

Internal Audit Cycle Within The Patient Care Setting



Presented by Weaver & Tidwell, LLP

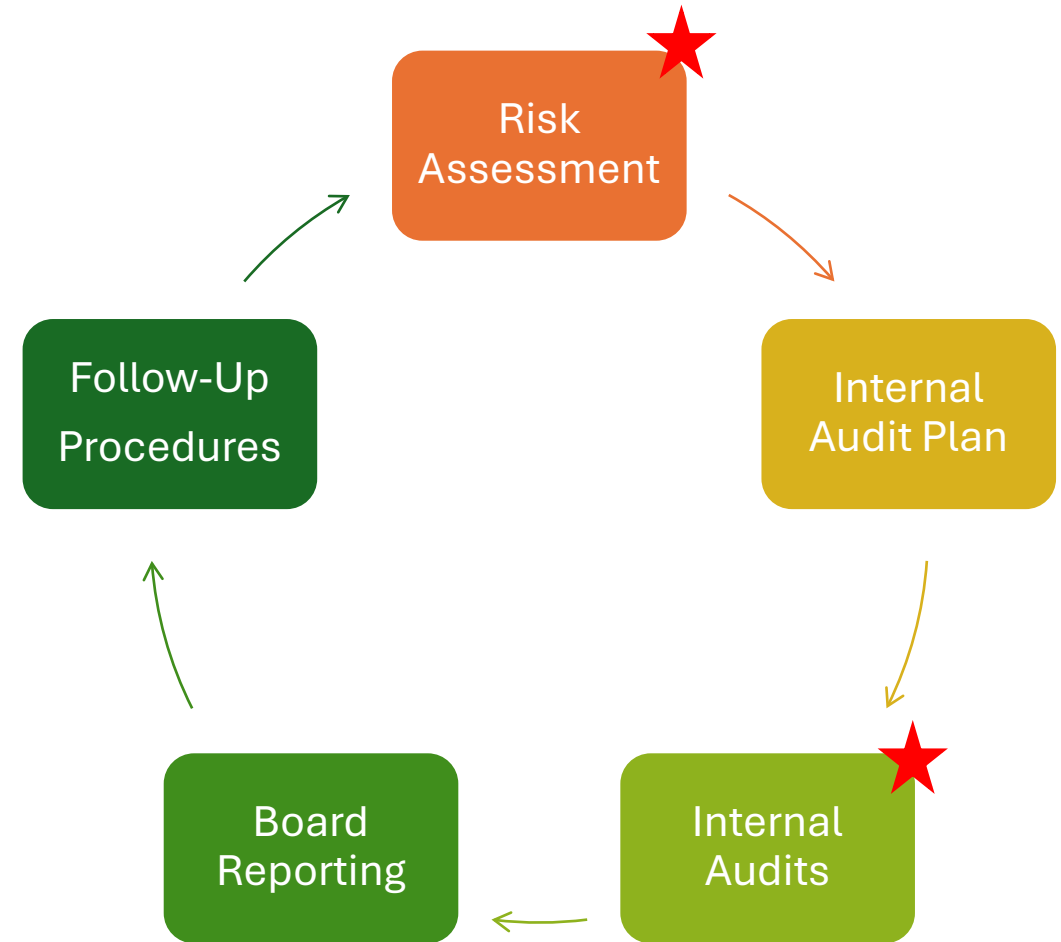
May 2025

Learning Objectives

- ✓ Review the Internal Audit Cycle within the Patient Care Setting
- ✓ Understand Internal Audit's Role within the Risk Assessment Process
- ✓ Process Level Risk Assessment (PLRA) Overview
- ✓ Review Inherent vs. Residual Risk
- ✓ Internal Audit Cycle [Planning, Fieldwork, Reporting]
- ✓ Advisory & Consulting Projects

Internal Audit Cycle Within Patient Care

- ✓ Risk Assessment sets the foundation
- ✓ Internal Audit Plan is approved by the governing body
- ✓ Internal Audits test effectiveness of residual risk
- ✓ Open lines of communication and routine reporting
- ✓ Follow-up procedures based on management's response to assess remediation



★ Topic Focus Areas

Poll #1:

Have you ever participated in a risk assessment? (Y/N)

Process Level Risk Assessment (PLRA) Purpose

The process-level risk assessment (PLRA) is used to identify and quantify the inherent risks that affect the System's significant activities and processes.



