: Adherence to a set of rules, processes or procedures to control or mitigate risk that is determined by either internal or external forces.
  - The debate: IS COMPLIANCE A JUDGEMENT CALL LIKE MUCH OF RISK MANAGEMENT IS?

And Do It All Day, Everyday

Current Risk Managers

- Finance
- Compliance
- Internal Audits
- Risk Management
- Construction
- Treasury
- Security
- Case Management
- Medical Affairs

Risk Approaches Used

- TQM
- Six ∑
- Policy and Procedure
- Accounting Controls
- Portfolio Theory
- Game Theory
- Scenario Planning
- Clinical/critical pathways

What’s Really Different?

Current

- Siloed
- Board oversight often limited
- No infrastructure
- No standards
- Lack of rigor and quantitative analyses

ERM

- **Integrated** view of risk-across the organization
- **Stratification** of Risk into a portfolio
- **Systematic, rigorous, continuous, coordinated** well defined **process**
- **Senior Leadership Owns It**
- **Linked to strategy and business objectives**

A Simple Framework

- Set Scope
- Determine Approach
- Execute the Assessment
- Develop Mitigation Plan
- Monitor

Enterprise Risk Management Approach

Phase 1 – Implement governance and reporting standards

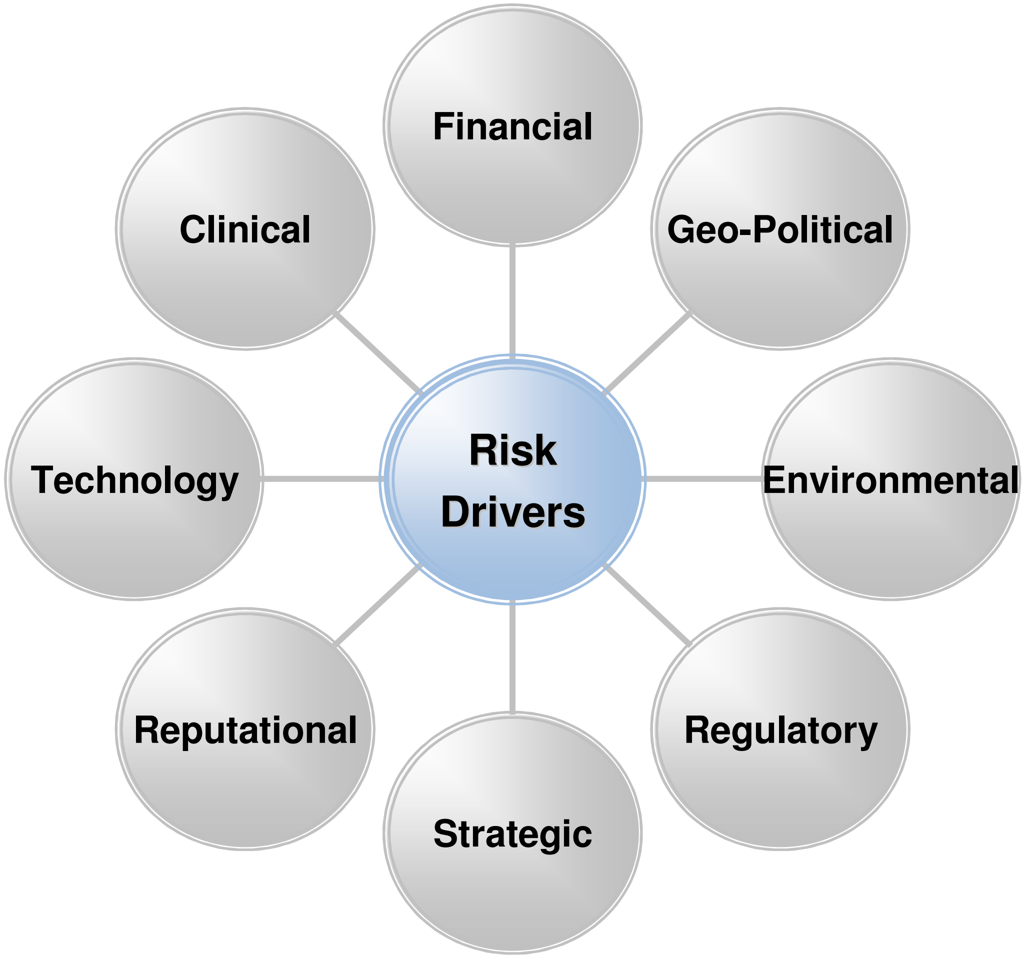
Phase 2 – Enterprise-wide risk assessment that engages all levels of management and all divisions of organization

