Compliance & Internal Audit Offices
A Collaborative Approach

Debra A. Muscio
Audit, Enterprise Risk Management, Privacy, Information Security, Ethic and Compliance Professional

Agenda

Compliance and Internal Audit (IA) Offices – Collaboration Approach

- WHY
- WHAT
- HOW
- RESULTS

- Comments and questions

Agenda

Background

Traditionally Compliance

The primary function of the compliance role is to **promote ethical conduct** and compliance with rules, regulations, and standard processes that govern how organizations should conduct business.

Today and Future - The Chief Compliance Officer should be involved in strategic discussions about where the business is going and what it needs to achieve its objectives in a compliant way.

Agenda

Background

Traditionally Internal Audit takes business objectives and looks back to see if they were achieved in the way they were meant to be.

The primary **purpose** of an **audit** is to evaluate the level of compliance with internal and external policies, identify the effectiveness of internal controls, and get feedback for continuous improvement.

It's a method to keep the quality system alive; they are an essential tool in a well-functioning management system and provide a report to external and internal audiences.

Every organization needs aspects of both audit and compliance.

Compliance and IA Offices – Collaboration
WHY

Remember your C's

- **Culture**- Engage in a top-down approach. Formal and informal organizational norms
- **Commitment** – dedicated to a cause, activity, etc.
- **Compliance** – Rules and Regulations
- **Clarification** – Roles and expectations
- **Connection** – interpersonal relationships and information networks
- **Collaboration** – working together to reach a goal. Putting talent, expertise, and smarts to work

Compliance and IA Offices – Collaboration WHY

Remember your C's

- **Collaboration** – working together to reach a goal. Putting talent, expertise, and smarts to work
- **Communication** – Sharing thoughts, questions, ideas & solutions
- **Critical thinking** – Looking at problems in a new way and linking learning across subjects & disciplines
- **Creativity**- Trying new approaches to get things done equals innovation & invention

Compliance and IA Offices – Collaboration
WHY

Remember your C's

- **Comprehensive** – develop a robust training program
- **Change** – an alteration of the environment, structure, technology, or people; a reality, force, opportunity, or threat.
- **Cost effective** - training programs have been streamlined and are becoming more affordable

Compliance and IA Offices – Collaboration
WHY

Remember your "WHY" P's

- **Professional** a person who is expert at their work
- **Purpose is** the reason something is done or created or for which something exists.
- **Policy** is a law, regulation, procedure, administrative action, incentive, or voluntary practice of governments and other institutions.

Compliance and IA Offices – Collaboration
WHY

Remember your "WHY" P's

- **Process** a series of actions or steps taken to achieve a particular end.
- **Progress** forward or onward movement toward a destination.
- **People** are the entire body of persons who constitute a community or other group by a common culture, history, religion, or the like.
- **Partnership** the state or condition of being a partner; participation; association; joint interest.
- **Participatory** allowing people to take part in or become involved in an activity

Compliance and IA Offices – Collaboration
WHY

Remember "WHY" your P's

- **Performance** is the execution or accomplishment of work, acts, etc.
- **Protection** the act of protecting or the state of being protected; preservation from injury or harm.
- **Preventative** serving to prevent or hinder
- **Proactive** serving to prepare for, intervene in or control an expected occurrence or situation, especially a negative or difficult one; anticipatory

Internal Audit and Compliance Offices IACOs Collaboration
WHY

Strong collaboration between Internal Audit and Compliance can improve the overall effectiveness of both Offices.

Clearly understanding the rules can help Compliance and Internal Audit better define the Scope of Work for a particular activity.

Clearly defining what controls you intend to test in a compliance review or internal audit, Scope of Work is critical to ensuring that the audit findings are understood and help avoid scope creep.

Internal Audit and Compliance Offices IACOs Collaboration
WHY

Internal audit and Compliance share an important set of common objectives.

Working together is critical to achieving common goals. IA and Compliance must meet often, clarify their responsibilities, communicate well, and be willing to each take a supporting role when necessary.

It can be challenging to quantify the value that each function brings to the organization; when Internal Audit and Compliance work together the increase in that value is difficult to deny!

Internal Audit and Compliance Offices IACOs Collaboration

WHY

Shared Data & Insight

Leverage technology to:

Transform how you collect and classify data – start with the end in mind

- A taxonomy will give you more agility and operational control in accessing information in meaningful ways

Standardize your data creation

Implement standard-based analysis tools

- Bring context to data by presenting information in a way that is semantically pure and relevant to the decision on hand

Internal Audit and Compliance Offices IACOs Collaboration

WHY

Help Compliance develop internal control knowledge

Compliance professionals typically come from legal or coding backgrounds, so many don't always have a great understanding of internal controls.

Teaming up with Internal Audit can offer the Compliance professionals the necessary know-how to address these controls in detail, and together, to be able to build a solid line of defense against irregularities that could lead to compliance failures.

Internal Audit and Compliance Offices IACOs WHY

Back up Compliance when a 'no' is involved

Saying "no" takes courage but also requires strong support from others in the organization. Compliance individuals face such challenges daily and are often labeled as being negative, hindering progress, or "doing things by the book."

This is primarily because some rules are not always well supported with justifications. Some view them as unnecessary, either because they don't understand the reasoning for the rule or can't see its value.

Convincing the business units takes additional work to articulate how rules can translate into gains and losses.

Internal Audit is trained to analyze monetary impacts to resonate with audit recommendations. Therefore, by allying with Compliance, Internal Audit could help compliance ease the tension with business units and make compliance's job more productive.

Internal Audit and Compliance Offices IACOs WHY

Consider the significant impact of small failures

Risk – legal, financial, operational, reputational

Internal audit looks at risk mainly from the point of view of material impact. What would be the monetary impact on revenue, for example, if a control failed? What would be the cost justification if an internal control were implemented to detect payment fraud?

Contrarily, the idea of materiality may not be relevant to addressing some compliance issues.

Internal Audit needs to adjust its view when working with Compliance to analyze compliance risks in a relevant way properly.

Internal Audit and Compliance Offices IACOs WHY

Cooperate, but maintain clear lines between IAC

It is easy to blur the lines between each other's job responsibilities when Internal Audit works together with Compliance. Not only can unclear lines of responsibility confuse others, but they also create inefficiency.

Despite efforts by some organizations to lump both functions into one, they are fundamentally different.

Compliance is a management function; as such, compliance is the client of internal Audit.

In contrast, Internal Audit is independent of management functions and oversees management activities.

Yes, Internal Audit and Compliance serve as counterparts to each other, but they play separate, and distinct roles and those roles should be well defined.

In practice, Internal Audit should never treat Compliance as part of the Audit team or vice versa.

Internal Audit and Compliance Offices IACOs WHY

Engage Compliance for better policies and procedures

Among the most common recommendations in audit reports is to improve policies and procedures. The existing policies are often not specific or comprehensive enough to guide business activities.

Compliance is the perfect team to call to take action. With their legal expertise, Compliance professionals are good at drafting policies, and they often are the lead policymakers in an organization.

However, policies without procedures to back them up will be considered not documented, not in place. Inadequate procedures equally harm operational efficiencies and create conflicts.

Developing reasonable procedures requires in-depth insights into processes and controls, which can be a weak spot for compliance. Therefore, Compliance alone can't fix the problems.

A partnership between Internal Audit and Compliance would be the right approach for Compliance to reshape the policies and Internal Audit to help with the procedures. This partnership reaffirms the bond between the two functions.

Internal Audit and Compliance Offices IACOs WHY

Emphasize deterrence over detection in compliance controls

Managing compliance risks is all about taking pre-emptive measures or adopting controls to prevent undesirable events.

Examining sales margins before potential deals with channel sales partners may potentially stop a bribery scam.

Conducting a third-party screening may disengage a supplier with a bad reputation before it's too late.

Internal audit should keep in mind that it's not good enough to have the Compliance become a referee regarding these critical controls, but instead, it should exercise these controls on its own.

Internal Audit and Compliance Offices IACOs WHY

Assure compliance training is adaptive and effective

Compliance training is one of the key elements of any good compliance program. Training the right people at the right time in the right way is critical.

Compliance is responsible for those training programs and should be held accountable for doing a good job of developing them. When evaluating the training, however, Internal Audit can help focus those programs and provide assurance that they are effective.
Training could be less adaptive and focused, meaning compliance has not customized the training contents based on the audiences' job scope, or it is not tailored training for a dispersed workforce in high-risk markets.

The employees or management who have direct contact with government officials or deal with state-owned entities should be prioritized with more intense training programs. The form of training also needs to be adjusted to fit the risk profile of the audience.

Internal Audit and Compliance Offices IACOs

WHY

View compliance risk through the lens of behaviors and actions

- Compliance usually focus on regulatory risk. Keeping track of what regulators are saying is how they typically start their day. Gauging regulatory risks largely involves predicting which corporate behaviors could lead to potential compliance lapses and how to prevent such behaviors. Risk acceptance is generally not an option from compliance's point of view.

- Internal Audit must view risk from a much broader scope that includes operational and financial risks, as well as other types of risk. It might involve a risk strategy that constitutes risk acceptance and mitigating efforts based on the organization's risk appetite. Indeed, Internal audit assesses risks based on analyzing robust issues like magnitude and chance of occurrence, rather than merely on behaviors. Therefore, when working with compliance on compliance risk assessment, internal audit should keep in mind the assessment will be focused on behaviors or activities rather than financial impacts.

