East Carolina University | Board of Trustees
Audit, ERM, Compliance, and Ethics Committee Meeting
November 10, 2016 | Agenda

I.	Approval of September 29, 2016 Minutes		Action
II.	Office of Internal Audit – Ms. Stacie Tronto		
	A.	Internal Audit Dashboard	Information
	B.	OSA Audits	Information
	C.	Cyber Security and Internal Audit	Information
III.	Cyber Security – Dr. Jack McCoy		Information
IV.	Enterprise Risk Management – Mr. Tim Wiseman		
	A.	Update of Activities	Information
	B.	Risk Appetite and Risk Tolerance	Information
V.	Research Compliance – Dr. Hiromi Sanders		Information
VI.	Other Business		
VII.	Closed Session		

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 10, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Kel Normann, Chair
Agenda Item	I.
Item Description	Approval of minutes – September 29, 2016
Comments	
Action Requested	Approval
Disposition	
Notes	

Back To Agenda

DRAFT

Minutes from ECU BOT Audit, Enterprise Risk Management, Compliance, and Ethics Committee
September 29, 2016
Murphy Center

The Audit, Enterprise Risk Management, Compliance, and Ethics Committee (formerly named and still sometimes referred to as "Audit Committee") of the ECU Board of Trustees met in regular session on September 29, 2016 at 8:15am in the Murphy Center on the campus of East Carolina University. Committee members present included Kel Normann (Chair), Vern Davenport, Bob Plybon, and Mark Copeland.

Other board members present included Kieran Shanahan, Edwin Clark, Deborah Davis, and Ryan Beeson.

Others present included Chancellor Cecil Staton, Phyllis Horns, Rick Niswander, James Hopf, Donna Payne, Chris Dyba, Michael Van Scott, Steve Duncan, Nick Benson, Dee Bowling, Tim Wiseman, Michelle Evans, Norma Epley, Hiromi Sanders, Holly West, Stacie Tronto, and Wayne Poole.

Kel Normann, Chair of the Committee, convened the meeting at 8:15AM. Mr. Normann read the conflict of interest provisions as required by the State Government Ethics Act. Mr. Normann asked if anyone would like to declare or report an actual or perceived conflict of interest. None were reported.

Mr. Normann asked for the approval of the minutes of the July 14, 2016 audit committee meeting.

Action Item: The minutes of the July 14, 2016 audit committee meeting were approved with no changes.

Mr. Tim Wiseman provided the **Enterprise Risk Management** (**ERM)** update.
Mr. Wiseman advised the committee that the interim regulation on Unmanned Aircraft Systems has been published and the review and approval process has been implemented and followed several times over the last two months.

Mr. Wiseman stated that he has provided ERM orientation to Chancellor Staton and will soon provide it to Chief of Staff Hopf.

Mr. Wiseman provided an overview of this year's risk survey process. He stated that the 2016-2017 top risks survey has been launched. Inputs for the University's risk register will include the results of this survey, interviews with academic deans and directors, input from the Chancellor's Executive Council, and input from the ERM Committee. Mr. Wiseman stated that once all inputs are received, the risk evaluation process will consider the probability, impact, and speed of onset of the various risk scenarios. Speed of onset is a new evaluation criteria for this year. Mr. Wiseman will keep the committee updated at subsequent meetings as the risk evaluation exercise progresses.

Dr. Hiromi Sanders presented the **Research Compliance Report**
Dr. Sanders provided an overview of the University's conflict of interest reporting process. She also provided a report on the University's conflict of interest reporting compliance for the 2015-2016 fiscal year.

Dr. Sanders advised the committee that there are two primary conflict of interest compliance requirements. First, all personnel involved in federally funded research (for example, research funded by Department of Defense, Department of Energy, National Institutes of Health, National Science Foundation, etc.) must disclose potential conflicts of interest annually. The University was 100% compliant – all 208 affected personnel submitted the required disclosures for the year. Second, pursuant to UNC system and ECU policies, all faculty and EHRA employees (regardless of their involvement in federally funded research) must submit conflict of interest disclosures. Dr. Sanders stated that 93% of the approximately 2,800 affected employees submitted the required disclosures for the year. Vice Chancellors Mitchelson and Horns are engaged with the applicable colleges and units to ensure the remaining personnel submit the required disclosures.

Back To Agenda

Dr. Sanders reported that she has coordinated with Human Resources to ensure that part-time personnel submit the required COI disclosures at the time of hire. Internal Audit will also be partnering with Dr. Sanders to review COI management plans and to review units where compliance has not been 100%. This is on the annual audit plan.

Mr. Copeland asked about the risks of non-compliance with COI reporting requirements. Dr. Sanders stated that the highest risk is related to the personnel engaged in federally funded research endeavors, as their non-compliance could result in loss of funding for the University. The risks of other personnel not complying include non-compliance with UNC and ECU policy, and the potential that conflicts of interest are unknown and therefore unmanaged.

Ms. Michelle Evans presented the **Health Sciences Compliance Report**
Ms. Evans updated the committee on the recent formation of the HIPAA Security Office within the Division of Health Sciences. Ms. Evans stated that HIPAA security compliance oversight was previously housed within ITCS, but has been moved because approximately 90% of the University's protected health information (PHI) that is subject to HIPAA is housed within the Division of Health Sciences.

Ms. Evans stated that in addition to herself, the HIPAA Security office is staffed by two HIPAA Security Specialists and an Administrative Support person. These professionals are responsible for assisting and advising the staff and management in clinical areas and other units with ensuring that the systems and processes in place are compliant with the requirements of the HIPAA Security rule. The need for these additional resources was pointed out by Internal Audit in previous years.