Phase 3 – Implementation of risk mitigation plans, monitoring and reporting

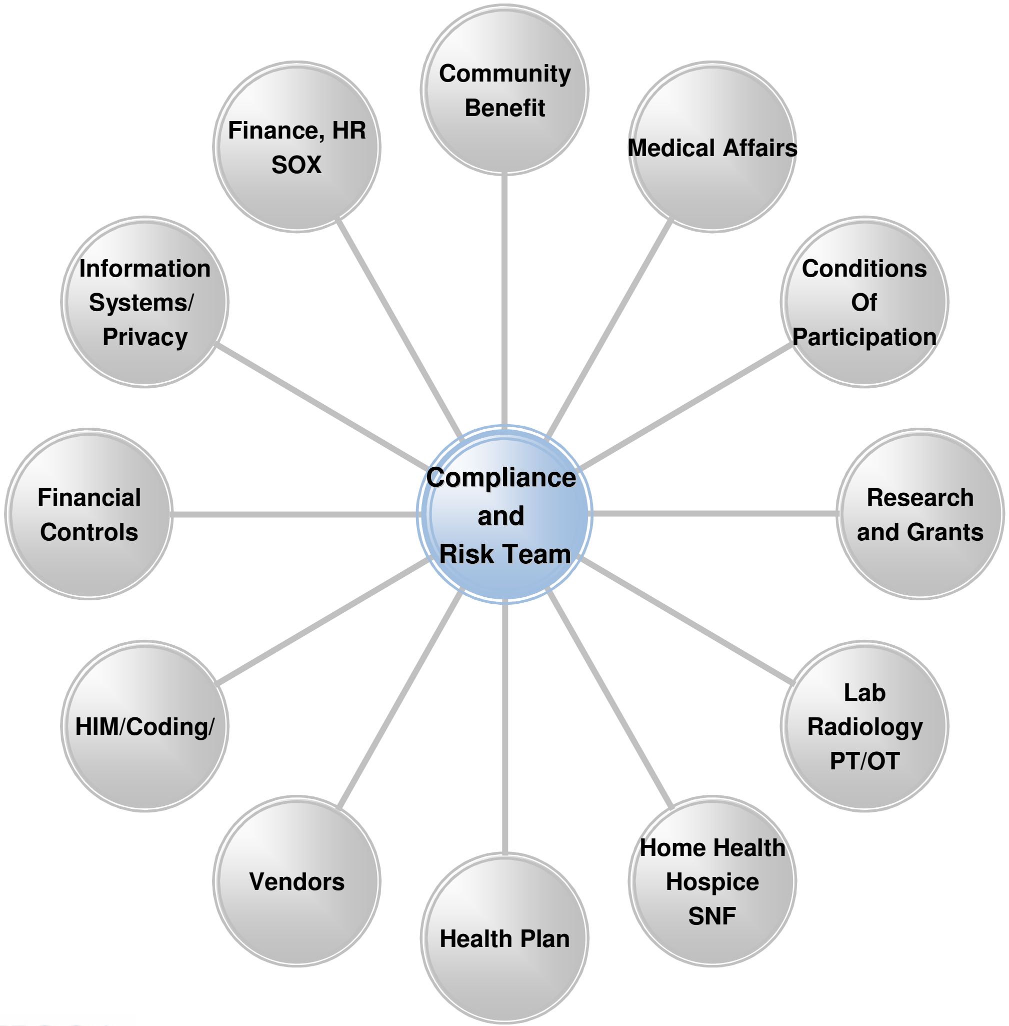
Phase I: Governance and Structure

- Establish Board or Committee responsibility
  - Receives "dashboard" report from management on risk
  - Reviews risk tolerance
- Establish a management's risk committee to oversee the program
  - Composition includes leaders from major operations (CEO, CFO, COO, CCO, CNO, CMO, CIO, etc)
    - CEO should chair
    - Limit to a manageable size (5 to 8)
  - May have subcommittees that support the overall enterprise risk management structure

Phase I: Set Scope



Phase I: Set Scope



Phase I: Determine Approach

Structure

- Trial/Grant
- Departmental
- Process
- Topic

Tools

- Checklists
- 1-1 interviews
- Group interview
- Electronic data gathering/interviews
- What If exercises
- Scenario modeling
- Hazard Assessment

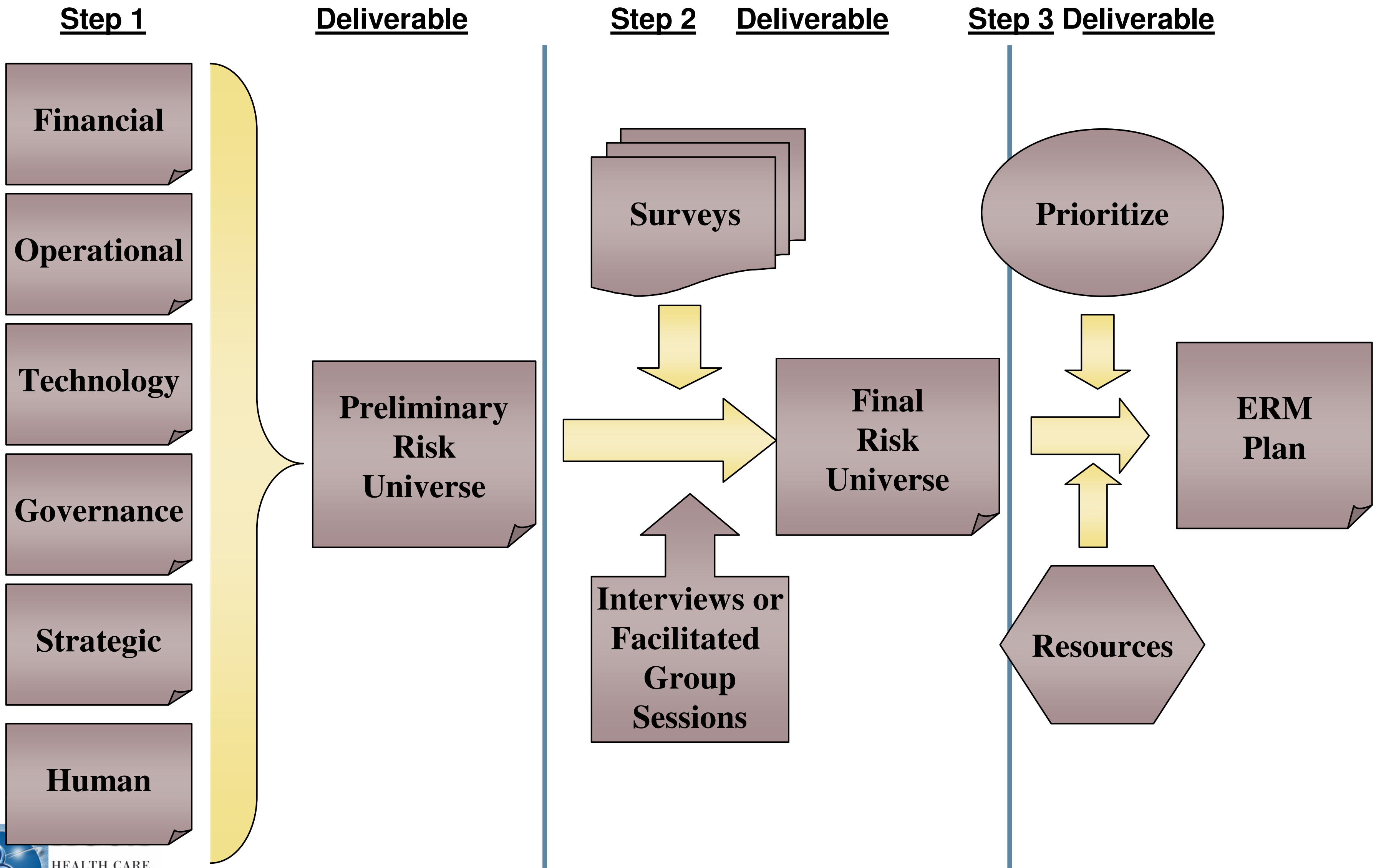
Phase I: Determine Approach

- Probability
  - High, Medium, Low
  - Imminent, Probable, Possible, Unlikely
  - Scary, Unfortunate, Who Cares
- Impact
  - High, Medium, Low
  - Multivariate
    - Financial, Clinical, Reputational, Political

Phase II: Look Everywhere

- Board Members
- Executives
- Vendors
- Partners
- Community Members
- Department Heads
- Employees

Phase II: Enterprise Risk Management Process



Phase II – Enterprise Risk Assessment

Gathering Information on Risk

- Review and understand components of the strategic plans
    - Major acquisitions and consolidations
    - Major initiatives
    - New operations
    - Lines of business outside the norm
    - Significant capital expenditures
    - Vendor and physician relationships
    - Competition and market share information
  - Review financials for trends
    - Revenues
    - Expenses
    - Growth
    - Loss
    - Major initiatives

Phase II – Enterprise Risk Assessment

Gathering Information on Risk (continued)

