“Picking Up the Pieces- Re-designing Your Compliance Plan from Head to Toe”

Health Care Compliance Association’s Annual Compliance Institute
Chicago, Illinois
April 25, 2007

Presented by
Tom Feuerstein, NYU Medical Center
Sandy Piersol, Navigant Consulting, Inc
John Stearns, Navigant Consulting, Inc
Andrea Williams, Caritas Christi Health System
Agenda

- **Where do you start?**
  - Matching your needs assessment with the real life challenges of your organization
  - Establishing relationships within the organization
  - Some war stories about climbing this mountain

- **Assessing your Compliance Program**
  - What’s missing
  - What needs to be totally redesigned
  - What needs to be tweaked

- **Keeping the wave rolling And making sure it reaches all corners**
  - Your role as a change agent
  - Compliance program implementation and organizational control

- **Internal Controls, Internal Audit & Regulatory Compliance**
  - Risk Management and Internal Controls
  - Internal Audit / Compliance – Two Sides of Same Coin
  - Open Discussion
Challenges for Your Organization

- Over the past decade you have been working on developing a compliance program with all the right pieces:
  - Seven Elements
  - Hotline
  - Code of Conduct
  - Auditing and Monitoring

- You have also been putting out fires and if you are lucky you have done some monitoring based on your plan
  - Focused reviews
  - Investigations
  - Self-disclosures
  - CIAs
Challenges for Your Organization

- Whether your compliance program is new or well established, it is important to periodically evaluate if ethical and regulatory standards are adequately addressed.
- Risk assessment is not a one-time event, ongoing identification and monitoring of risk areas is mission critical.
- Don’t underestimate the importance of increasing awareness of risk areas.
- Best practices may not exist, the right solutions depends on several factors.
Establishing Relationships within Your Organization

- As a compliance officer you are both the enemy and a friend depending on the situation
- Get to know everyone
- Get the trust of the physicians and leadership
Untangling the Web of Regulatory Compliance Issues

- All of the OIGs compliance guidance documents are organized around risk areas – areas of vulnerability
- Identifying and understanding where the enterprise is vulnerable is the best starting point for figuring out what steps are needed to prevent problems
- This risk assessment process is precisely how generic compliance program principles can be fashioned into practical applications
Risk Assessment Approach

- Identify risk area
- Prioritize high risk areas
- Assess risk
- Analyze findings and solutions
- Operationalize corrective actions

*Repeat As Necessary*
Identify Risk Areas

- What risk areas have special relevance to your portfolio?
- Where is the enterprise vulnerable?
- Risks areas are not static
  - New laws and regulations (or interpretations)
  - New lines of business
  - New ways of doing things
  - New staff
Identify Risk Areas (cont’d)

Sources for Identifying Risk Areas

- OIG documents: compliance program guidance, special fraud alerts, advisory opinions, audit reports, inspection reports, annual work plans and semiannual reports

- Analysis of applicable laws, regulations and interpretations

- Relevant lawsuits, qui tam cases, settlement agreements

- Stated enforcement priorities

- Conferences, industry newsletters, word of mouth
Prioritize High Risk Areas

- Unless resources are unlimited, it is essential to start with the risk areas that are most likely to give rise to "liability" $$$

- Strategy: Emphasize attention upon higher risk areas and devote less effort to lower risk areas
Assess Risk

- Determine “current state” of compliance
  - Are we in compliance? Yes-No-Maybe
    - If Yes, why?…..Got Lucky or Was it by Design
    - If No, why not?….Redesign Control
Analyze Findings and Solutions

- Seek to understand the cause and extent of the problems identified
  - Evaluate the need for further investigation
  - Not every “rumor” requires investigation
- Identify plausible solutions and timeframe for corrective action
Operationalize Corrective Actions

- Prioritize corrective actions and assign accountability
- Operationalize corrective actions through
  - Policies and procedures
  - Training
  - Monitoring and Auditing
- Strategy: Compliance controls should be part of the basic infrastructure (controls should be “built-in” versus “added-on”)

13
Discussions of War Stories
Assessing Your Compliance Program
Why Assessing Compliance is Critical?

- 2004 Federal Sentencing Guidelines
- OIG Model Compliance Program Guidance
- Deficit Reduction Act/Qui Tam Actions/False Claim Prosecutions
- Avoidance of mandatory/imposed program
- Fraud and abuse detection is a top Federal and state priority
Accessing the Effectiveness of a Compliance Program

- The OIG recommends that organizations evaluate all elements of compliance program through “employee surveys, management assessments and periodic review of benchmarks established for audits, investigations, disciplinary action, overpayments, and employee feedbacks.”