The **purpose** of the PLRA process is to receive input on risks within your operation's most significant activities.



The **objective** of the PLRA is to both identify and understand the natural risks existing within processes across the entity, as well as collectively determine the level of risk exhibited by the System's significant activities



The PLRA also gives us insight into the **inherent risks** across the organization, which will help direct planned internal audit activities.

Key Concept: Internal Audit evaluates risk at an inherent level during the risk assessment process, but tests internal controls in their residual state; i.e., after internal controls are in place.

Residual vs. Inherent Risk

Inherent Risk: The natural risk (exposure) in the significant activities of the organization ***without consideration of internal controls*** or other actions that mitigate risk.



The RA is aimed at understanding risks in their inherent state.

Vs.



IA would perform procedures to test the safety effectiveness of the harness, ropes, tether points, etc. in this example

Poll #2:

Residual Risk is the risk that remains after internal controls are present (T/F)?

Revenue Cycle Risks – Registration & Encounter

Pre-Registration

- Visit scheduling IT System
- Patient demographics
- Insurance coverage verification
- Pre-authorization from Payors
- Setting payment expectations
- Sharing HIPAA & Privacy policies

Registration

- Verify insurance completeness
- Collect copay and balances
- Proof of identity
- Schedule follow-up

Clinical / Patient Care

- Medical Documentation – EHR, imaging, laboratory, pathology, IT System
- Patient Care – Vital signs, diagnosis, notes, checkup
- Quality Measures tracked in EHR system

Inherent Risks

- Incomplete demographics info
- Incomplete/Inaccurate insurance
- Unauthorized user access
- Failure to verify pre-authorization

Inherent Risks

- Failure to verify insurance
- Failure to collect co-pay
- No proof of identity
- Failure to provide necessary patient forms/information

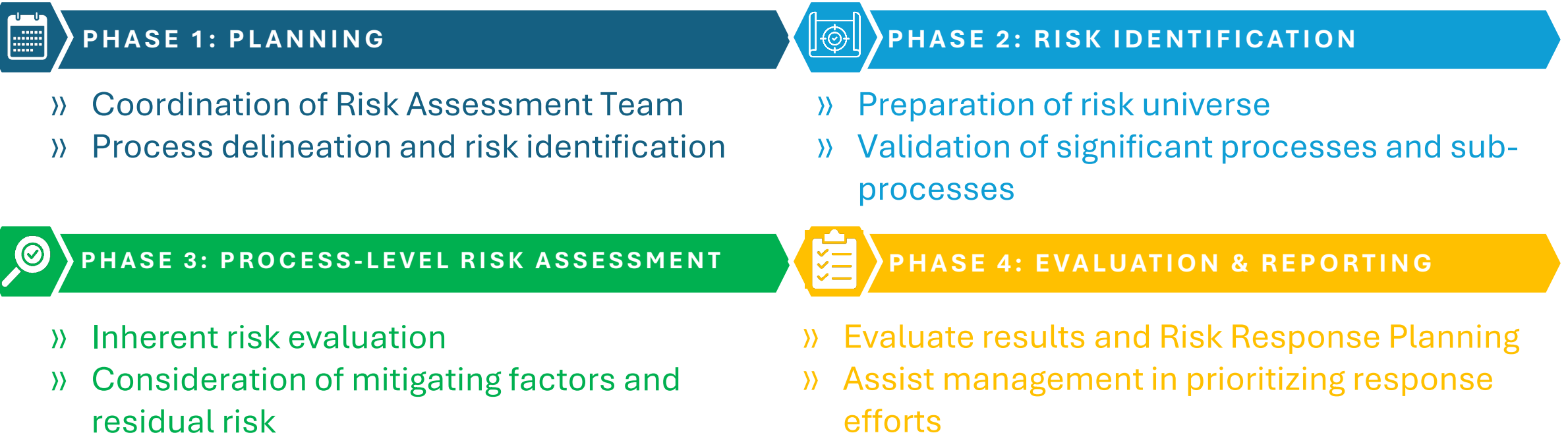
Inherent Risks

- Incomplete, not signed medical record documents
- Imaging /lab results outdated
- Quality measures not collected
- Missing charges

These are inherently high-risk areas if internal controls are not in place.