- Internal and External Audit Findings
  - External auditor's reports: The financial report, management letter comments, significant audit adjustments
  - Internal auditor's reports and findings from prior years
  - Regulatory reports or investigations (CMS, DHS)
  - Survey Results (JC, CLIA, CMS, DHS)
  - Insurance Utilization Reports (general & professional liability)
- Information Technology Plan
  - Major IT initiatives such as system implementations or significant upgrades
  - IT control environment, system security and system password policies

Phase II – Enterprise Risk Assessment

Gathering Information on Risk (continued)

- Operations
  - Capacity (inpatient, outpatient, ED)
  - Revenue cycle performance
  - Technology needs (CT, MRI, surgical)
  - Consulting activities/results
- Human
  - Employee benefit trends
  - Employee satisfaction
  - Turnover rate
  - Vacancy rates (physicians, nurses, technicians, leadership)
- Surveys/software tools to identify risk
  - Email surveys internally on risk
  - Purchased risk assessment tools (software)

Phase II – Enterprise Risk Assessment

Gathering Information on Risk (continued)

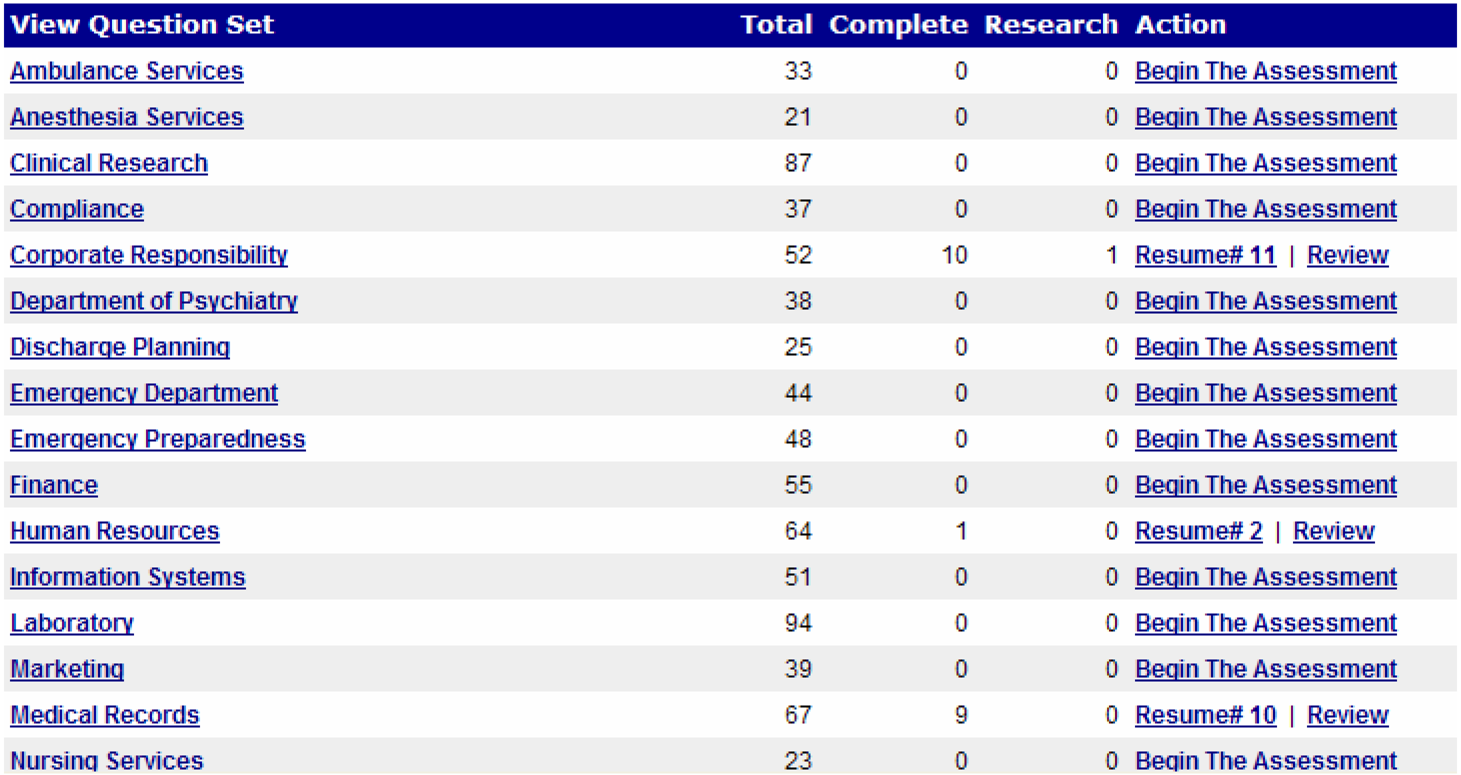
- Clinical Practices
  - Care initiatives
  - Core measures
  - Patient safety, National Patient Safety Goals
  - Evidence based practices
  - Medical staff and medical directors
- Management Interviews
  - The process owner for the processes and business units to be reviewed
  - Typical interviewees: Compliance Officer, Controller, Director of Marketing, Director of HR, Legal, Operations, Director of Research Affairs

Phase II – Enterprise Risk Assessment

Gathering Information on Risk (continued)