Internal Audit and Compliance Offices IACOs WHY

Aid compliance in evaluating and communicating its value proposition

Contingent-based approach - The only time compliance generally gets attention is when a company receives a large penalty for violating a regulation, even though it is deemed shortsighted.

How many organizations would take time to do a cost analysis for how much they would have to pay for a **Violation** for every single dollar made for profit.

Nor is there an infinite amount of resources to spend on compliance. With its unique position, Internal Audit will be an ideal ally for compliance to leverage its voice to advocate the best practice of Corporate Compliance Programs and evaluate its value proposition.

Internal Audit and Compliance Offices IACOs WHY

Internal Audit and Compliance should cooperate on investigations

Legal and/or Compliance is typically the first function notified when there are whistleblower complaints. It is often responsible for maintaining the whistleblower hotline—but it may be the last party to be considered for conducting investigations into those complaints.

There are various reasons for this: It could be either budget constraints or lack of resources. But largely, compliance professionals are not hired to focus on investigations. Compliance investigations are complex, involve a unique set of skills, and can be easily derailed if not handled correctly.

However, compliance is a great source to mitigate legal issues that are encountered in the course of investigations. Teaming up with compliance enables the investigation team, including Internal Audit, to get to the bottom of the case with limited legal exposure.

Internal Audit and Compliance Offices IACOs Collaboration - WHAT

Encourage Open Communication

- How a compliance function is perceived is directly correlated to the culture and management style of the leadership. It is important to foster a work environment consisting of open and honest communication, which fosters trust and empowers employees. Management training on how to empower employees is critical to prevent micromanagement, while a policy regarding whistleblowing/compliance should also be established.

Build A Culture Of Commitment

- Building a culture of commitment is a journey that begins with inspiring people with a purpose. The only way to sustain this commitment is to make leaders' visible behaviors mirror the company's core values. Upskilling people is good, but the only way to guard your culture is by holding leaders accountable for leading by example and practicing what they preach.

Shift Your Mindset First

- The first thing is to shift your mindset from compliance function to compliance business partner. That means actively seeking to understand the business and ensuring that compliance solutions are tailored and communicated in a way that solves these problems. Establishing the partnership prior to enforcing the rules also helps both parties feel that they're working together rather than being watched.

July 202 Forbes Slides 12 - 16

Internal Audit and Compliance Offices IACOs Collaboration - WHAT

Bring Employees Into The Conversation

Compliance is a necessary "what," but organizations need employees to partner with leadership in demystifying the "why." A compliance committee with employee involvement can create internal champions for policies that keep everyone safe and protected. Bring employees into the conversation to help co-create solutions and they can help bring others along.

Actively Listen And Provide Feedback

- Effective compliance management involves active listening and providing feedback to managers and employees that helps them navigate decisions before they become minefields. Our compliance leaders provide a safe environment where the exchange of questions and answers does not create an air of suspicion but rather a collegial and team-based one of making the best decisions possible.

July 202 Forbes Slides 12 - 16

Internal Audit and Compliance Offices IACOs Collaboration - WHAT

Help People Understand The 'Why'

- I think you have to help people understand the "why" behind the policies. Most compliance documents and statements are permutations (many times removed) of common-sense practices. If you can help people understand what the policies are there to do, and why they're important, it goes a long way.

Explain The Consequences Of Non-Compliance

- It's crucial to build the awareness of consequences that can result from non-compliance within your workplace. HR has an important role in establishing an organization's culture, and a critical part of being transparent with employees surrounding compliance functions is clearly illustrating the potential issues that can arise from violating compliance protocols.

July 202 Forbes Slides 12 - 16

Internal Audit and Compliance Offices IACOs Collaboration - WHAT

Share Compliance Needs Differently

- While compliance is essential, to become a business partner, it's time to communicate and share compliance needs differently. Instead of always being the first thing employees see or read, it should be the next thing. Share what the employee needs to know as it relates to their own personal interest (in layman's terms, of course), and then have the in-depth compliance details as a second click.

Make It A Shared Responsibility

- Make compliance a shared responsibility by creating a cross-functional team led by HR, finance, legal, security and members from other critical business functions. While each of the members may have individual deliverables, creating a team destigmatizes compliance-related tasks, and encourages collaboration and awareness throughout the organization.

July 202 Forbes Slides 12 - 16

Internal Audit and Compliance Offices IACOs Collaboration - WHAT

Provide Constant Compliance Training

- The most effective way for leaders to get employee buy-in to their corporate compliance plan is by providing initial training during onboarding, as well as annual follow-up training. Employees are far more likely to follow company rules and procedures when they're educated on how to stay compliant than they are when they're reprimanded or punished for failing to do so.

Reframe It As A Necessary Checkpoint

- Compliance is essential for most businesses as companies are required to adhere to external rules. Reframe compliance as a necessary checkpoint to ensure best practices. Big Brother personas are oppressive and intrusive. Compliance should be framed as transparent and helpful processes to maintain regulatory objectives, which guarantee fair markets and protect employees and investors.

July 202 Forbes Slides 12 - 16

Compliance and IA Offices – Collaboration

WHAT RISK AREAS

COMPLIANCE & IA –TRAIN TOGETHER & SHARE KNOWLEDGE!

- Contracts
  - Due Diligence Level
- Revenue Integrity
  - Minimize compliance risk
  - Optimize revenue reimbursement opportunities
  - Improve clinical documentation practices
  - Ensure appropriate capture of severity of illness (SOI) and risk of mortality (ROM)
  - Survey and rapidly reduce risk of improper claims: rejections, underpayment, overpayments, audits, fines, and penalties
  - Identify regulatory changes that impact services and delivery

Compliance and IA Offices – Collaboration

WHAT RISK AREAS

AREAS COMPLIANCE & IA –TRAIN TOGETHER & SHARE KNOWLEDGE!

PRIVACY

- HHS, the Office for Civil Rights ("OCR")
- Data Breach
- Consistent Documentation, Investigations, Action Plans
- Contracts – Risk Assessments
  - BAA – Business Associate Agreement
  - DUA – Data Use Agreement
- Monitoring – Reactive, Active, Proactive

INFORMATION SECURITY

- Contracts – Risk Assessments
- Cyber Security

Internal Audit and Compliance Offices IACOs Collaboration

WHY

Internal audit and Compliance share an important set of common objectives.

Working together is critical to achieving common goals. IA and Compliance must meet often, clarify their responsibilities, communicate well, and be willing to each take a supporting role when necessary.

It can be challenging to quantify the value that each function brings to the organization; when Internal Audit and Compliance work together the increase in that value is difficult to deny!

Internal Audit and Compliance Offices IACOs Collaboration

WHY

Shared Data & Insight

Leverage technology to:

Transform how you collect and classify data – start with the end in mind

A taxonomy will give you more agility and operational control in accessing information in meaningful ways

Standardize your data creation

Implement standard-based analysis tools

Bring context to data by presenting information in a way that is semantically pure and relevant to the decision on hand

Internal Audit and Compliance Offices IACOs Collaboration

WHY

Help Compliance develop internal control knowledge

Compliance professionals typically come from legal or coding backgrounds, so many don't always have a great understanding of internal controls.

Teaming up with Internal Audit can offer the Compliance professionals the necessary know-how to address these controls in detail, and together, to be able to build a solid line of defense against irregularities that could lead to compliance failures.

Internal Audit and Compliance Offices IACOs WHY

Back up Compliance when a 'no' is involved

Saying "no" takes courage but also requires strong support from others in the organization. Compliance individuals face such challenges daily and are often labeled as being negative, hindering progress, or "doing things by the book."

This is primarily because some rules are not always well supported with justifications. Some view them as unnecessary, either because they don't understand the reasoning for the rule or can't see its value.

Convincing the business units takes additional work to articulate how rules can translate into gains and losses.

Internal Audit is trained to analyze monetary impacts to resonate with audit recommendations. Therefore, by allying with Compliance, Internal Audit could help compliance ease the tension with business units and make compliance's job more productive.

Internal Audit and Compliance Offices IACOs WHY

Consider the significant impact of small failures

Risk – legal, financial, operational, reputational

Internal audit looks at risk mainly from the point of view of material impact. What would be the monetary impact on revenue, for example, if a control failed? What would be the cost justification if an internal control were implemented to detect payment fraud?

Contrarily, the idea of materiality may not be relevant to addressing some compliance issues.

Internal Audit needs to adjust its view when working with Compliance to analyze compliance risks in a relevant way properly.

Internal Audit and Compliance Offices IACOs WHY

Cooperate, but maintain clear lines between IAC

It is easy to blur the lines between each other's job responsibilities when Internal Audit works together with Compliance. Not only can unclear lines of responsibility confuse others, but they also create inefficiency.

Despite efforts by some organizations to lump both functions into one, they are fundamentally different.

Compliance is a management function; as such, compliance is the client of internal Audit.

In contrast, Internal Audit is independent of management functions and oversees management activities.

Yes, Internal Audit and Compliance serve as counterparts to each other, but they play separate, and distinct roles and those roles should be well defined.

In practice, Internal Audit should never treat Compliance as part of the Audit team or vice versa.

Internal Audit and Compliance Offices IACOs WHY

Engage Compliance for better policies and procedures

Among the most common recommendations in audit reports is to improve policies and procedures. The existing policies are often not specific or comprehensive enough to guide business activities.