Overview of Potential Risk Assessment Phases

An approach to the Process Level Risk Assessment (PLRA) is to divide the project into multiple phases, including the following:



IA's Role within the Risk Assessment Process



COORDINATION OF RISK ASSESSMENT TEAM

- » Identify Risk Assessment team participants to collaborate and help champion the risk assessment process internally
- » Preparation of kickoff materials, including guidance and instructions



PROCESS DELINEATION & RISK IDENTIFICATION

- » Understand your organization's structure and operations
- » Delineate organizational channels and significant processes
- » Information gathering sessions with key stakeholders
- » Preparation of preliminary risk inventory



PREPARATION OF RISK UNIVERSE

- » Validate risk universe with risk assessment team for completeness and appropriate aggregation
- » Conduct initial meeting with System management and come to consensus on all process risk areas in the Risk Universe



VALIDATION OF SIGNIFICANT RISK PROCESSES & SUB-PROCESSES

- » Perform additional meetings with process owners to gain an understanding of all process elements
- » Verify organization's risk processes and sub-processes are complete and accurate with process owners

IA's Role within the Risk Assessment Process



INHERENT RISK EVALUATION

- » Facilitate risk assessment forum meetings with relevant stakeholders and risk rate the identified processes
- » Determination and ranking of inherent risk ratings
- » Following forum meetings, Weaver will aggregate the results and analyze the scores for reasonableness



CONSIDERATION OF MITIGATING FACTORS

- » Identification of mitigating factors, such as monitoring and risk transfer activities, as well as accepted risks
- » Determination of risk reduction and residual risk rating



EVALUATE RESULTS & RISK RESPONSE PLANNING

- » Final results will be organized into a heat map
- » A follow-up meeting with management will be performed to confirm amended risk ratings
- » A risk response plan will be prepared for the high-risk activities



INTERNAL AUDIT PLAN DEVELOPMENT

- » Determine risks for priority attention
- » Determine mitigating factors for priority validation
- » Assist management in planning coordination of internal audit and other mitigation mechanisms and efforts, with consideration of PLRA results

Poll #3:

What is generally internal audit's role in the risk assessment process?

- A) Developing remediation strategies for process owners
- B) Designing internal controls
- C) Facilitating the risk assessment process
- D) None of the above

Risk Category Considerations, included but not limited to:

Financial Risks



- The risk the entity will fail to adequately forecast and plan to achieve necessary cash flow, manage liquidity, receive adequate funding and accurately report financial results.

Patient Safety



- The risk that internal operations and daily processes do not adequately identify and provide for the safety of patients.

Reputational Risks



- The risk of an event generating poor public opinion and/or reduced employee commitment. Considers stakeholder relations, external relations, internal and external communications.

Fraud Risks



- The risk of the occurrence of illegal acts characterized by deceit, concealment, or violation of trust. Risks associated with dollar volume, non-conformance with ethical standards.

IT Risks



- The risk the entity's IT strategy is not aligned with the business model to embrace and rely on technology. Also includes the risk the entity is highly dependent on technology to execute strategic operations, and that IT infrastructure is not reliable

Regulatory & Compliance



- The risk that regulatory compliance will have an adverse impact on the System and inhibit its ability to achieve strategic objectives, or that regulatory changes impair operations and the ability to conduct business.