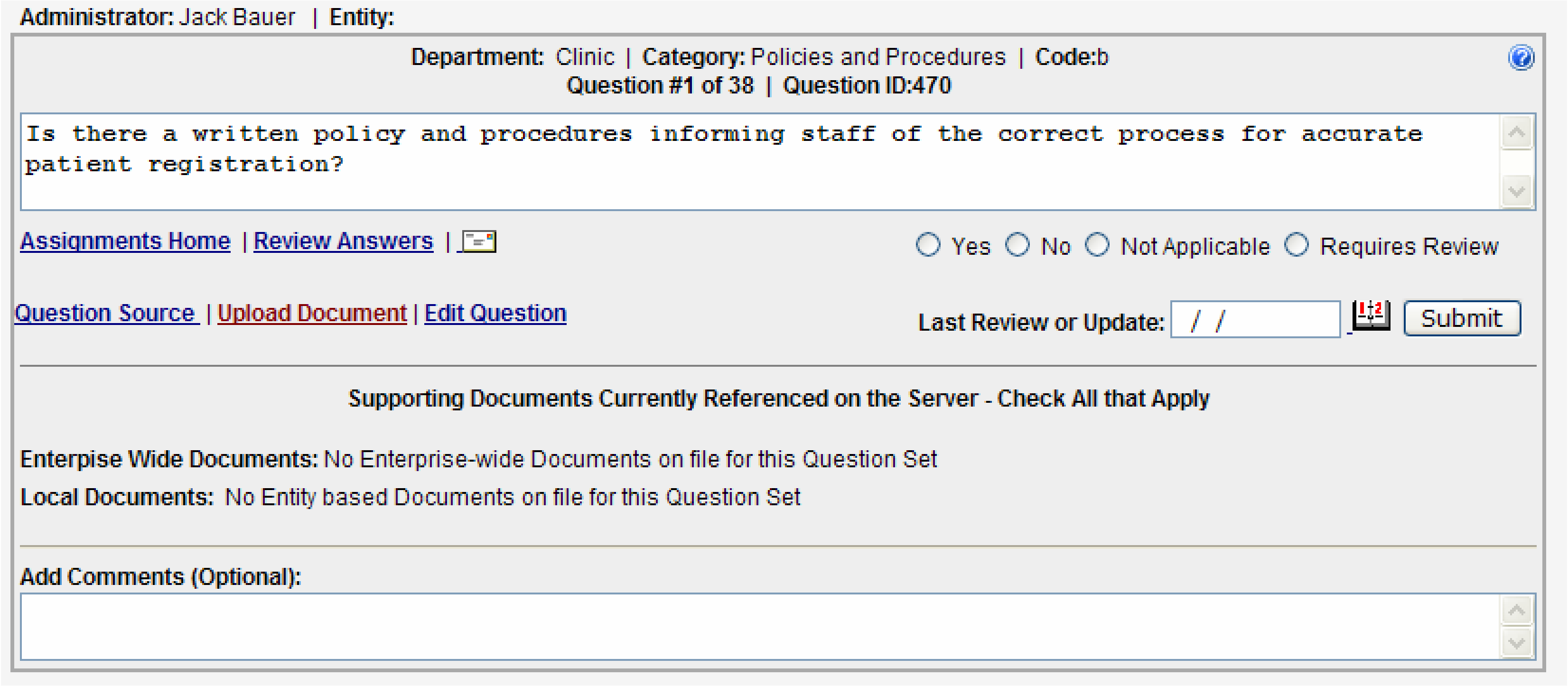
- Minutes from Board and Board Committees
  - Finance Committee
  - Audit Committee
  - Executive Hiring Committee
  - Compliance Committee
- Industry Updates
  - Major communications from regulatory bodies
  - Trade organizations
  - Network with other organizations
  - OIG work plan

Execute: The Power of Automation



View Question Set	Total	Complete	Research	Action
Ambulance Services	33	0	0	Begin The Assessment
Anesthesia Services	21	0	0	Begin The Assessment
Clinical Research	87	0	0	Begin The Assessment
Compliance	37	0	0	Begin The Assessment
Corporate Responsibility	52	10	1	Resume# 11 | Review
Department of Psychiatry	38	0	0	Begin The Assessment
Discharge Planning	25	0	0	Begin The Assessment
Emergency Department	44	0	0	Begin The Assessment
Emergency Preparedness	48	0	0	Begin The Assessment
Finance	55	0	0	Begin The Assessment
Human Resources	64	1	0	Resume# 2 | Review
Information Systems	51	0	0	Begin The Assessment
Laboratory	94	0	0	Begin The Assessment
Marketing	39	0	0	Begin The Assessment
Medical Records	67	9	0	Resume# 10 | Review
Nursing Services	23	0	0	Begin The Assessment

Execute: Electronic Interviews



Administrator: Jack Bauer | **Entity:**

Department: Clinic | **Category:** Policies and Procedures | **Code:**b
Question #1 of 38 | **Question ID:470**

```
Is there a written policy and procedures informing staff of the correct process for accurate
patient registration?
```

Assignments Home | Review Answers |
○ Yes ○ No ○ Not Applicable ○ Requires Review
Question Source | Upload Document | Edit Question
Submit

Last Review or Update: / /

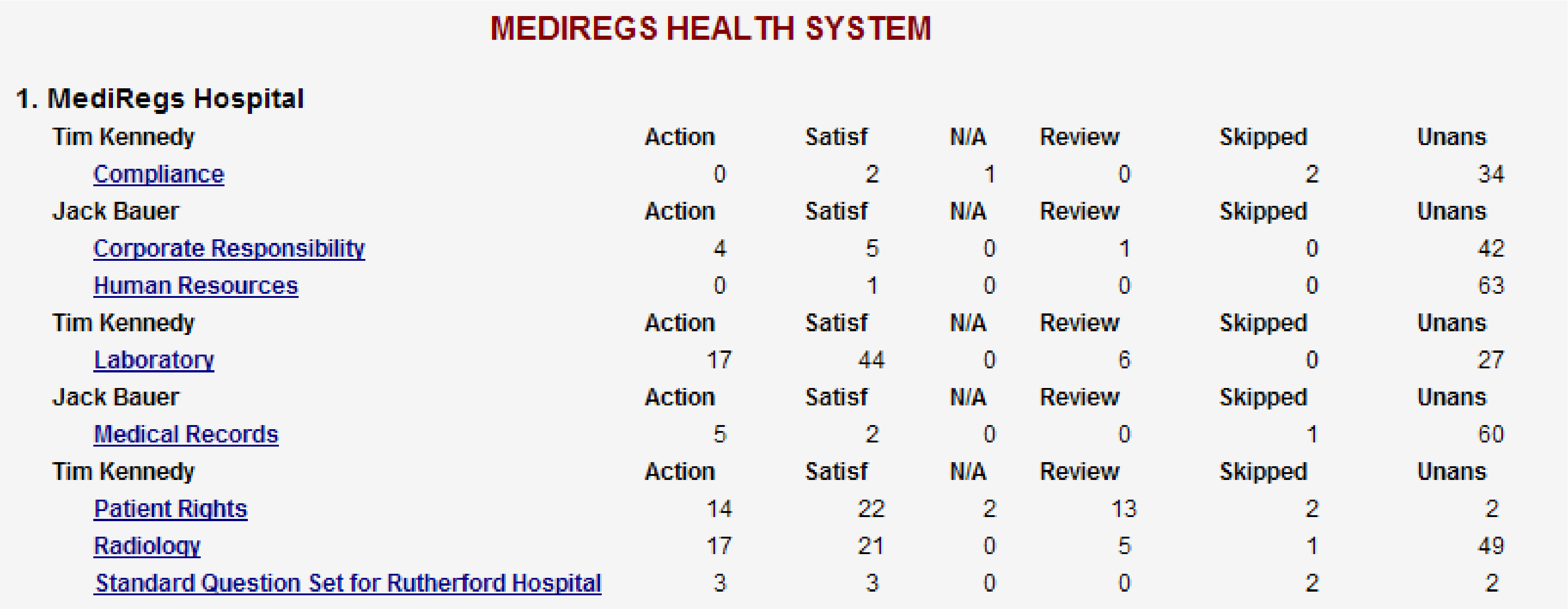
Supporting Documents Currently Referenced on the Server - Check All that Apply

Enterpise Wide Documents: No Enterprise-wide Documents on file for this Question Set