Compliance is the perfect team to call to take action. With their legal expertise, Compliance professionals are good at drafting policies, and they often are the lead policymakers in an organization.

However, policies without procedures to back them up will be considered not documented, not in place. Inadequate procedures equally harm operational efficiencies and create conflicts.

Developing reasonable procedures requires in-depth insights into processes and controls, which can be a weak spot for compliance. Therefore, Compliance alone can't fix the problems.

A partnership between Internal Audit and Compliance would be the right approach for Compliance to reshape the policies and Internal Audit to help with the procedures. This partnership reaffirms the bond between the two functions.

Internal Audit and Compliance Offices IACOs WHY

Emphasize deterrence over detection in compliance controls

Managing compliance risks is all about taking pre-emptive measures or adopting controls to prevent undesirable events.

Examining sales margins before potential deals with channel sales partners may potentially stop a bribery scam.

Conducting a third-party screening may disengage a supplier with a bad reputation before it's too late.

Internal audit should keep in mind that it's not good enough to have the Compliance become a referee regarding these critical controls, but instead, it should exercise these controls on its own.

Internal Audit and Compliance Offices IACOs WHY

Assure compliance training is adaptive and effective

Compliance training is one of the key elements of any good compliance program. Training the right people at the right time in the right way is critical.

Compliance is responsible for those training programs and should be held accountable for doing a good job of developing them. When evaluating the training, however, Internal Audit can help focus those programs and provide assurance that they are effective.
Training could be less adaptive and focused, meaning compliance has not customized the training contents based on the audiences' job scope, or it is not tailored training for a dispersed workforce in high-risk markets.

The employees or management who have direct contact with government officials or deal with state-owned entities should be prioritized with more intense training programs. The form of training also needs to be adjusted to fit the risk profile of the audience.

Internal Audit and Compliance Offices IACOs

WHY

View compliance risk through the lens of behaviors and actions

- Compliance usually focus on regulatory risk. Keeping track of what regulators are saying is how they typically start their day. Gauging regulatory risks largely involves predicting which corporate behaviors could lead to potential compliance lapses and how to prevent such behaviors. Risk acceptance is generally not an option from compliance's point of view.

- Internal Audit must view risk from a much broader scope that includes operational and financial risks, as well as other types of risk. It might involve a risk strategy that constitutes risk acceptance and mitigating efforts based on the organization's risk appetite. Indeed, Internal audit assesses risks based on analyzing robust issues like magnitude and chance of occurrence, rather than merely on behaviors. Therefore, when working with compliance on compliance risk assessment, internal audit should keep in mind the assessment will be focused on behaviors or activities rather than financial impacts.

Internal Audit and Compliance Offices IACOs WHY

Aid compliance in evaluating and communicating its value proposition

Contingent-based approach - The only time compliance generally gets attention is when a company receives a large penalty for violating a regulation, even though it is deemed shortsighted.

How many organizations would take time to do a cost analysis for how much they would have to pay for a **Violation** for every single dollar made for profit.

Nor is there an infinite amount of resources to spend on compliance. With its unique position, Internal Audit will be an ideal ally for compliance to leverage its voice to advocate the best practice of Corporate Compliance Programs and evaluate its value proposition.

Internal Audit and Compliance Offices IACOs WHY

Internal Audit and Compliance should cooperate on investigations

Legal and/or Compliance is typically the first function notified when there are whistleblower complaints. It is often responsible for maintaining the whistleblower hotline—but it may be the last party to be considered for conducting investigations into those complaints.

There are various reasons for this: It could be either budget constraints or lack of resources. But largely, compliance professionals are not hired to focus on investigations. Compliance investigations are complex, involve a unique set of skills, and can be easily derailed if not handled correctly.

However, compliance is a great source to mitigate legal issues that are encountered in the course of investigations. Teaming up with compliance enables the investigation team, including Internal Audit, to get to the bottom of the case with limited legal exposure.

Compliance and IA Offices – Collaboration

HOW

Compliance "How" — P's:

Example Revenue Cycle

- **Practicum**
- **Prods**
- **Probes**
- **Programs**
- **Projects**

The "HOW"  of the Compliance Program – Practicum

Practicum

- ❑ *Verb: to poke or stir, to incite to action*
- ❑ Prods are frequently conducted by the compliance office and only convert to Probes if there is sufficient evidence demonstrating a failure in compliance with a law, rule, regulation, or policy/procedure.
- ❑ Prods typically look at real-time data or within a 6-12 month time frame.
- ❑ Initiating a Prod will allow time to provide education and/or implement an immediate resolution before proceeding with a Probe.
- ❑ Prods will have a written report issued; this may or may not require a management response depending on if findings.

The "HOW"  of the Compliance Program – Prod(s)

Prod(s)

- *Verb: to poke or stir, to incite to action*
- Prods are frequently conducted by the compliance office and only convert to Probes if there is sufficient evidence demonstrating a failure in compliance with a law, rule, regulation, or policy/procedure.
- Prods typically look at real-time data or within a 6-12 month time frame.
- Initiating a Prod will allow time to provide education and/or implement an immediate resolution before proceeding with a Probe.
- Prods will have a written report issued; this may or may not require a management response depending on if findings.

The "HOW"  of the Compliance Program – Prod(s)

continued

Preventive / Detective

Where a PROD can originate from:

- **OIG, CMS, Regulations, RAC, TPE (pre-payment), Revenue Integrity**

1. Compliance Lead to define the problem and assign compliance staff responsible for the PROD

Assigned staff member will:

2. Research regulations for requirements
3. Research previous Webi/Clarity Reports in files (Departmental, Compliance, and Internal Audit)
4. Take identified CPT/HCPCS Codes per regulations and search in the charge description master (CDM) for every department (cost center) with a quantity and zero in those CPT/HCPCS Codes.
5. Meet with Manager Data Integrity and validate the information and share information with the compliance team.

The "HOW"  of the Compliance Program – Prod(s)

continued

Preventive / Detective

6. Identify operating areas/departments, schedule a meeting to discuss and confirm the potential area of concern and next steps.
7. IAC (Compliance and Internal Audit) to meet and determine Webi Charge and Payment report criteria
8. Run a Webi by criteria (3-mos) or time period determined
   A. Governmental payers
      - Medicare
      - Medi-Cal
      - TRICARE/CHAMPUS/CHAMPVA
      - Managed Medi-Cal (will be within Offsetting period)
9. Select Sample for Clinical review (Compliance)
10. Meet with Manager Data Integrity for Outcome Review. (Final Review)
11. If no issues identified > STOP PROD > WRITE REPORT
12. If issues identified > EXPAND PROD > identify timeframe or convert to a PROBE
13. Meet with areas/departments regarding findings

The "HOW"  of the Compliance Program – Probe(s)

Probe(s)

- *Verb: to search into and explore very thoroughly: subject to a penetrating investigation*
- Probe if there is sufficient evidence demonstrating a failure in compliance with a law, rule, regulation, or policy/procedure
- Initiating a Probe immediate education and/or implement an immediate resolution before proceeding with a Probe
- Phase I – **Re-bill** period (4 years)
  - Medicare, TRICARE/CHAMPUS, Medi-Cal, CCS & Managed Payers*
- Phase II – **Repayment** period (2 years)
  - Medicare, TRICARE/CHAMPUS, +/-Medi-Cal & CCS

The "HOW"  of the Compliance Program – Probe(s)

continued

Where a PROBE can originate from:

Reports of Inappropriate Billing, Compliance Office Findings, Compliance Working Committee (CWC), Findings from a Previous PROD.

Preventive / Detective

1. Meet with operating areas/departments
2. STOP > Inappropriate billing (if applicable)
3. Education

The "HOW"  of the Compliance Program – Probe(s)

continued

Preventive / Detective

4. Define the problem (Rebill and Repayment) and assign a person responsible for the PROBE
5. Research regulations for requirements of all the years involved. (max 6 years)
6. Research previous Webi/Clarity reports in history files (Departmental, Compliance **and Internal Audit**) (max 6 years)
7. Take identified CPT/HCPCS Codes per regulations and search in the charge description master (CDM) for every department (cost center) with a quantity or all years involved. (max 6 years) in those CPT/HCPCS Codes.
8. Meet with Manager Data Integrity and validate the information and share information with the compliance team and **the internal audit team**.