Patient Care Risk Examples



Financial Risks:

- Incomplete medical documentation results in denials
- Charge capture, charge entry, billing/coding inaccurate or ineffective
- Collection of copays & deductibles

Regulatory Risks:

- Department of Justice (anti-kickback, stark law)
- Food and Drug Administration
- The Joint Commission
- Loss of accreditation – CMS
- Civil and Criminal Lawsuits
- Penalties and Fines

Revenue Cycle IT Risks:

- HIPAA confidentiality
- Inaccurate/incomplete data
- User Access / Segregation of duties
- Claims editor is not updated
- Charge Description Master (CDM) is not updated or is inaccurate

Risk Assessment Results – Audit Universe

No.	Function	Significant Processes / Sub-Processes	F&F		Rep.		O&C		HC		IT		Combined		Overall	Quadrant
			P	I	P	I	P	I	P	I	P	I	Probability	Impact		
1	Technical	IT Security	4	4	4	4	4	4	4	4	4	4	4.00	4.00	4.00	4
2	Combined	In-patient Admissions & Encounters	4	4	3	4	4	4	4	4	2	4	3.40	4.00	3.70	4
3	Combined	Out-patient Admissions & Encounters	4	4	3	4	4	4	4	4	2	4	3.40	4.00	3.70	4
4	Administrative	Bad Debt	4	4	3	4	2	4	3	4	3	4	3.00	4.00	3.50	4
5	Combined	Charting and Charge Capture	4	4	2	3	4	4	4	4	2	4	3.20	3.80	3.50	4
6	Administrative	Patient Billing & Collections	4	4	2	3	3	4	3	4	3	4	3.00	3.80	3.40	4
7	Administrative	Revenue & Accounts Receivable	2	4	2	3	3	3	4	4	4	4	3.00	3.60	3.30	4
8	Combined	In-patient Management	3	4	2	4	3	3	4	4	2	4	2.80	3.80	3.30	4
9	Combined	Facilities Management	4	4	4	4	3	4	3	4	1	1	3.00	3.40	3.20	4
10	Combined	Scheduling/Rostering	3	4	2	3	3	4	4	4	2	3	2.80	3.60	3.20	4
11	Combined	Cash Handling	4	3	2	2	3	4	4	4	2	3	3.00	3.20	3.10	4
12	Administrative	Employee Retention	3	4	2	4	3	4	4	4	1	2	2.60	3.60	3.10	4
13	Combined	Out-patient Management	3	2	2	4	3	3	4	4	2	4	2.80	3.40	3.10	4
14	Technical	System Implementation	1	4	1	4	3	4	3	4	3	4	2.20	4.00	3.10	4
15	Administrative	Employee Recruitment	2	4	2	4	2	3	4	4	2	4	2.40	3.80	3.10	4
16	Administrative	Benefits Administration	3	4	2	4	2	2	2	4	4	4	2.60	3.60	3.10	4
17	Administrative	Health Information Management (HIM)	3	4	1	2	3	4	3	4	2	4	2.40	3.60	3.00	4
18	Combined	Medication Administration	3	4	2	3	3	4	2	3	2	4	2.40	3.60	3.00	4
19	Administrative	Accounts Payable	3	4	2	3	2	3	2	3	3	4	2.40	3.40	2.90	4
20	Combined	Patient Safety	2	4	2	4	3	4	2	4	1	3	2.00	3.80	2.90	4
21	Technical	Disaster Preparedness	2	3	2	2	4	3	2	2	4	3	2.80	2.60	2.70	4
22	Technical	IT Services	2	1	2	2	3	4	3	3	4	3	2.80	2.60	2.70	4
23	Administrative	Payroll	2	3	3	3	2	3	2	3	2	4	2.20	3.20	2.70	4
24	Clinical	Housekeeping Services	2	3	2	4	2	4	3	3	1	2	2.00	3.20	2.60	4
25	Administrative	Physician Contracting & Payments	2	3	2	3	2	4	1	3	2	4	1.80	3.40	2.60	2
26	Combined	Police & Security	1	3	2	4	1	4	1	3	3	4	1.60	3.60	2.60	2
27	Administrative	HR Administration	3	4	2	3	2	3	3	3	1	2	2.20	3.00	2.60	4
28	Administrative	Risk Management	2	4	1	4	2	3	2	3	2	3	1.80	3.40	2.60	2
29	Administrative	Credentialing and Privileging	1	4	1	4	1	4	2	4	1	3	1.20	3.80	2.50	2

Internal Audit Plan & Global Internal Audit Standards



- Chief Audit Executive (CAE) must create an internal audit plan that supports the achievement of the organization's objectives, and it must be based on a documented assessment of the organization's strategies, objectives, and risks.