Local Documents: No Entity based Documents on file for this Question Set

Add Comments (Optional):

Execute: Electronic Scoreboards



MEDIREGS HEALTH SYSTEM

1. MediRegs Hospital

Tim Kennedy	Action	Satisf	N/A	Review	Skipped	Unans
Compliance	0	2	1	0	2	34
Jack Bauer	Action	Satisf	N/A	Review	Skipped	Unans
Corporate Responsibility	4	5	0	1	0	42
Human Resources	0	1	0	0	0	63
Tim Kennedy	Action	Satisf	N/A	Review	Skipped	Unans
Laboratory	17	44	0	6	0	27
Jack Bauer	Action	Satisf	N/A	Review	Skipped	Unans
Medical Records	5	2	0	0	1	60
Tim Kennedy	Action	Satisf	N/A	Review	Skipped	Unans
Patient Rights	14	22	2	13	2	2
Radiology	17	21	0	5	1	49
Standard Question Set for Rutherford Hospital	3	3	0	0	2	2

Managing Real Time Risk Amidst the Chaos

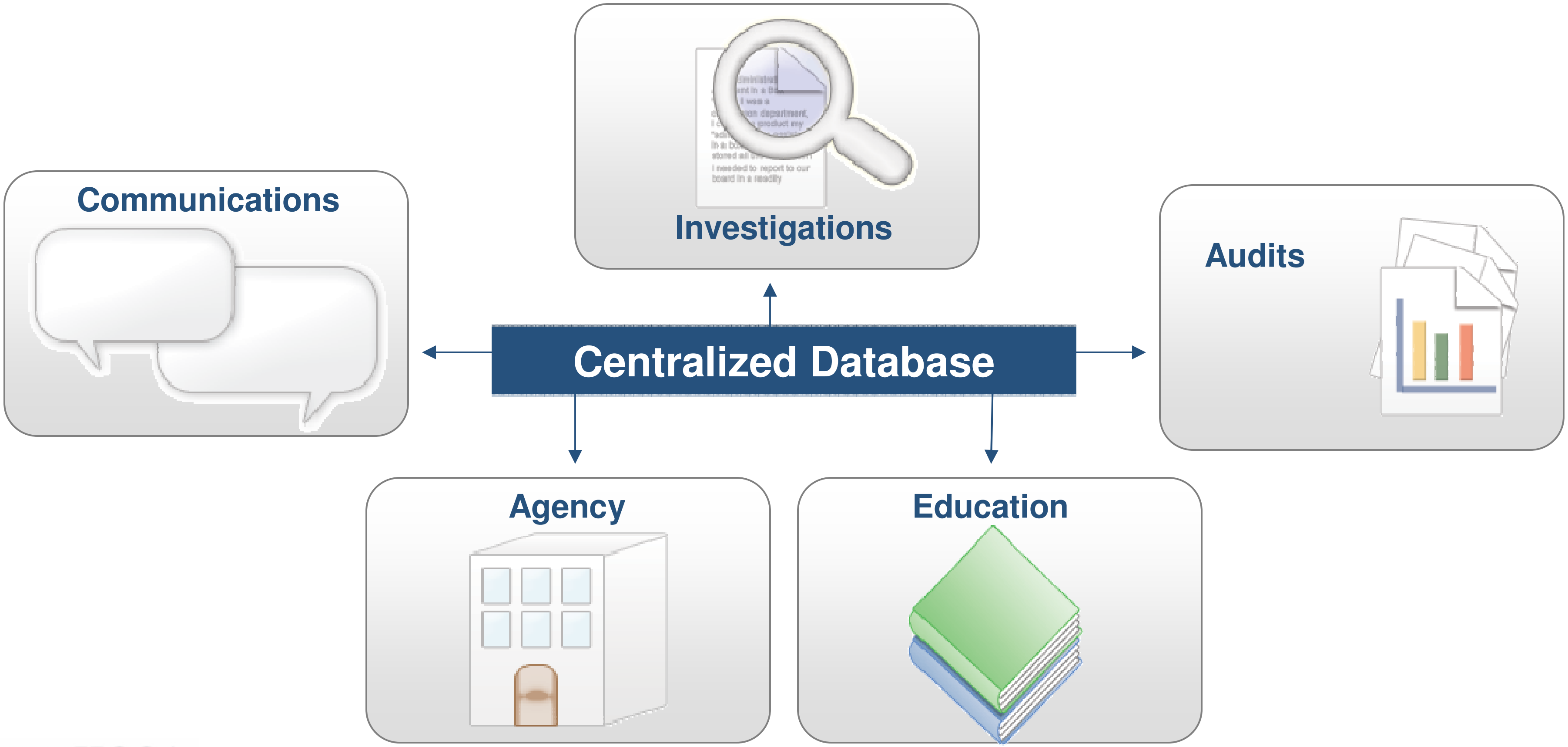
Happenings

> You get told things every day that don't happen. It's printed in the press. The world thinks all these things happen. They never happened. Everyone's so eager to get the story before in fact the story's there that the world is constantly being fed Things that haven't happened. All I can tell you is, It hasn't happened. It's going to happen.

Department of Defense briefing Feb. 28, 2003

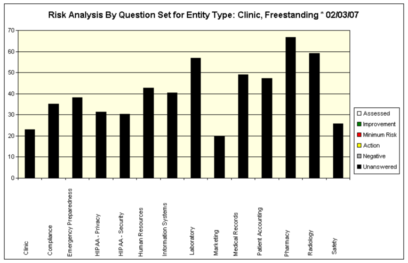
Assessing Real Time Risks Requires Tools

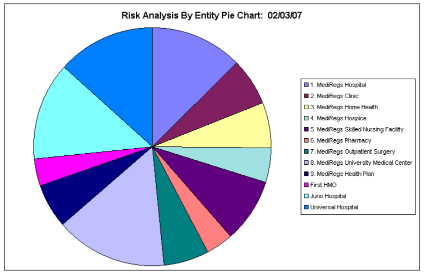
- Integrated end to end management of issues, events, incidents and matters.