OIG Model Compliance Program Guidance
Assessing Oversight Personnel

- **Board:**
  - Governing authority with oversight for implementation of effective program

- **President or CEO:**
  - High-level authority assigned overall responsibility for the compliance program

- **Compliance Officer:**
  - Member of senior management assigned day-to-day/operational responsibilities with direct access to the Board and CEO. Supported with adequate resources and a Compliance Committee

*Federal Sentencing Guidelines and OIG model Compliance Program Guidance*
Assessing the Compliance Officer/Committee

- Is there a compliance officer assigned day-to-day/operational responsibility?
- Do they have knowledge, training, and experience?
- Are they members of senior management?
- Are resources, funding, staffing and authority adequate?
- Do compliance officers compromise Program goals because of their other roles/responsibilities in the organization?
Standards and Policies

Compliance Program document describes how each element is implemented

- Code of Conduct
  - Annual Review
  - Board Acceptance
  - Reading Level
  - Parity with facility Policies and Procedures
- Annual Acknowledgement and Attestation
- Compliance Policies
  - Code of Conduct
  - Compliance Responsibilities
  - Reporting Requirements
  - Confidentiality, Non-retaliatory and Non-retribution for Reporting
  - Business Ethics
  - OIG/GSA/FDA Exclusion Review
Assessing Policies and Procedures

- Do employees:
  - Disobey standards and policies because they observe no buy-in from management
  - Misunderstand compliance policies and procedures
  - Experience reoccurring impermissible activities

- Does the organization routinely experience systemic billing errors?

- Is there a trend related to inadvertent Protected Health Disclosures?
Assessing Education and Training

- Are employees trained during orientation?
- Do employees receive annual training?
- Do relevant employees receive specialized training (e.g. coders)?
- How many employees fail post-training tests?
- Does the training program adequately summarize standards, policies and perform interim assessments?
- Are instructors qualified and experienced?
- Can employees name their compliance officer?
Education and Training

Compliance Awareness:

- Mandatory
- All employees should be able to respond to the following:
  - What is the name of your Compliance Officer?
  - Are you aware there is a Compliance Program?
  - What is the telephone number of the Compliance Hotline?
  - How would you report a compliance question or concern?
Assessing Communication

“Open communication is essential to maintaining an effective compliance program. The purpose of communication is to increase the hospital’s ability to identify and respond to compliance problems.”

OIG Supplemental Compliance Guidance for Hospitals, 2005
Assessing Communication

- Do compliance officers receive appropriate inquiries from employees?
- Do standards/policies and training provide instructions on “How to report concerns/issues/questions?”
- Is the reporting process free of retaliation or retribution?
- Is there a process of confidentiality, as is legally feasible?
- Do responses provide guidance?
- Do compliance officers maintain historical record/log of compliance issues/concerns?
Audits and Monitoring

- “The hallmark of effective monitoring and auditing compliance efforts is how an organization determines the parameters of its reviews.”
Assessing Auditing and Monitoring

- Do audits focus on high risk departments?
- Do audits address applicable regulations and third party payer requirements?
- Are outcomes from past audits, exceedences or prior deficiencies re-evaluated?
- Are the elements of the compliance program monitored?
- Are auditing techniques valid and conducted by independent and objective reviewers?
Auditing and Monitoring

- Auditing Goals and Objectives:
  - Process vs. Outcome
  - Measurement vs. Education
  - Structural and substantive assessment

- Auditing Methodology
  - Concurrent vs. Retrospective
  - Sampling
  - Independent and objective
Corrective Action

“By consistently responding to detected deficiencies hospitals can develop effective corrective action plans and prevent further losses to Federal health care programs.”