The "HOW"  of the Compliance Program – Probe(s)

continued

Preventive / Detective

9. Identify areas/departments and schedule a meeting
10. Internal Audit & Compliance (IAC) to meet and determine Webi Charge and Payment report criteria
11. 4-Years REBILL & 2-Years REPAYMENT > **Internal Audit (**IA) >Run a Webi by criteria for a time period determined
    A. Governmental payers
        a. Medicare
        b. Medi-Cal
        c. TRICARE/CHAMPUS/CHAMPVA
        d. Managed Medi-Cal (will be within Offsetting period)
    B. Clinical Review
        a. Small population > Compliance clinical review (100%)
    C. External Clinical Review
        a. Large population > Extrapolation

The "HOW"  of the Compliance Program – Probe(s)

continued

Preventive / Detective

12. Meet with Manager Data Integrity > Internal Audit (IA)
13. IA to create a base report for Clinical review (Compliance) from Webi charge to payment report
14. IA to meet with (Compliance) coder assigned to the PROBE
15. Clinical review (Compliance)
16. Meet with Manager Data Integrity > Compliance
17. If 100% DRAFT IAC report REBILL/REPAYMENT to be written sent to Compliance and IA Leaders for approval and then to operational areas for management responses and approval
18. Operational areas for REBILL for Patient Financial Services (PFS) and Hospital Billing (HB) Team
19. IA > REPAYMENT and letters and checks

The "HOW"  of the Compliance Program – Probe(s)

continued

Note: If disagreement between coders (next steps)

1. Contact Health Information Management (HIM)
   - Present detail information of what type of review is needed
     - If still a disagreement
2. Contact Outside Vendor

The "HOW"  of the Compliance Program – Project(s)

Project(s)

- ❑ *Verb: to plan, figure or estimate for the future*

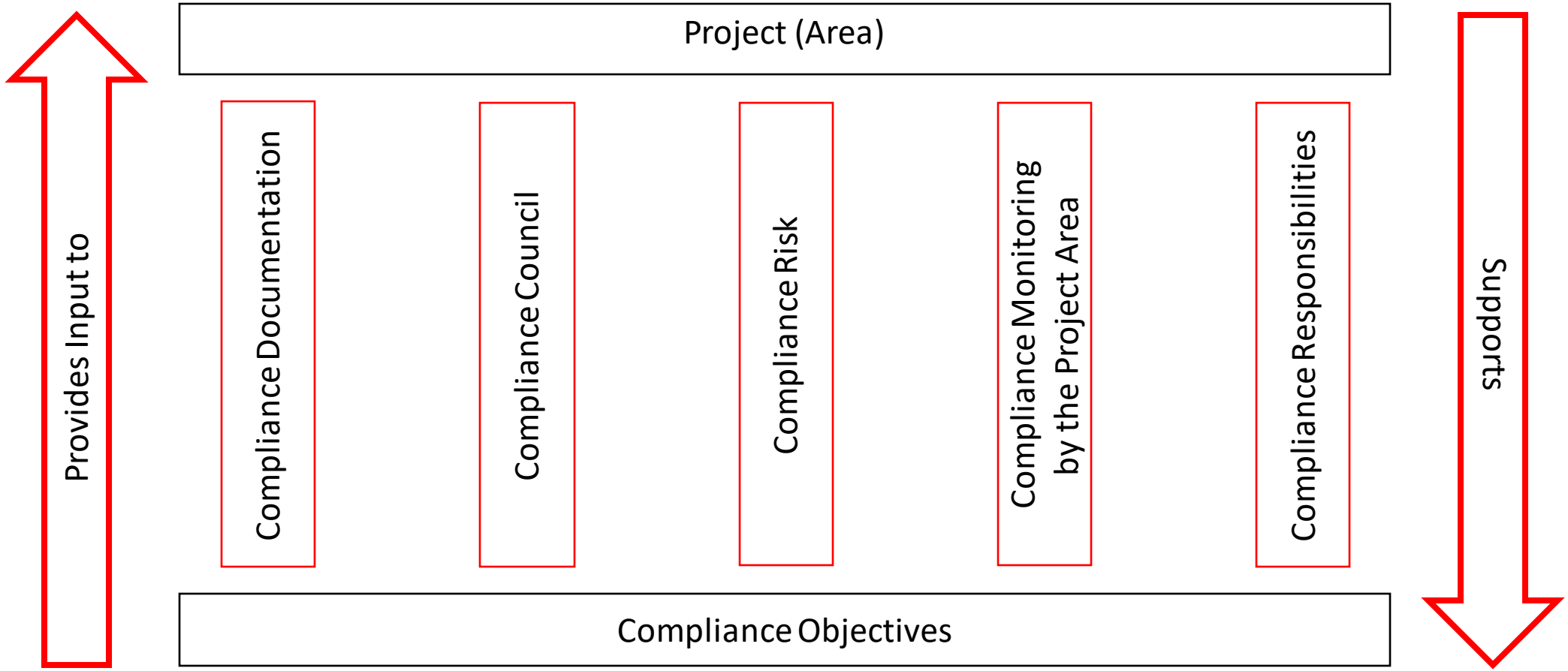
❑Compliance **Initiated**

❑Internal Audit **Initiated** *OR*

❑Compliance/Internal Audit **Involvement**

The "HOW"  of the Compliance Program – Project(s)

continued



The "HOW"  of the Compliance Program – Project(s)

Project Compliance Framework

The framework's base recognizes the rules, regulations, or standards that the project covered must meet. As part of the project initiation phase, it is suggested that those rules should be explicitly documented. For purposes of this framework, they are called "compliance objectives."

Once this recognition has been made explicit, it is necessary to establish five pillars on which the project's various activities must rest. These pillars also act as tools of the framework:

- **Compliance Documentation:** The proposed tool is a set of draft documents that dynamically will change in each of the stages and components. It is necessary that the documentation be aligned with the principles of quality managed by the organization and, therefore, is treated as a deliverable of the project.
- **Compliance Council:** Although it is not likely that a functional organization provides resources in the area of control or review to the project, it is essential to involve them in compliance activities. Incorporated into the project experts in various areas such as legal, environmental, and technical. Establishing a compliance council is the best strategy to achieve appropriate coverage of all required activities.

The "HOW"  of the Compliance Program – Project(s)

continued

Project Compliance Framework - continue

- **Compliance Risk**: Project managers are used to handling project risks; however, compliance risks occasionally fall beyond the scope of the project itself. For example, according to standards established by the owners, failures in the implementation of security measures may be reflected years after the project has been closed, when fraud is reported. Clearly, the project manager is not responsible for the results of the "operational" problem, but these risks must be understood during the execution of the project. Additionally, these risk analyses generate corporate decisions that can affect other areas of the project itself.
- **Compliance Monitoring:** Monitoring is one of the key elements in the framework and is reflected in establishing a specific review for the project in aspects of compliance. Each project activity aimed to comply or to build the compliance objectives should be analyzed by the review. This pillar requires the existence of an organization, internal or external to the project, to record all aspects that need to be considered high risk or that create a high impact on the compliance objectives.
- **Compliance Responsibilities**: To the extent that the various team members understand the importance of compliance, all activities and their corresponding compliance objectives shall be allocated as parts of the project's tasks and processes.

The "HOW"  of the Compliance Program – Project(s)

Business Continuity/Crisis Planning

- Background – CMS requirement and COVID has spotlighted the importance
- Education – Review/understand the impact of scenarios on processes
- Category I – Process that if not performed poses an immediate threat to employee or patient safety or immediate negative financial impact
- Category II – Process that if delayed can cause a large negative impact – function can be disrupted temporarily but most be reestablished within xxx hours
- Category III – Contractually required processes with vendors, employees, or patients (both external and internal) that could cause a minor impact if delayed

The "HOW"  of the Compliance Program – Project(s)

continued

Business Continuity/Crisis Planning *continued*

- Hazard Vulnerability Analysis conducted by multi-disciplinary team
- Incident Command Center
- Supply Chain Resiliency Plan – Pre-event, Response, Recovery

The "HOW"  of the Compliance Program – Program(s)

Program(s)

- 1 of the 7 Elements of an Effective Compliance Program

- Monitoring – involves ongoing checking/surveillance to measure and ensure quality internal controls are in place. By doing so this allows the organization to prevent, detect and resolve potential compliance violations. This process is usually performed by departmental staff or management.

- Testing – periodic selection and review of submitted monitoring tools by operations to validate the operating effectives of internal controls and adherence to Federal/ State laws, rules, regulations as well as policies and procedures.

The "HOW"  of the Compliance Program – Program(s)

continued

Preventive / Detective Compliance Program

Ongoing monitoring is the program managers' responsibility. They are the ones most familiar with their own operations and should be charged with identifying risk areas of their responsibility; developing appropriate internal controls, policies, and procedures; and monitoring them to verify they are being followed.

- What reports are used by management each day to manage operations (detective monitoring).
- What activities occur in day-to-day processes to correct mistakes as they occur (preventive monitoring).
- What is the manager's understanding of the compliance program.
  - Opportunity to find out where the program has weaknesses
  - Opportunity to educate manager on what Compliance's role is and where accountability for compliance rests
  - Lastly, talk to them about your game plan for the program and solicit support

The "HOW"  of the Compliance Program – Program(s)

continued

- Goal is to **not** replicate or duplicate anything if there is something in place that can include compliance monitoring.

- If it has to be created, see if you can move the organization to a dashboard that is **more than compliance**….key to integration into operations.

The "HOW"  of the Compliance Program – Program(s)

continued

- How monitoring activities are identified? – based on risk
- Who is responsible for conducting monitoring? – management
- Frequency of monitoring reporting? – monthly, quarterly but no longer
- Who is monitoring reported to? – compliance department is one of the customers
- Is monitoring a component of a corrective action plan? – yes, if it falls below the acceptable accuracy threshold
- What is the acceptable accuracy threshold? – 90% or 95% (organization needs to decide based on their risk appetite)
- What happens if consecutive months of monitoring results fall below the accuracy threshold? – define an escalation process
- What happens if consecutive months of monitoring results meet or exceed

The "HOW"  of the Compliance Program – Program(s)

continued

- Once risks are identified and monitoring needs are determined, need to develop an easy reporting tool.
- Suggest using Excel….because it can easily convert data to graphs (management and committees like this).
- Determine "how many" monitoring elements should be reported and how often to report information to senior management and board. It may be different based on the audience.
- Senior Management and Compliance Committees should see results before reported to the Board or a Board Committee.