- The assessment must be informed by input from the board and senior management as well as the CAE's understanding of governance, risk, and controls.

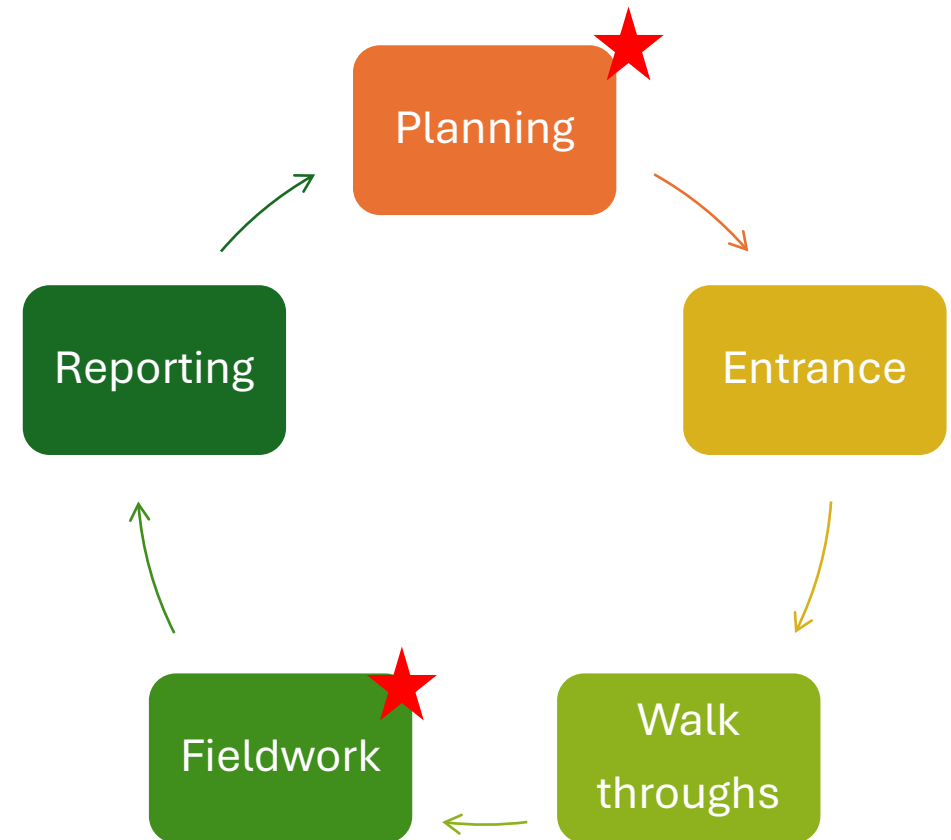


- Evidence of conformance with the standards may include the following: Approved Internal Audit Plan, Documented Risk Assessment, Meeting Minutes, Documented Methodologies, etc.

Standards: *Global Internal Audit Standards (GIAS) Standard 9.4 Internal Audit Plan*

Internal Audit Process

- Internal audit engagements begin with **planning**, which involves collaboration and meetings with management and key stakeholders to determine in scope areas of focus.
- **Entrance conferences**, or kickoff meetings are often held with all relevant process owners and stakeholders. This step usually includes an initial document request list for policies, procedures, or populations.
- To gain a thorough understanding of the design of internal controls, **walkthroughs** are typically held.
- Testing procedures are performed during **fieldwork** to test the effectiveness of in-scope internal controls within the process areas.
- **Reporting** can look different based on the organization but should include the requirements found within the Standards.