OIG Supplemental Compliance Guidance for Hospitals, 2005
Accessing Corrective Action

- When a provider learns of an issue does he/she disregard regulations and/or policies?
- Is there a response team to evaluate detected deficiencies quickly?
- Is there a correlation between deficiencies identified and the action necessary to remedy?
- Are overpayments resolved through the proper notification and repayment process?
- Are identified overpayments promptly reported and repaid?
Assessing Discipline

“By enforcing disciplinary standards hospitals help create an organizational culture that emphasizes ethical behavior.”

OIG Supplemental Compliance Guidance for Hospitals, 2005
Assessing Discipline

The OIG states that, in general, the number and type of disciplinary actions can be insightful.

- Have you publicized the Program and distributed the document?
- Have appropriate sanctions been taken to address misconduct?
- Are there incentives to comply?
- Are sanctions applied consistently, regardless of the employee’s level in the organization?
- Is Federal health care program excluded individual and vendor checking performed?
Keeping the Wave Rolling and Making Sure it Reaches ALL the Corners

- Compliance Program Implementation and Organization Structure
- Your Role as a Change Agent
What is Your Organization’s Effectiveness Checklist?
Compliance Scorecard

“We recommend that hospitals examine program outcomes, and assess the underlying structure and process of each compliance program element.”

OIG Supplemental Compliance Program Guidance for Hospitals, 2005
Four-Step Approach to Develop Effectiveness Measures

- Step 1: Identify Stakeholders
- Step 2: Identify the Purpose and Context for evaluating effectiveness
- Step 3: Identify the Standards against which effectiveness will be measured
- Step 4: Select effectiveness Measures
Step 1: Identify Stakeholders

- Patients and Staff: enforce reputation of ethics, integrity and reliability
- Law Enforcement (e.g., Justice Department and Federal Sentencing Guidelines)
- Regulators (e.g., Office of Inspector General)
- Provider Management and Third-party payers
Step 2: Identify Purpose/Context

- **Law Enforcement Purpose**
  - Evaluate intent to obey law

- **Regulators**
  - Evaluate Program participation status
  - Define conditions of program participation

- **Provider Management and Third-party payers**
  - Evaluate usage of compliance program as a “risk management” tool
Step 3: Identify Standards

- Law Enforcement Purpose
  - Standard: “Effort” and “Due Diligence”

- Regulators
  - “Integrity” or “Capacity” for future compliance

- Provider Management and Third-party payers
  - Cost-effectiveness
Step 4: Select Measures

- **Structure** Measures
  - Employee Education
  - Policies, Standards and Procedures
  - Compliance Committee Attendance
  - Independent Compliance Officer
  - Awareness, Compliance Handbook, Website, and Posters
  - Existence of Hotline-Mailbox
Step 4: Select Measures (cont’d.)

- **Process Measures:**
  - Assessment/Prioritization of Risk – Work Plans
  - Evaluation/Remediation of Findings
  - Timely Filings – Corrective Action Plans
  - Interim Assessments – Monitoring
  - HIPAA Privacy walk-throughs
Step 4: Select Measures (cont’d.)

- **Outcome Measures:**
  - Internal/External Audit results
  - Overpayments
  - Pepper report outcomes
Key Points

- *Structure, Process* and *Outcome* measures and linkages are equally important and critical.
- When evaluating effectiveness, different measures are appropriate (e.g., with new compliance program, regulations or unclear regulations).
- Important to identify stakeholders, purpose and standard before adopting effectiveness measures.
Compliance Scorecard Advantages

- Practical Management Tool
- Useful in health care systems to standardize evaluations
- Must be supported by upper management
- Useful as a performance evaluation tool
- Elements should change with progress of Program
# Quarterly Compliance Scorecard