The "HOW"  of the Compliance Program – Program(s)

continued

Example: Stimulus Program Management

- Background – Stimulus Program Management
- Education – Understand the stimulus programs available
- Phase I – Determine eligibility
- Phase II – Evaluate applications for accuracy
- Phase III – How is data captured, managed and verified
- Phase IV – Are policies/procedures to address this are in place?
- Phase V – Do any existing policies need to be modified due to conflicts?
- Phase IV – Is a master change log in place to memorialize events and decisions to include changes in regulatory interpretation?

The "HOW" for Privacy Compliance

Contracts: BAA, DUA, Monitoring Reactive, Active/Proactive

- CONTRACTS: BAA Business Associate Agreement
- CONTRACTS: DUA Data Use Agreement
- PRIVACY MONITORING – REACTIVE
- PRIVACY MONITORING – ACTIVE or PROACTIVE

The "HOW" of Privacy-Contracts: BAA

"Bee – Aware" ….. Do you need a BAA?

- **Bees = Business Associates**
- **Business Associates Agreement (BAA)**: Is a written agreement with a person or entity that performs certain functions (i.e., treatment, payment, or health care operations) that involve the use or disclosure of protected health information (PHI) on behalf of, or provides services to, a covered entity WITHOUT the written authorization of the patient.

- **Bee Hive = Covered Entity** is one of the following: **1.) A Health Care Provider 2.) A Health Plan 3.) A Health Care Clearing house** – who electronically transmit any health information in connection with transactions for which the U.S. Department of Health & Human Services has adopted standards.
- **Subcontractor** – an entity to whom a business associate delegates a function, activity or service (other than a workforce member). **The covered entity does not need to obtain a BAA from it's BA's subcontractors.*

- ***Bee Keeper = Enforcement Agencies*** **-** OCR - Office of Civil Rights
- ***Bee's Honey = Money $$$***
- *Abbreviations used throughout power point: BAA – Business Associate Agreement; BA – Business Associate; PHI – Protected Health Information*

"HOW"
Don't get STUNG!

Preventive / Detective

- **BEE – Proactive:** Ask yourself before engaging with a Vendor for their services … WILL they have access to PHI and HOW will they use it… do I need a BAA PRIOR to signing a contract ???

- **BEE – Assertive:** provide the Vendor CMC's BAA for review, if the Vendor provides a copy of their BAA provide to Legal ASAP!

- **BEE – Cautious:** if your not sure if a BAA is needed then contact your legal or compliance department for further direction.

- 4**BEE – Happy!** You followed the law, remained compliant and protected the patient's rights!!!

"HOW"
Don't get STUNG!

Preventive / Detective

- ❑Utilize Internal Audit to probe vendors in Accounts Payable or Contracting and verify that BAA's are in place if appropriate

- ❑Verify that the BAA's match the contract and are contained in the appropriate area for easy of retrieval/review

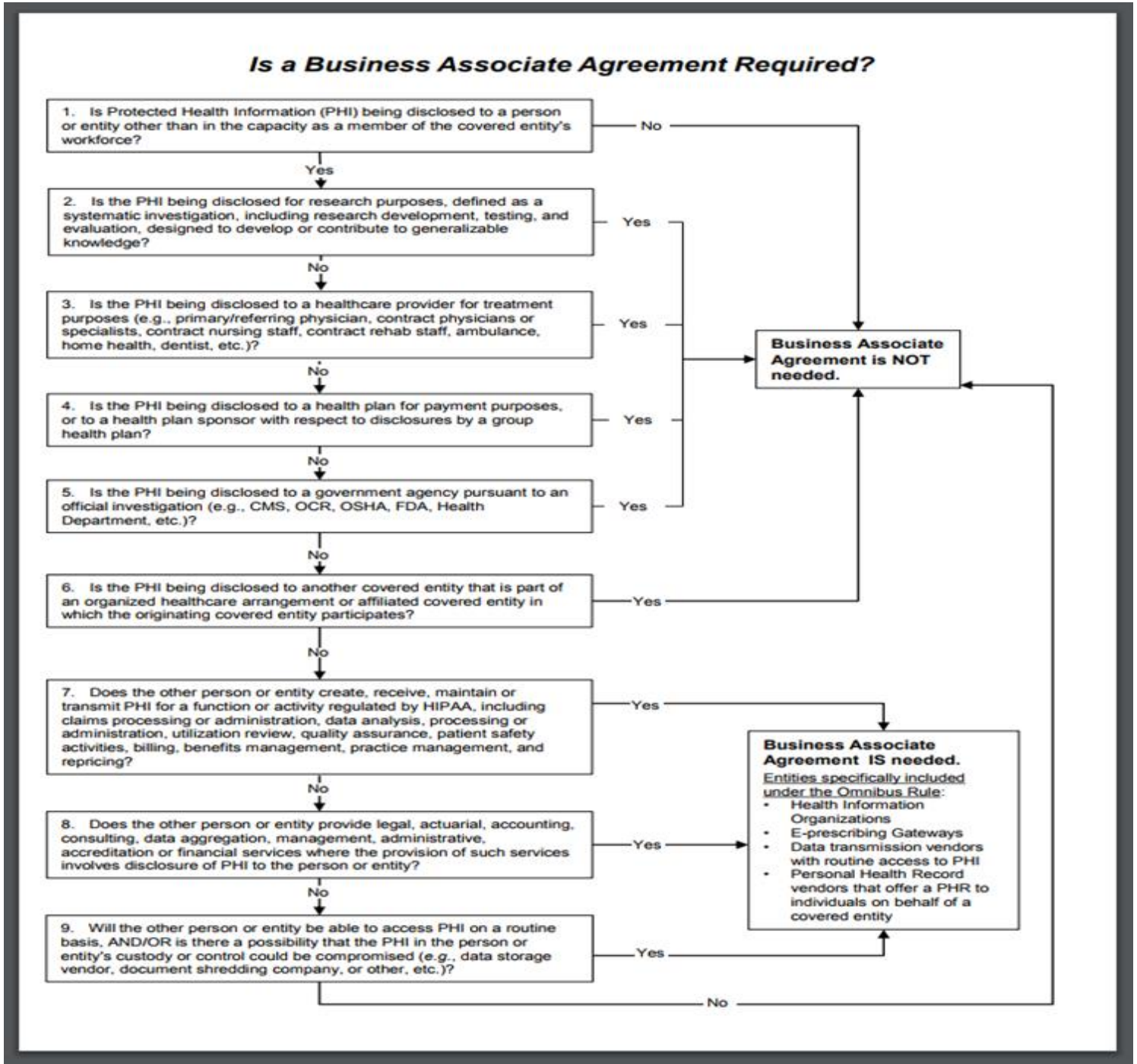
- ❑Are appropriate signatures on the BAA

The following steps should be considered when reviewing contracts for HIPAA Privacy and business associate impacts:

- Those contracts that are initiated from other organizations that perform non-treatment related functions on your behalf AND that involve the use and disclosure of individually identifiable health information should be reviewed for potential HIPAA Privacy Business Associate relationships. These contracts should be reviewed with the Privacy Office and if necessary with the Legal Office to determine whether a BA relationship exists.
- Requests from external entities to enter into a business associate agreement with the Organization should be forwarded to the Privacy Office to review and prepare a response. These requests could result from your area initiating or receiving a contract.
- Confidentiality and protection of health information should be part of your general contract terms and provide language that extends this if needed for specific grant/contract requirements. This requirement, however, is different than HIPAA business associate agreements, which are administratively very specific to the HIPAA Privacy Rule and who is covered. We want to ensure confidentiality per state and federal laws but do not want to create legal obligations under HIPAA where none exist.

- If HIPAA Privacy BA relationship exists, we will need to include a business associate agreement addendum to the contract based on the approved HIPAA BAA template. For inter-governmental agreements, we will need to either include the approved BAA addendum to an MOU or execute a standalone HIPAA BAA MOU based on the approved template.
- Most of the **confusion in general centers on the misconceptions** that any exchange of identifiable health information constitutes a business associate relationship. However, A business associate relationship usually does not exist between providers for treatment-related services, a grantor and grant recipient, or payer and provider.
- Testing services provided by the lab for healthcare providers do not require a BAA since 1) they are treatment-related and 2) they are public health activities and are required by law.
- The business associate relationship most often exists when an entity provides other than healthcare services for the covered entity (covered component), such as legal, accounting, consulting, billing, utilization review services, among others.

Is A Business Associate Agreement Required?



"HOW" Privacy-Contracts: DUA

Preventive / Detective

- A data use agreement (DUA) is an agreement that is required under the Privacy Rule and must be entered into ***before*** there is any use or disclosure of a limited data set (defined below) to an outside institution or any party. A limited data set is still protected health information (PHI), and for that reason, covered entities must enter into a data use agreement with any recipient of a limited data set.
- A data use agreement is the means by which covered entities obtain satisfactory assurances that the recipient of the limited data set will use or disclose the health information in the data set only for specified purposes. Even if the person requesting a limited data set from a covered entity is an employee or otherwise a member of the covered entity's workforce, a written data use agreement meeting the Privacy Rule's requirements must be in place between the covered entity and the limited data set recipient.
- At a minimum, any DUA must contain provisions that address the following:
  - Establish the permitted uses and disclosures of the limited data set;
  - Identify who may use or receive the information;
  - Prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as otherwise permitted by law;
  - Require the recipient to use appropriate safeguards to prevent an unauthorized use or disclosure not contemplated by the agreement;
  - Require the recipient to report to the covered entity any use or disclosure to which it becomes aware;
  - Require the recipients to ensure that any agents (including any subcontractors) to whom it discloses the information will agree to the same restrictions as provided in the agreement; and
  - Prohibit the recipient from identifying the information or contacting the individuals.