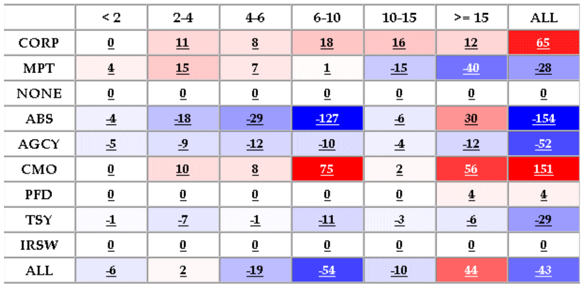


Talking to Management About RA

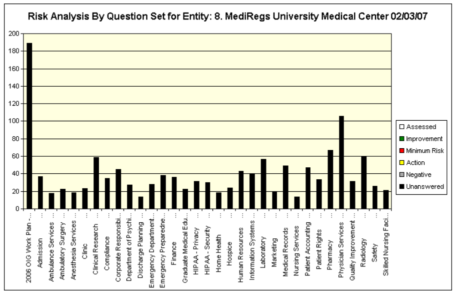
- What is the progress of our assessments?
- What are we assessing and how?
- What are the business risk to our strategies, finances and organization?
- What are the compliance issues?
- What are our significant risks, scenarios or risk events?
- How significant are these risks and what is the impact?
- How should we manage these risks?
- How should we monitor these risks

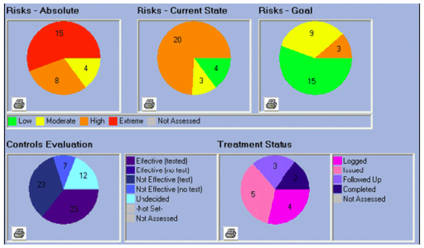

Risk Analysis By Question Set for Entity Type: Clinic, Freestanding * 02/03/07

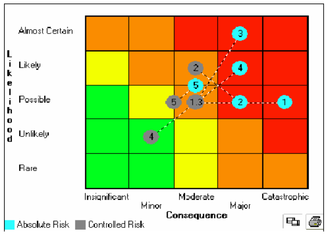

Risk Analysis By Entity Pie Chart: 02/03/07

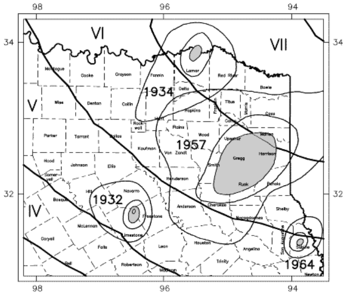


	< 2	2-4	4-6	6-10	10-15	>= 15	ALL
CORP	0	11	8	18	16	12	65
MPT	4	15	7	1	-15	-40	-28
NONE	0	0	0	0	0	0	0
ABS	-4	-18	-29	-127	-6	30	-154
AGCY	-5	-9	-12	-10	-4	-12	-52
CMO	0	10	8	75	2	56	151
PFD	0	0	0	0	0	4	4
TSY	-1	-7	-1	-11	-3	-6	-29
IRSW	0	0	0	0	0	0	0
ALL	-6	2	-19	-54	-10	44	-43


Risk Analysis By Question Set for Entity: 8. MediRegs University Medical Center 02/03/07







Charts Sources: MediRegs and Chief Security Officers.com

Phase II – Enterprise Risk Assessment

- Management risk committee
  - Review compilation of risk data
  - High level validation of risk data
  - Communicate importance/support of facilitation sessions
- Facilitation sessions
  - Includes leaders from all levels and operating units
  - Group leaders by area of specialty or have all evaluate each risk
  - Talk through risks with dialogue so all understand each risk
  - Educate leaders on risk
  - Leaders score risks

Phase II – Enterprise Risk Assessment

- Scoring Risk
  - Can weight each category or treat equally
  - Create scoring criteria and scale (1 – 5)
  - Define criteria example
    - Degree of regulation and compliance
    - Growth and profitability
    - Non-standardized systems, and processes
    - Technology changes
    - Size of business unit
    - Controls, policies and procedures
    - Training
    - Management/employee turnover
    - Management estimates
    - New business objectives and strategies
    - Acquisitions and potential divestitures

Phase II – Enterprise Risk Assessment

- Rating and definition example for Degree of Regulation and Compliance criteria
  - The level of regulatory impact on services provided or business unit
    1. Tasks performed are relatively simple and technical in nature with no special regulatory concerns over the activities of the unit.
    2. Tasks performed are of moderate difficulty and only limited activity in this unit is an area of regulatory concern.
    3. Tasks performed are of moderate difficulty and some of the activities in this unit are areas of regulatory concern.
    4. Tasks performed are somewhat complex and a significant amount of this unit's activities are of regulatory concern.
    5. Tasks performed are complex and are of high regulatory concern. Errors may result in damage to the brand image and/or civil penalties.

Phase II – Enterprise Risk Assessment

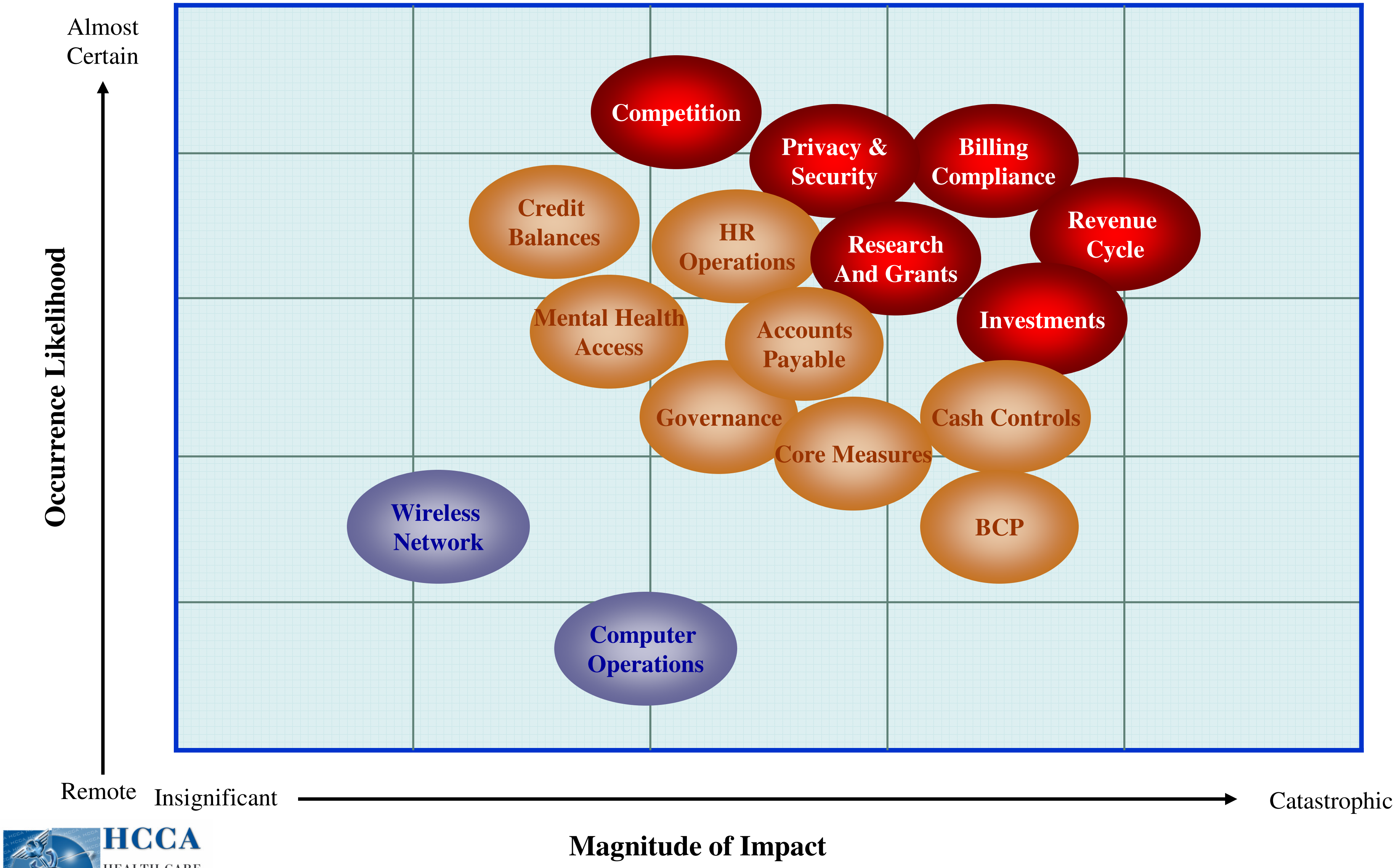
- Compile results from facilitated sessions with leaders
- Review and validate results from facilitated sessions with management risk committee
- Bring leaders together to review scored results
  - Determine which risks are a priority
  - Assign accountability
  - Educate on how to develop a mitigation plan
  - Provide mitigation plan tools that meet organization needs. Include:
    - Tactics
    - Measurement criteria
    - Monitoring activities
  - Set timeline for completion of plans