<table>
<thead>
<tr>
<th>Date</th>
<th>Compliance Structure:</th>
<th>Compliance Process:</th>
<th>Compliance Outcome:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Employee Education</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Standards and Procedures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Reporting Mechanism</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Program Oversight</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Communication Framework</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Assessment/Prioritization of Risk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Evaluation/Remediation of Findings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Corrective Action, Timely Filings</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Ongoing Monitoring</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>HIPAA Privacy</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Internal/External Audit Error Rate</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Date</th>
<th>Outcome</th>
<th>Hospitals (6)</th>
<th>Physician Practices (68)</th>
<th>Hospice</th>
<th>Home Care</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Evaluation Key</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Green</td>
</tr>
<tr>
<td>Yellow</td>
</tr>
<tr>
<td>Red</td>
</tr>
</tbody>
</table>
Compliance and Risk Assessment

- Compliance and risk management functions, at a minimum, should be coordinated
- Focus of compliance should be risk management
- To be effective, compliance and risk assessment must be an ongoing process as part of the organization’s ethics and mission
Compliance Program Determinants

- Industry standards set by applicable Federal and state regulations
- Size of Organizations
- Similar Misconduct
Why Evaluate Effectiveness?

- Culpability Score determines the Fine
- Gear Program approach toward deterrence
  - Restitution
  - Fines
  - Probation
- Rehabilitate Organizations by Instituting Mandatory Compliance Program
- Guidelines provide that offending organization may be given credit for the effective compliance program
Compliance and the Role of the Internal Auditor
Role of Internal Audit and Compliance Department

- Define who does what
- Avoid Duplications and Ambiguous Accountability
- Identify Levels of Controls for Review
Internal Auditor Role

- Independent and objective review
- Collaborate Risk-based Compliance assessment design
- Identify Internal Controls and High-risk exposure
Compliance Officer Role

- Independent and objective review
- Collaborate Risk-based Compliance assessment design
- Ensure Education and Training
- Assess auditing and monitoring outcomes
Risk Management & Internal Control
RISK
Possibility of an adverse event which may negatively affect the ability of an organization to achieve its objectives.

RISK MANAGEMENT
Process to increase confidence in the ability of an organization to anticipate, prioritize and overcome obstacles to the attainment of its goals.

INTERNAL CONTROL
A process designed to provide reasonable assurance regarding the achievement of business objectives.
What is Internal Control?

- **Internal Control** is a process — established by an entity's board of directors, management, and other personnel — designed to provide reasonable assurance regarding the achievement of stated objectives.*

- Internal Control has 3 main objectives:*
  - To promote effectiveness and efficiency of operations
  - To ensure reliability of financial reporting
  - To maintain compliance with applicable laws and regulations

- In short, internal control helps an entity get to where it wants to be and some confidence that it may avoid the pitfalls and surprises that could occur along the way.

* Internal Control – Integrated Framework, Committee of Sponsoring Organizations (COSO) of the Treadway Commission
Why is Internal Control Important?

**Operations**
- Promotes efficiency and effectiveness of operations through standardized processes
- Ensures the safeguarding of assets through control activities

**Financial**
- Promotes integrity of data used in making business decisions
- Assists in fraud prevention and detection and creates an auditable trail of evidence

**Compliance**
- Helps maintain compliance with laws and regulations through periodic monitoring
COSO offers an integrated framework which defines internal control by five interrelated components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring
Control Environment

- The Control Environment is the control consciousness of an organization; it is the environment in which people conduct business activities and fulfill their control obligations.
- The control environment includes both intangible and tangible elements:
  - Integrity and ethical values
  - Commitment to competence
  - Governance and organization structure
  - Management philosophy and operating style
  - Assignment of authority and responsibility
  - Human resource policies and practices
- An effective control environment exists when employees understand their responsibilities, authority, and are committed to acting ethically.
- Management influences an organization’s control environment through setting the standard through actions and effectively communicating written polices and procedures, a code of ethics, and standards of conduct – “tone at the top.”
Risk Assessment

- **Risk Assessment** starts with identifying risks associated with business objectives linked through all levels of the organization.
- **Entity-wide**
  - The cornerstone for effective control, entity-wide objectives provide guidance on what the entity wishes to achieve.
  - Should be consistent with budget, strategic and business plans.
- **Activity-level**
  - Align with entity-wide objectives but differ in that they relate directly to goal setting with specific targets and deadlines.
  - Provides guidance for management focus.
- Risk assessment requires evaluation of external and internal factors and the impact on operations, financial reporting, and compliance.
- May employ techniques for risk identification, assessment and management.
  - Control Self Assessment (CSA), Enterprise Risk Management (ERM), Risk and Control Assurance (RCA), questionnaires, and many others.
Control Activities

- **Control Activities** are policies and procedures that help to ensure that actions identified to manage risks are executed and timely.