What is a limited data set?

- A limited data set is a data set that is stripped of certain direct identifiers specified in the Privacy Rule. A limited data set may be disclosed to an outside party without a patient's authorization only if the purpose of the disclosure is for research, public health, or health care operations purposes and the person or entity receiving the information signs a data use agreement (DUA) with the covered entity or its business associate.

- *Limited data sets may include only the following identifiers:*
  - Dates such as date of birth, admission, discharge, or service
  - City, state, and/or zip code (with street address removed)
  - Age
  - Any other unique code or identifier that is not listed as a direct identifier.

What is a limited data set?

continued

- This means that in order for a data set to be considered a limited data set, all of the following direct identifiers as they relate to the individual or his/her relatives, employers, or household members *must* be removed:
  - Names
  - Street addresses (other than town, city, state, and zip code)
  - Telephone and fax numbers
  - Email addresses
  - Social security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/driver's license numbers
  - Vehicle identifiers and serial numbers, including license plate numbers
  - Device identifiers and serial numbers
  - URLs and IP addresses
  - Biometric identifiers
  - Full face photographic images and any comparable images.

What is a limited data set?

continued

- **If the intended recipient of a limited data set is also creating the limited data set as my business associate, do I need both a data use agreement and business associate agreement?**

- Yes, you will need both a data use agreement (DUA) and business associate agreement (BAA) because the covered entity (Affiliated Covered Entity) is providing the recipient with PHI that may include direct or indirect identifiers. For that reason, a BAA could be required to before we disclose the direct identifiers to the recipient outside of Covered Entity.

“HOW” of Privacy
Monitoring – Reactive

Preventive / Detective / Resolution

Wait for the fax, email or call…… then investigate.

"HOW" of Privacy
Monitoring – Active

Preventive / Detective / Resolution

- Computerized
  - Implement technology to assist
  - Focus on a 3-4 rules
- Physical Locations
  - Create monitoring tools
    - Incorporate in Joint Commission tracers questions
  - Require high risk areas to submit self monitoring quarterly and privacy office spot check annually.
- Work with HR to establish and educate to a formal discipline policy for privacy violations.
- Measure how investigations are going:
  - How long to closure?
  - How often is notice required?
  - Which facilities are doing well?
  - How often is a violation confirmed?
  - What types of incidents are trending?
- Ensure consistent disciplinary process across organization

"HOW" of Privacy
Monitoring – Active

continued

- Corrective action plans
- Consistent investigations
- Complete documentation
- Prepare for a catastrophic breach before an incident.
  - □ Build an incident plan
  - □ Contract with a breach response vendor now.
  - □ Contract for breach insurance.
- Stay involved in the legislative process at both state and federal levels.
- Assess the state of your program at least annually.
- Build a work plan for your team that addresses program gaps.
- Add time to your calendar to work on these goals.
- Think like an auditor.

Security
Contracts, Risk Assessments, Trending, Tools

- **CONTRACTS**
- **RISK ASSESSMENTS**
- **TRENDING**
- **TOOLS**

"HOW" of Information Security Contract Review

Compliance, regulation

- Does the vendor agree to maintain compliance with an industry standard or government regulation (e.g. HIPAA, FERPA, FISMA, PCI DSS)?
- Will the vendor create, receive, maintain, or transmit Protected Health Information (PHI)? If yes, contact the Chief Privacy Officer for assistance.
- Will the vendor receive, maintain, or transmit credit card and/or debit card information?
- Will the vendor provide services that control or could impact the security of credit card and/or debit card information? If yes, contact the Payment Card Program for assistance.

"HOW" of Information Security Contract Review

continued

Assessment, certification, attestation, audit

- Does the vendor offer to provide a current third-party/independent attestation of information security controls (e.g. SSAE 18, PCI DSS, AOC), or a self attestation (e.g. HECVAT, CSA CAIQ) for themselves and any sub-contractors on a regular (usually annual) basis?

- Does the vendor agree to respond and cooperate during an information security investigation/assessment, process/record review/audit?

"HOW" of Information Security Contract Review

continued

Insurance, indemnification, liability

- Will the vendor add the Organization as an 'additional insured' party to the vendor's insurance to cover potential breach costs? The standard insurance indemnification clause in Organization contracts is for a $10M indemnity.
- Does the contract obligate the vendor to indemnify Organization and faculty/staff against legal actions/third party claims, including costs and fees?
- Does the vendor assume liability for costs of investigating, responding/mitigating an information security breach due to failure to conform to the contract's terms?

"HOW" of Information Security Contract Review

continued

Service Levels

- Does the vendor specify Service Levels with Service Level Objectives (e.g., 99.9% uptime) and scheduled maintenance cycle?

Disaster Recovery

- Does the vendor state that they have an established/documented Disaster Recovery process to protect Organization data or operations?

Intellectual Property

- Does the contract contain language to protect Organization data or intellectual property to the same level as the vendor's own protection?

"HOW" of Information Security Contract Review

continued

Information Security Awareness

- Does the vendor state that they have an established/documented information security awareness program for their employees and contractors?

Non-disclosure, confidentiality

- Does the vendor bind its employees and contractors to non-disclosure of customer data or intellectual property?

Sub-contractors

- Does the vendor state that all sub-contractors are obligated to comply with the same terms and conditions? This particularly applies to data destruction at termination of contract and notification of information security incidents.

"HOW" of Information Security Contract Review

continued

System Maintenance

- Does the vendor agree to maintain current software versions and patch regularly?
- Does the vendor agree to fix/patch information security deficiencies or bugs in its or subcontractors' service/software in a timely fashion? Contracts frequently use the term 'commercially reasonable.'

Notification, Incident Response

- Does the contract obligate the vendor to notify customer within 24 hours of major/significant issues?
- Does the contract define major/significant?

Notification, data breach

- Does the vendor agree to notify Organization within 48 hours of an information security incident or breach that has likely compromised or involves inappropriate access to Organization data?

"HOW" of Information Security Contract Review

continued

At contract termination

- Will, the vendor, agree to return the data at the Organization's request, and the data will be in a commonly readable program?
- Does the vendor agree to expedite the return of all Organization data or destroy the data, including backup copies, within a specified time period after termination of the agreement? It is reasonable to allow an extended period for the destruction of backup data.
- Does the vendor allow Organization to review or audit the data destruction process in real-time as well as afterward?