Example: Identified Risks

- Revenue Cycle
- Privacy & Security
- Billing Compliance
- Grants and Research
- Accounts Payable
- Competition
- Governance (Committee Roles & Responsibilities)
- Business Continuity Planning

- Credit Balances
- Wireless Network
- Computer Operations
- Human Resources Operations
- Investments
- Cash Controls
- Mental Health Access
- Core Measures

Example: Heat Map



Example: ERM Components (Point System)

Risk Area/Project Name	Assign Risk Domain:	Total Points
Revenue Cycle	Financial	655
Billing Compliance	Regulatory	655
Privacy and Security	Regulatory	655
Grants and Research	Financial	625
Competition	Strategic	625
Investments	Financial	610
Business Continuity Plan	Operational	560
Mental Health Access	Operational	560
Core Measures	Operational	525
Cash Controls	Financial	525
Human Resources Operations	Human	520
Accounts Payable	Financial	495
Governance (Committee Charters)	Governance	475
Credit Balances	Regulatory	465
Computer Operations	Technology	445
Wireless Network	Technology	445

Example: Work Plans

Operation's Risk Mitigation Plan

- Revenue Cycle
- Privacy & Security
- Billing Compliance
- Grants and Research
- Accounts Payable
- Competition
- Governance
- BCP
- Credit Balances
- Human Resources
- Investments
- Cash Controls
- Mental Health Access
- Core Measures

Operation's Assumes Risk

- Wireless Network
- Computer Operations

Compliance Work Plan

- Privacy and Security
- Billing Compliance
- Grants and Research
- Credit Balances
- Mental Health Access

Internal Audit Work Plan

- Revenue Cycle
- Billing Compliance
- Grants and Research
- Business Continuity Plan
- Investments
- Cash Controls

Example: Operation’s Risk Mitigation Plan

Privacy and Security

Employee access to electronic medical record

- Accountability:
  - No clear single owner but a number of departments have ownership. Need to designate a lead to be effective (CIO)
- Stakeholders:
  - Chief Information Officer, Chief Clinical Officer, Health Information, Human Resources, Compliance Officer, Legal, Patients, Others …
- Mitigation Strategies:
  - Policy and Procedures, Education and Training, Communication and Awareness, Discipline and Enforcement
- Timeline:
  - Prioritize with other initiatives
- Metrics:
  - Monitor and Evaluate

Grants and Research

Approval process for sponsored research projects

- Accountability:
  - Director of Research Administration or Chief Clinical Officer
- Stakeholders:
  - Chief Clinical Officer, Hospital Presidents, Institutional Review Board, Chief Financial Officer, Billing Office, Registration Lead, Compliance Officer, Research Investigators, Vendor Sponsor
- Mitigation Strategies:
  - Policy and Procedures, Education and Training, Communication and Awareness, Discipline and Enforcement
- Timeline:
  - Prioritize with other initiatives
- Metrics:
  - Monitor and Evaluate

Example: Compliance Work Plan

Billing Compliance

Charging for Observation Services

- Structure: (Program Infrastructure):
  - Policy Development
  - Education and Training
  - Oversight and Reporting Mechanisms
- Process: (How address risk):
  - Risk Assessment
  - Response and Prevention
    - Internal Investigation
    - Corrective Action Plan
    - Enforcement and Discipline
- Outcome: (Measure/Report Actual Results)
  - Auditing and Monitoring Effort
  - Report to Appropriate Level (Operation Leaders vs. Senior Leadership vs. Board Leadership)