- The control activities should be embedded within the operations of the business and used to manage risks to reasonable levels. Focuses on *Prevention, Detection, Correction*.

- Types of control activities:
  - Approvals, authorizations and verifications (e.g. delegation of authority)
  - Direct functional or activity management (e.g. reconciliations)
  - Review of performance indicators (e.g. KPIs, metrics)
  - Security of assets (e.g. physical controls)
  - Segregation of duties (e.g. custody - authority - recording)
  - Information systems controls (e.g. security access)

- Disciplinary action should be established, communicated and consistently administered for non-compliance.
Information and Communication

- Information and Communication requires that relevant external and internal information be identified, captured, processed and communicated throughout the organization in a timely manner.

- Provided through various formal and informal means.
  - Verbal communication (e.g. meetings, feedback)
  - Written communication (e.g. policies, procedures, job descriptions)
  - Demonstrated through actions (e.g. management sets example)

- The integrity of information quality is imperative for making business decisions.
  - Requires internal control mechanisms to provide reasonable assurance that information is appropriate, current, timely, accurate and accessible.

- Managements responsibilities:
  - Employee duties and responsibilities should be communicated
  - Communication across the organization should be fluid – up, down, and laterally across the organization
  - Channels of communication with customers, suppliers and other external parties should be open
Monitoring

- The purpose of **Monitoring** is to determine whether internal control is adequately designed, executed, effective and adaptive.

- Internal control performance should be assessed over time through ongoing monitoring of operations and separate periodic evaluations.

- Scope and frequency of monitoring activities depend on significance of risks being controlled and importance of controls in reducing risks.

- Monitoring activities should be built into normal, recurring operating activities of an organization.

- Deficiencies found should have defined escalation path for reporting and follow-up and accountability for corrective action.
Internal Audit

Risk – Control = Exposure

An independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

The Institute of Internal Auditors
What is Compliance?

Know everything and do it right every time?
Or
Risk – Controls = Exposure
Internal Audit & Compliance

Risk – Control = Exposure

COSO and the OIG seven rules go hand in hand. COSO's focus is on effective and efficient operations, reliable financial statements, and compliance with laws and regulations. HHS OIG guidelines stress a recurring theme of internal controls and internal audit

Elements of a Compliance Program

- Written Standards of Conduct, P&P promoting compliance commitment
- Designation of independent Chief Compliance Officer
- Regular, effective education programs for all affected employees
- A method to anonymously receive complaints (hotline)
- System to respond to allegations of improper activity & disciplinary action
- The use of audits or other evaluation techniques to monitor compliance
- Investigation and remediation of identified systemic problems
OIG Compliance Auditing & Monitoring

DHHS - Office of Inspector General
Supplemental Compliance Program Guidance
Federal Register / Vol. 70, No. 19 / January 31, 2005

- Internal Monitoring and Auditing

- Effective auditing and monitoring plans will help hospitals avoid the submission of incorrect claims to Federal health care program payors.

- Hospitals should develop detailed annual audit plans designed to minimize the risks associated with improper claims and billing practices
Some factors hospitals may wish to consider: (selected)

- Is the audit plan re-evaluated annually, and does it address the proper areas of concern?

- Does the audit plan include an assessment of billing systems, in addition to claims accuracy, in an effort to identify the root cause of billing errors?

- Is the role of the auditors clearly established and are coding and audit personnel independent and qualified, with the requisite certifications?