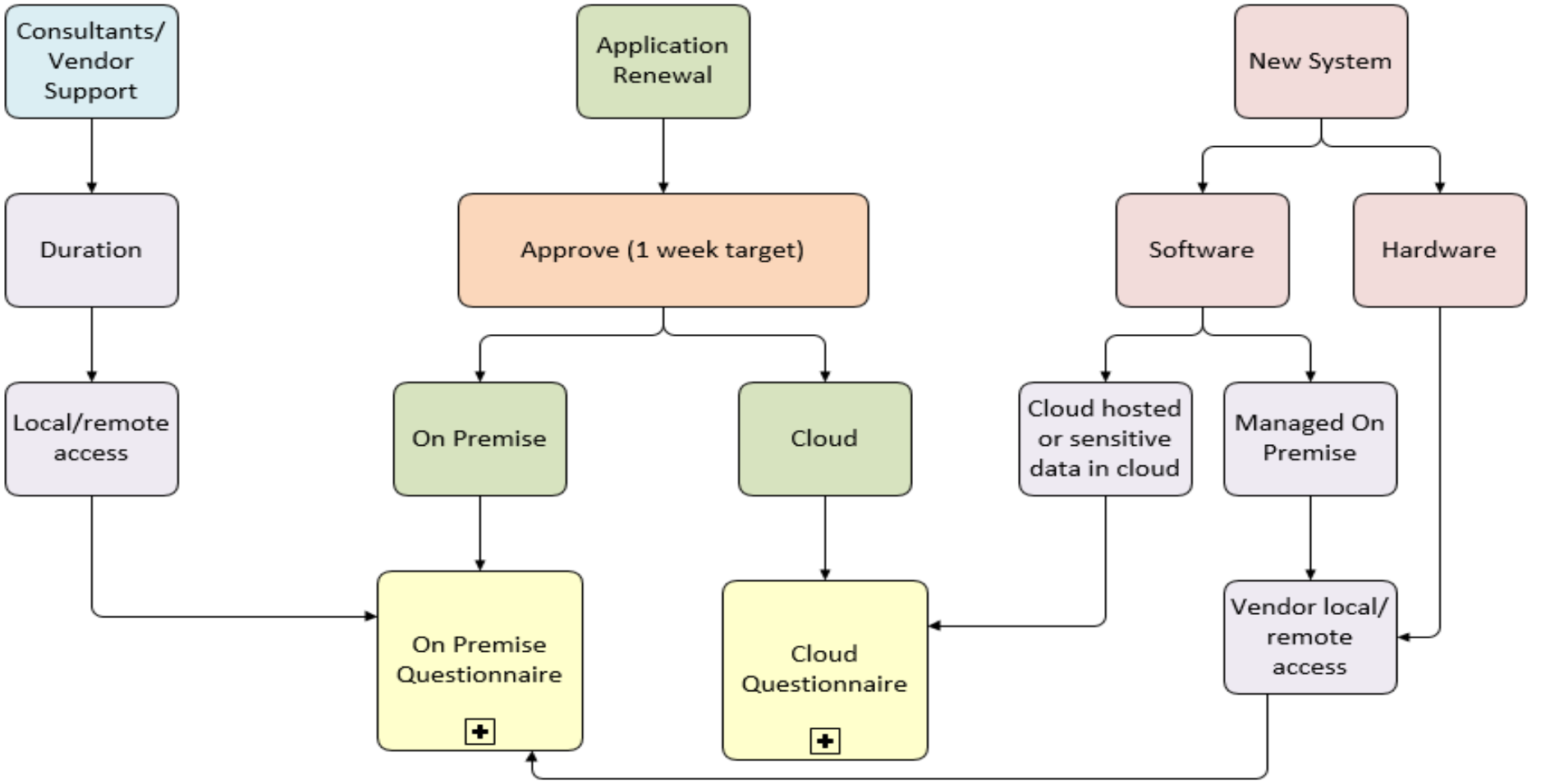
OR

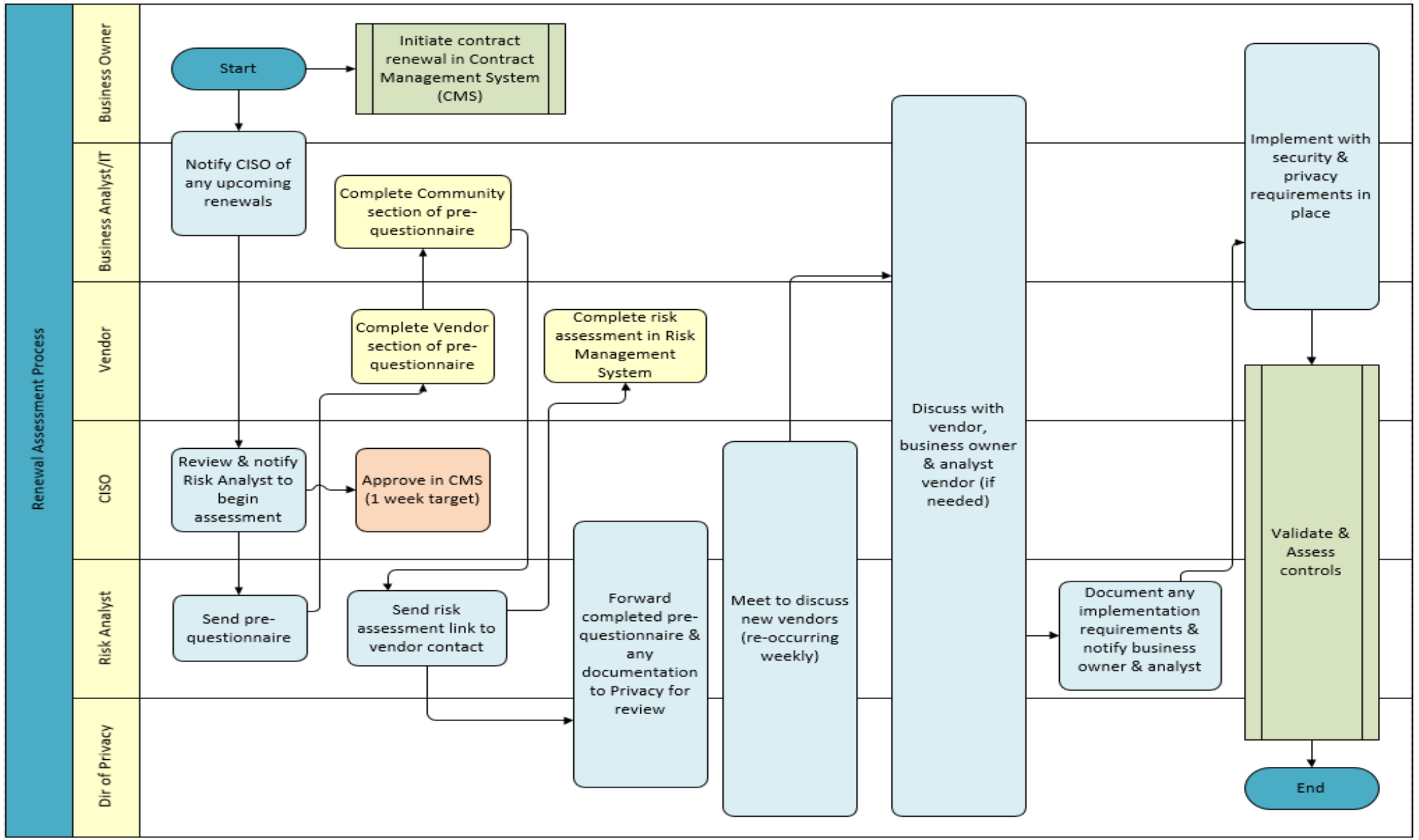
- Does the vendor acknowledge responsibility to protect Organization data for itself and subcontractors, continuing after the contract's termination?

"HOW" of Information Security Contract Review

Be preventive and detective

Vendor Risk Assessment Decision Tree





"HOW" of Information Security Contract Review

Be preventive and detective *continued*

"HOW" of Information Security – Risk Assessments

Preventive / Detective / Resolution

Information Security Compliance

- Categorize risks for acceptance, remediation, additional compensating controls
- Develop service level agreements for critical, high, medium, low
- Develop corrective action plans
- Develop metrics and trending on risks

"HOW" of Information Security – Risk Assessments

1. Identify and catalog your information assets
2. Identify threats
3. Identify vulnerabilities
4. Analyze internal controls
5. Determine the likelihood that an incident will occur
6. Assess the impact a threat would have
7. Prioritize the risks to your information security
8. Design controls
9. Document the results

"HOW" of Information Security – Risk Assessments

NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes & Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

"HOW" of Security - Trending

Phishing	Ransom ware	Outdated OS	Loss/ Theft	Data Loss	(IoT) Devices
Clicking on a link **may install malware**, like viruses, **spyware**, or **ransomware** on your device.	Malware that threatens to **publish the victim's data** or perpetually block access to it **unless a ransom is paid**.	Older versions of operating systems that are more vulnerable due to known security	Equipment Portable device Physical records	Insider, accidental, or intentional data loss	Attacks against smart medical **(IoT) devices** "Internet of Things."
2020 top scams – COVID relief payment and Centers Disease Control & Prevention (CDC) bulletin scams.	Maze was the top ransomware ploy in 2020, emulating security firm and gov't sites to infiltrate and steal data	Ongoing focus, with remediation ongoing with security patch support through 2022	Raley's lost 10,000 pharmacy patient records in 2018 due to stolen lap top. Now all encrypts laptops	"Firewalls" medical equipment networks to protect from patient data breaches	

“HOW” of Security - Trending

continued

Each year, data security trends change as we discover new cyber-attacks developing. As more of the world integrate advanced technology into their day-to-day lives, cybersecurity risks become a more dangerous and legitimate threat. Although the healthcare industry is advancing along with other industries, the healthcare industry's information is particularly sensitive. To keep this information safe, healthcare IT departments must be extra careful in keeping up with security trends to ensure their data is secure at all times.

"HOW" of Security - Trending

continued

Email Security

- Email phishing is a very common but problematic security breach that occurs across all industries. Even in the healthcare industry, phishing rates are up, as hackers rely on human oversight to access their information. Today, hackers are becoming smarter in their phishing by imitating reputable sites and finding unexpected moments to steal security info.

- To avoid falling into phishing traps, hospitals should invest in security software that flags and redirects any phishing email to keep them from employees. Hospitals should also have their employees change their passwords regularly to keep hackers from potentially breaking into their personal accounts.

"HOW" of Security - Trending

continued

Personal Devices

- It is usually a hospital's IT department's responsibility to promptly apply updates meant to repair software vulnerabilities found in operating system products. However, they cannot do this with products and services that the hospital does not own or that they don't know are present. This is more common today than ever because employees in the healthcare industry want to use their personal technology and software in their workflow as it may be more convenient at times.
- This results in consumer IT finding its way into the office, leaving company information vulnerable to hackers, as those in charge did not develop the products with a company-specific security focus. Examples of these products include free, easy-to-use applications, such as file-sharing technologies like Dropbox, Google Drive, and other Google Apps. A similar risk is posed when employees wish to connect their personal devices, like laptops and smartphones, with company software applications without going through the IT department.
- To mitigate the risk associated with shadow IT, IT departments teach hospital employees about the need to use only hospital-secured devices as part of their workday technology. They are also using shadow IT discovery tools to detect unapproved applications and quickly prevent dangerous ramifications. Finally, IT departments are teaming up with high-quality software developers to encrypt patient information when it comes to patient portal software.

"HOW" of Security - Trending

continued

Shadow IT

- One security risk that is becoming more common due to consumerism in the healthcare industry is shadow IT. Shadow IT refers to technology or software, like cloud services or SaaS applications, that run without the IT department's awareness or approval. These softwares are often installed by unwary employees who are simply looking for tech that is easier to use than the software approved by their IT department.

- While keeping patients connected to their physicians is an incredible and potentially life-saving benefit, the influx of devices brought into hospitals that have not undergone proper IT-sanctioned solutions poses several potential risks. These risks include data loss, exposure to software errors, and data protection compliance issues.