★ **Topic Focus Areas**

Internal Audit Planning – Scope and Objectives

- ✓ Objectives are documented and articulate the purpose of the engagement.
- ✓ Identifying boundaries; systems, locations, processes, components, period of time.
- ✓ Determines where the engagement is intended on providing advisory or assurance services.
- ✓ Changes to the scope must be approved by the CAE.
- ✓ Outline the planned procedures and anticipated deliverables or outcomes.
- ✓ Include an anticipated timeline to complete.
- ✓ Outline in-scope criteria such as laws, regulations, policies and procedures.

Standards: *Global Internal Audit Standards (GIAS) Standard 13.3 Engagement Scope and Objectives*

Revenue Cycle Risks – Internal Controls

Pre-Registration

Inherent Risks

- Incomplete demographics info
- Incomplete/Inaccurate insurance
- Unauthorized user access
- Failure to verify pre-authorization

Registration

Inherent Risks

- Failure to verify insurance
- Failure to collect co-pay
- No proof of identity
- Failure to provide necessary patient forms/information

Clinical / Patient Care

Inherent Risks

- Incomplete, not signed medical record documents
- Imaging /lab results outdated
- Quality measures not collected
- Missing charges

Inherent Risks + Internal Controls = Residual Risk

Internal Control Examples – Front End Revenue Cycle

- Daily, the access services director or lead reviews pre-authorizations, insurance verification, and patient demographics for completeness and accuracy.
- Automated notifications within the EHR system require patient notification letters depending on the level of service, and insurance; General Consent to Treat, IMM, MOON, ABN, etc.
- Segregation of duties internal controls are built into the EHR system that prevent unauthorized access, use, and disclosure to sensitive patient information.

Revenue Cycle Risks – Internal Audit Procedures

Based on the scope of the **internal audit** procedures may be designed for **advisory** or **audit** services. These procedures are designed to evaluate the effectiveness and efficiency within the **residual risk** environment.

Advisory Procedures

- Conduct walkthroughs and interviews to gain an understanding of the design of the process and controls.
- Document risk and control matrixes, process flowcharts, narratives.
- Obtain and review HIPAA Privacy Rule policies and procedures for safeguards.
- Review and make recommendations to enhance the control structure of policies and procedures.
- Identify points for consideration or observations to improve the internal control environment and mitigate inherent risks.

Audit Procedures

- Select a sample of patient encounters for testing and verify that applicable patient notification letters were obtained and signed.
- Test user access within the EHR system to determine if segregation of duties is present.
- Obtain and review recent denial reports and evaluate corrective action and mitigation strategies taken by management.
- Test for unauthorized access, use, or disclosure under HIPAA.
- Select a sample of encounters and review medical record documentation for completeness and accuracy.

Internal Audit Governance Frameworks

Professional practice frameworks that guide the internal audit profession include, but are not limited to the following:

- **COSO ERM Framework** – Provides a comprehensive and integrated approach to identifying, assessing, responding to, and monitoring risks that could impact an organization’s ability to achieve its objectives.
- **Global Internal Audit Standards (GIAS)** – A set of guidelines and principles established by the Institute of Internal Auditors (IIA) to promote effective internal audit practices worldwide.
- **COBIT Framework** – Control Objectives for Information and Related Technologies was developed by Information Systems and Control Association (ISACA) for governance and management of enterprise IT.
- **National Institute of Standards and Technology (NIST)** – Develops and promotes standards, measurements, and technology to enhance innovation, competitiveness, and security across various industries.
- **HITRUST** – Health Information Trust Alliance, is a cybersecurity framework and certification program designed to address the unique security and privacy challenges faced by organizations within the healthcare industry.

Key Takeaways

- ✓ Internal audit can partner with management to facilitate risk assessments
- ✓ Periodic risk assessments assist management with evaluating entity-wide risk
- ✓ Inherent Risk + Internal Controls = Residual Risk
- ✓ The development and execution of an internal audit plan monitors residual risk
- ✓ Internal audit provides both audit and advisory services based on the needs

Thank You!

Jeff Jones, CIA | Senior Manager, Governance Risk & Compliance (GRC)
Direct: 512.609.1981 | Email: jeff.jones@weaver.com