- Is the audit department available to conduct unscheduled reviews and does a mechanism exist that allows the compliance department to request additional audits or monitoring should the need arise?
The Evolution Continues

  - Emphasized the control environment, codes of conduct, and competent and involved audit committees.
  - Called for sponsoring organizations to integrate the various concepts and develop a common reference point. The result was the Committee Of Sponsoring Organizations or COSO.
    - COSO incorporated learnings from other existing authoritative sources (e.g., CoCo, Cadbury, Turnbull, etc.)
  - COSO developed and published practical, broadly accepted criteria for establishing internal control and evaluations of effectiveness.
      - Outlined the roles and responsibilities of management
      - Established a means to monitor, evaluate and report on internal control
Ongoing Focus on Internal Control

- Federal Sentencing Guidelines
  - Used by the criminal justice system, effectively reduces white-collar
crime penalties for entities with appropriate compliance related
internal controls.
- Blue Ribbon Commission
  - Focused on strengthening the independence of audit committees,
defining its accountability and on improving its effectiveness.
  - Issued report in 1999 outlining 10 recommendations and
requirements for audit committees.
  - The rules are enforced by the SEC, NASD, NYSE, AICPA.
- Sarbanes-Oxley Act of 2002
  - Far-reaching Federal legislation affecting public accounting firms,
public company governance and reporting
  - Considerable focus on management’s responsibility for internal
controls
- **CONCLUSION:** Organizations are continually being held to increased
standards for internal control and risk management.
Internal Audit / Compliance – Two Sides of Same Coin
Risk & Exposure

Risk

(Less)

Control

 Equals

Exposure

Assess Likelihood and Magnitude of Impact

Design & Operation of Controls

Residual Potential Impact

Same concepts in place – compliance or internal audit
Roles and Responsibilities

- **Executive Management**
  - Sets the standard for the control environment
  - Maintains ultimate accountability for internal control and risk management enterprise-wide
  - Supports control and risk management activities throughout the organization

- **Operating Management**
  - Directly responsible and accountable for business operations effectiveness and internal control related to business objectives
  - Periodically assesses and asserts on risk management and control environment
  - Develops and implements action plans for improvement

- **Compliance Staff**
  - Compliance oversight – compliance is management’s responsibility
  - Provides compliance training and regulatory updates
  - Investigates compliance concerns, reports to Exec. Mgt. & Board
Roles and Responsibilities (cont’d.)

- **Internal Audit**
  - Provides support for risk and control assessment activities
  - Monitors exposure of the organization and makes recommendations relating to risk and control activities
  - Designs internal audit plan based on strategic risk assessment
  - Tests adequacy and effectiveness of controls
  - Challenges and validates management control environment assertions
  - Reports independent findings and provides recommendations

- **Audit Committee (or Audit & Compliance Committee)**
  - Focuses Board attention
  - Evaluates overall risk exposure
  - Reviews adequacy of overall control environment
  - Provides oversight and advice
Roles and Responsibilities (cont’d.)

- **External Audit**
  - Evaluates the effectiveness of internal control to determine the scope of external audit procedures
  - Issues management commentary reports
  - Issues an opinion on the consolidated financial statements
  - Reviews control environment and uses results of risk assessments as input to develop external audit plan
Internal Audit / Compliance Connection

- Both functions
  - Regularly assess risk and develop plans in response
  - Identify significant exposures for management action
  - Add value through business process improvement and mitigation of potential exposure
  - Provide objective-party view of business issues
  - Internal consultative services
  - Report significant findings to executive management and board

- One big difference – audit approach – internal audit typically retrospective vs. compliance usually do concurrent reviews
Internal Audit Supports Compliance Program

- Internal auditors

- Are trained to assess risk, design audits, report findings and make recommendations for improvement

- Already have access to a wide range of systems and internal data

- Know how things work – can identify unintended consequences to changes in policy or procedure

- Use automated techniques to sample or view entire universe of transactions – can focus on the anomalies

- Already doing testing in an area related to financial controls – might only need to add some additional steps to test compliance activity

- May identify compliance concerns in course of typical internal audit – need to know when to put pencils down
Questions, Objections and Other Discussion