Credit Balances

Timely Refunding of Credit Balances

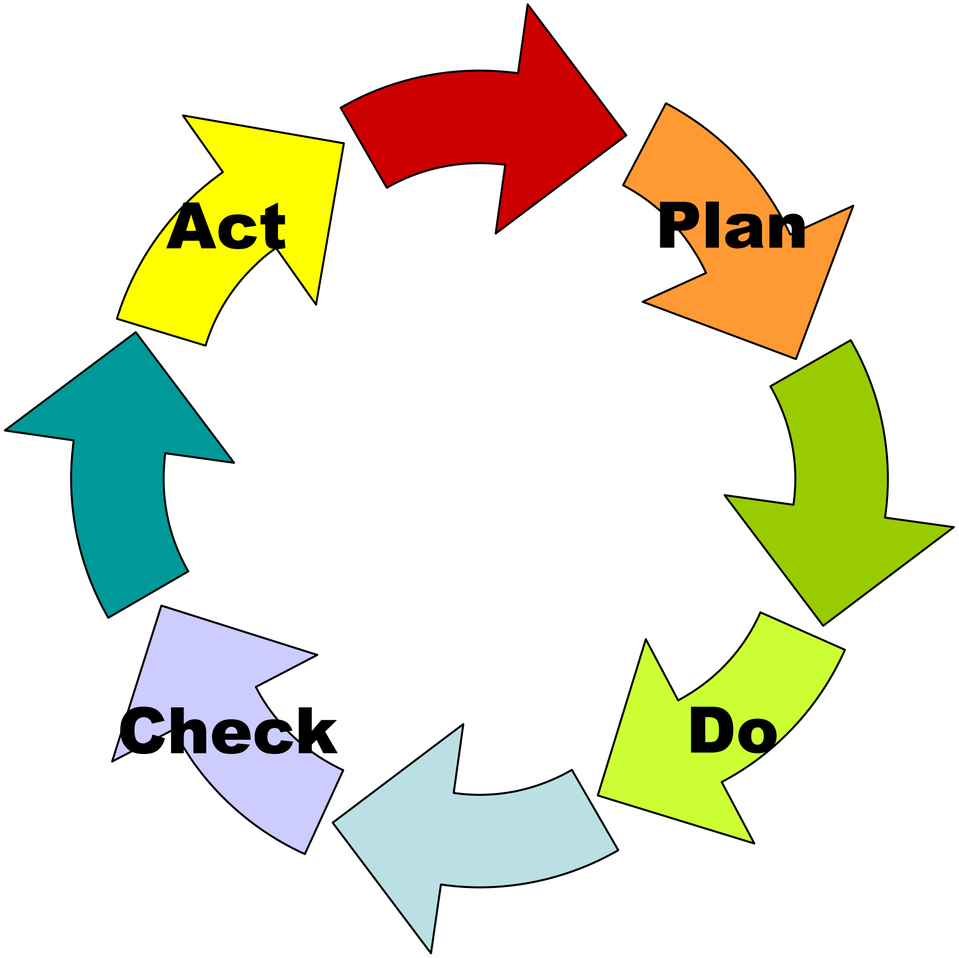
- Structure: (Program Infrastructure):
  - Policy Development
  - Education and Training
  - Oversight and Reporting Mechanisms
- Process: (How address risk):
  - Risk Assessment
  - Response and Prevention
    - Internal Investigation
    - Corrective Action Plan
    - Enforcement and Discipline
- Outcome: (Measure/Report Actual Results)
  - Auditing and Monitoring Effort
  - Report to Appropriate Level (Operation Leaders vs. Senior Leadership vs. Board Leadership)

Example: Internal Audit Work Plan

Project Name	Project Description	Risk Domain	Hours
Business Office Review	Integrated review of the processes and tools used for billing accounts receivable.	Financial	150
Health Information Management Review	Integrated review of the processes and tools related to outpatient and inpatient coding.	Operational	150
Inpatient & Outpatient Billing Compliance Review	Review of outpatient claims to determine compliance with payer requirements.	Regulatory	350
Grants and Research Review	Review of processes and related internal controls associated with grant funds and research projects.	Regulatory	150
Accounts Payable Review	Integrated review of the processes and tools used for accounts payable function.	Financial	100
Business Continuity Planning Review	Review of the outpatient business continuity plans for Tier I applications including data backup and storage.	Operational	200
Investment Review	Review of the investment management processes and related internal controls.	Financial	150
Cash Controls	Review of the internal controls associated with cash collections at point of service locations, business office and treasury department.	Financial	200

Phase III – Enterprise Risk Management Implementation

- Accountable managers monitor plans using quality improvement cycle of PSDA
- Accountable managers report quarterly to ERM facilitator
- ERM facilitator reports to the management risk committee on monitoring activities
- Management risk committee reports ERM activities to Board or Board Committee



Phase III – Enterprise Risk Management Implementation

- Implementation and Risk Management Process
  - Responsibility of the Accountable Manager
    - Periodically scan the assigned risk area, with participation from other stakeholders
    - Ensure adequate monitoring of the risk and that risk mitigation activities are in place
    - Report key elements of risk mitigation plan, changes in risk level and outcome monitoring to senior leadership
  - Role of Internal Audit Function
    - Internal audit does not manage risk, but is an independent validation mechanism for both the effectiveness of controls and the accuracy of management's assessment of controls
    - Measures validity of management's assertion of risk reduction due to mitigation activities
    - Consults on best-practice approach to further reduce risk

Phase III – Enterprise Risk Management Implementation

- Implementation and Risk Management Process
  - Reconciliation with other Processes
    - Risk assessment and mitigation plans developed should be considered as inputs to related activities
    - Where possible allow existing processes (e.g. billing compliance program) to serve as risk mitigation activity for certain mature risk areas
  - Period Review and Updating of Risk Matrix
    - Senior leadership should review annually to identify new risk areas, assess risk levels and determine if appropriate risk owners have been identified
    - Annual review of matrix, along with mitigation plan for high risk areas should be presented at the Board level for review and comment.
    - ERM management deficiencies should be reported upstream, with serious matters reported to senior leadership and the Board.

Phase III – Enterprise Risk Management Implementation

- Information Flows within the ERM Process
  - Risk Response
    - Management determines how it will respond
      - Risk avoidance, reduction, sharing or acceptance
      - Likelihood vs. Impact
      - Cost vs. Benefit
    - Opportunities Available
      - Entity wide approach
      - Is overall residual risk within the entity’s risk appetite
  - Control Activities
    - Policies and procedures that ensure risk responses carried out
    - Occur at all levels and in all functions

Phase III – Enterprise Risk Management Implementation

- Information Flows within the ERM Process
  - Information and Communication
    - Identified, captured, and communicated in a form that helps ensure management risks are carried out
    - Effective communication flows down, across and up the organization
    - Senior leadership communicates to all personnel that ERM is a priority and must be taken seriously
    - Internal stakeholders - employees must understand their role and how the ERM activities relate to the overall strategy of the entity.
    - External stakeholders – customers, vendors, regulators, etc.

Phase III – Enterprise Risk Management Implementation

- Information Flows within the ERM Process
  - Monitoring
    - ERM must be monitored – assessing the presence and functions of its components over time
    - Accomplished through ongoing monitoring activities, separate evaluations or a combination of the two
    - Ongoing monitoring occurs in the normal course of business
    - Scope and frequency depends on the level of risk
    - Results reported upstream

Rules Of The Road

- BOTTOM UP, BOTTOM UP, BOTTOM UP
- Keep it practical but exhaustive
- Don’t be idealistic. Look at what actually goes on.
- Identify the known-knowns, unknown knowns and unknown unknowns.
- Put it in business terms

Keys to Success

- Don’t name 100 potential risks & ask organization to assess and mitigate everything under the sun.
- ERM leader is a facilitator and advisor, the business must take ownership and accountability for mitigating risk.
- Create awareness & knowledge among business owners.
- Include a diverse group of leaders in process.

Conclusion

- Leading Providers…..
  - Understand the risks most pertinent to their organization
  - Manage the risks in an integrated fashion
  - Prioritize risk management efforts around:
    - Risks having the biggest potential impact and,
    - Are most likely to occur

Conclusion

Questions

Kelly Nueske,

Manager, LarsonAllen LLP

(612) 376-4739

knueske@larsonallen.com

Steven LeFar

MediRegs – Wolters Kluwer Law & Business

(847) 370-6941

slefar@mediregs.com

Jenny O’Brien

Shareholder, Halleland Lewis Nilan & Johnson

(612) 573-2968

jobrien@halleland.com