"HOW" of Security - Trending

continued

Automation and AI

- Now that automation and AI technology have become more accessible than ever, their value is being more readily explored by the healthcare industry to view the data at their hands fully. When noticing abnormal system behavior that might sign a data breach or other security event, machine learning technologies pose incredible value.

- Automated tech can analyze an abundance of information and data points within a matter of seconds, making it a valuable technology in finding outliers where an initial breach may have occurred. Therefore, hospitals that invest in AI stand to secure their hospital and patient information better. Additionally, they will have more details available to them regarding the accessed information. This can help them inform patients about the breach when necessary.

“HOW” of Security - Trending

continued

Blockchain Security

- Blockchain systems are used to record transactions using a lasting but efficient method known as “smart contracts”. These contracts keep the information throughout several databases. These systems embed contracts in a code that no entity can change. This could potentially make hospital transactions between parties more efficient and safe.

"HOW" of Security - Trending

Governance Risk & Compliance *(GRC)*

- GRC platforms are most commonly used by IT professionals, particularly Information Security professionals. They are usually used in large companies or companies that work with sensitive or proprietary data or heavily regulated.

- GRC products perform two main functions.
  - ❑First, they provide a framework for aligning IT strategy and processes with business goals and regulatory requirements.
  - ❑Then, they provide metrics for measuring how IT governance performs within that framework and facilitate compliance processes like audits and reporting.

Benefits of GRC Tools

continued

- Increase their value by providing preventative strategy
- Generate fast reporting so that decisions are made more swiftly and surely
- Detect exceptions to reduce damage as quickly as possible
- Automate detective controls for increased efficiently
- Reduce compliance costs going forward
- Get real-time alerts if/when regulations change
- Shorten audit cycles
- Business continuity in regards to compliance processes and compliance programs
- Configurable to meet the needs of your organization

"HOW" of Security - Tools

continued

- **Security Incident and Event Management (SIEM)** – Allow collecting logs from different assets. Correlation rules and threat intelligence allow the teams to shorten or prevent the time from incident to remediation.

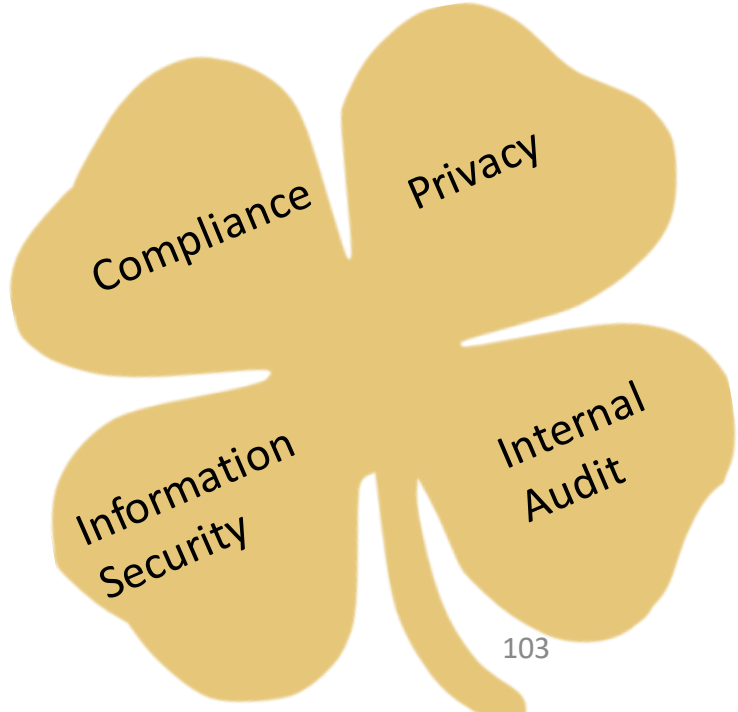
- **Vulnerability Management** – Scanners allow you to assess assets for vulnerabilities or lack of best practice controls.

- **Perimeter Assessment** – Several tools allow you to assess perimeter devices such as firewalls. The rules over time become stagnant or may not be following a best practice.

Compliance and IA Offices – Collaboration RESULTS
Utilize Internal Audit to Audit Key Areas – Compliance

Prevent, Detect, Response, Resolve / Recovery - 4 LEAF CLOVER

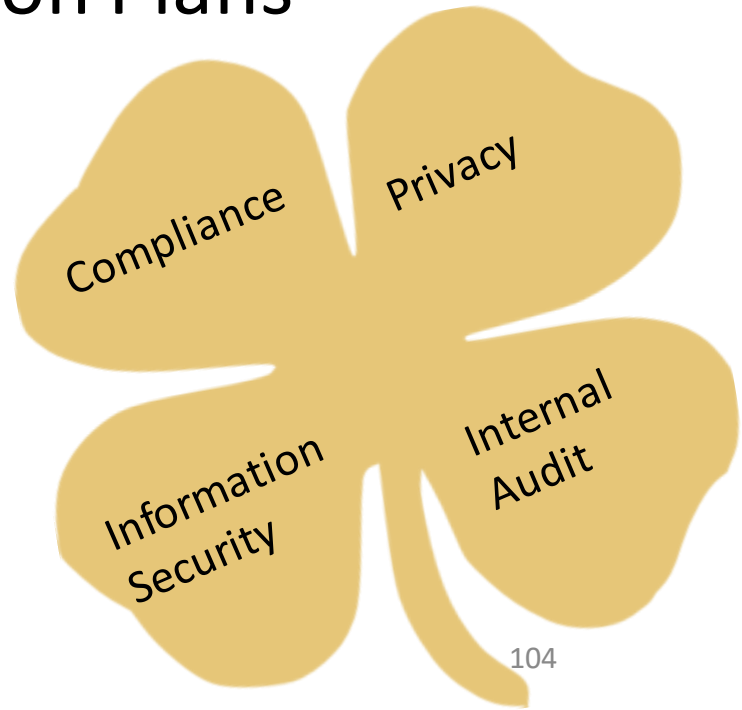
- OIG, CMS, Regulations, RAC, TPE (pre-payment), Revenue Integrity
- Inappropriate Billing, Compliance Office Findings, Compliance Working Committee (CWC), Findings from a previous review or audit.
- Contracts, FMV
- Business Continuity
- Crisis Planning, Risk
- Documentation, Education, Training, Mentoring
- Monitoring – Reactive, Active, Proactive, Testing
- Responsibilities, Accountabilities



Compliance and IA Offices – Collaboration RESULTS
Utilize Internal Audit to Audit Key Areas – Privacy

Prevent, Detect, Response, Resolve / Recovery - 4 LEAF CLOVER

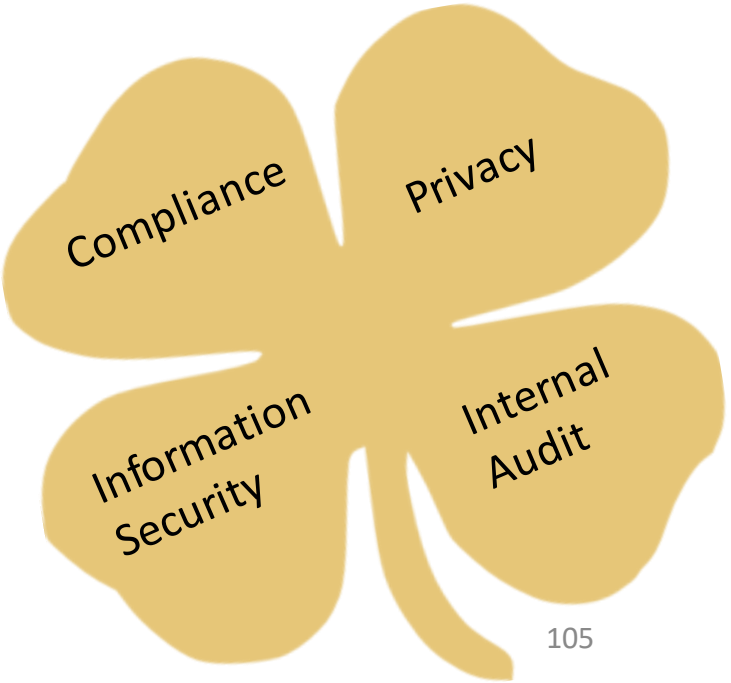
- HHS, the Office for Civil Rights ("OCR")
- Data Breach
- Consistent Documentation, Investigations, Action Plans
- Contracts
  - BAA – Business Associate Agreement
  - DUA – Data Use Agreement
- Monitoring – Reactive, Active, Proactive



Compliance and IA Offices – Collaboration RESULTS
Utilize Internal Audit to Audit Key Areas – Information Security

Prevent, Detect, Response, Resolve / Recovery - 4 LEAF CLOVER

- OCR, SSAE 18, SOC, PCI DSS
- NIST - Identify, Protect, Detect, Respond, Recover
- Phishing, Ransomware, Outdated OS, Loss/ Theft, Data Loss, (IoT) Devices
- Risk Assessments
- Change Controls
- Data Management / Data Governance
- Monitoring – Reactive, Active, Proactive
- Contracts
  - Third Party Risk Evaluation and Management
  - Remote Work



WRAP UP

Debra A. Muscio
Audit, Enterprise Risk Management, Privacy, Information Security,
Ethic and Compliance Professional
dmuscio71321@outlook.com