Mr. Davenport and other committee members stressed the importance of mitigating the risks associated with mobile devices. Ms. Evans concurred with this and advised that one of her highest priorities is coordinating with management and ITCS to get a University-wide mobile device policy in place as soon as possible. Ms. Evans stated that the majority of known breaches nationwide is a result of lost or stolen laptops that contain PHI related to research.

Ms. Stacie Tronto provided the **Internal Audit update**.
Ms. Tronto presented the FY 2017 Internal Audit Operating budget, along with the three prior years' budgets for the committee's review. Ms. Tronto discussed reasons for differences in the budgets, which include some one-time training funds for participation in a data analytics forum and the Tableau (analytics software) conference. Ms. Tronto stated that the office also had received one-time funds to hire a student intern. Internal Audit intends to treat the intern, who starts next month, as an entry-level professional auditor and allow her to learn about the internal audit profession by conducting projects from start to finish.

Action Item: The committee approved the annual budget for Internal Audit.

Ms. Tronto presented the Internal Audit dashboard for the fiscal year that ended June 30, 2016. Ms. Tronto highlighted the following metrics: Internal Audit completed 91% of the annual audit plan (the target is 80%). 78% of auditor hours were spent on direct audit and consulting activity (the target is 75%). Management completed 94% of the corrective actions for which Internal Audit performed a follow-up review. The target is 95%. Ms. Tronto advised the committee that significant progress has been made by management on the outstanding/incomplete items (most of which are related to Athletics camps), but that these need to be reviewed again.

Back To Agenda

Ms. Davis asked Ms. Tronto whether or not the risks related to Athletics Camps are an ongoing concern. Ms. Tronto stated that the University has made good progress and that the administrative support staff in Athletics had implemented good controls. However, some of the individual sport coaches had not fully complied with requirements for background checks, medical and liability forms, and formal reporting of external professional activities for pay. Ms. Tronto stated that Internal Audit will follow-up on these items again this year. Ms. Tronto and Mr. Wiseman stated that Athletics Camps-related risks to the University have been reduced significantly from what they were a few years ago.

Ms. Tronto briefed the committee on a recent presentation that she delivered to the Association of College and University Auditors (ACUA). The presentation was an overview of how data analytics is being used at ECU to review academic integrity and student athlete courses. Ms. Tronto stated that she has also been asked to present this information to UNC-GA, for potential implementation at other UNC system schools.

Ms. Tronto briefed the committee on some other training sessions that were part of the ACUA conference, including a session on "Audit Committee Engagement". Ms. Tronto stated that she was pleased because ECU's Audit Committee is already very engaged and its activities are consistent with the recommendations that were made by the ACUA presenters.

Mr. Copeland asked that Ms. Tronto include other Internal Audit staff members in the Audit Committee meetings when appropriate. Ms. Tronto agreed.

Mr. Plybon asked whether or not Ms. Tronto is still providing support to Elizabeth City State University. Ms. Tronto stated that the current agreement ends on December 31, 2016, and that it will not be renewed. She stated that ECSU asked for the agreement to be renewed, but she declined. Ms. Tronto will remain available to mentor the Chief Audit Officer at ECSU but that will be the extent of ECU's support in the area of Internal Audit after December 31.

Other Business
Mr. Normann asked if anyone had other business for the committee. No other business was brought forward by anyone in attendance.

Closed Session
At 9:00 AM, Mr. Copeland made a motion that the committee go into closed session in order to discuss items that are protected according to state statutes governing personnel information, criminal investigations, internal audit working papers, sensitive security information, and/or otherwise not considered a public record within the meaning of Chapter 132 of the North Carolina General Statutes. The motion was seconded and unanimously approved.

Return to Open Session
The Committee returned to open session and continued work on the agenda at 9:07 AM.

There being no further business, the Audit Committee meeting was adjourned at 9:07 AM.

_____

Respectfully submitted,
Wayne Poole
ECU Office of Internal Audit and Management Advisory Services

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 10, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Stacie Tronto, Director of Internal Audit
Agenda Item	II.
Item Description	Office of Internal Audit
Comments	
Action Requested	Information
Disposition	
Notes	A. Internal Audit Dashboard B. OSA Audits C. Cyber Security and Internal Audit

Back To Agenda

Internal Audit Dashboard - 1st Quarter FYE 2017

Completion of Audit Plan: Completed vs. Planned Audits

Status of Audit Plan	*Number of Audits*	*Percent of Total Plan*
Completed	12	**30%**
In Process	11	28%
Pending	17	43%
Total	**40**	**100%**

Goal = 80%

Staff Utilization: Direct vs. Indirect Hours

	With UPS	*Without UPS*
Direct Hours	69%	**75%**
Indirect Hours	31%	22%

Goal = 75%

Consultations

	Number	*% of Audit Plan*
Consultations	46	16%

Management's Corrective Actions

Observations by Division:	*Completed*	*Outstanding*	*% Complete*	*% Outstanding*	*Pending*
Academic Affairs	0	0	0%	0%	0
Administration and Finance	0	0	0%	0%	25
Athletics	0	0	0%	0%	4
Chancellor	0	0	0%	0%	0
Health Sciences	11	0	100%	0%	5
Research and Graduate Studies	0	0	0%	0%	0
Student Affairs	0	0	0%	0%	6
University Advancement	0	0	0%	0%	0
Total Observations	**11**	**0**			40
Total Percentages	**100%**	**0%**			

Goal = 95%

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 10, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Jack McCoy, Director of IT Security, ITCS
Agenda Item	III.
Item Description	Cyber Security
Comments	
Action Requested	Information
Disposition	
Notes	

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 10, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Tim Wiseman, Assistant Vice Chancellor, ERM
Agenda Item	IV.
Item Description	Enterprise Risk Management
Comments	
Action Requested	Information
Disposition	
Notes	A. Update of Activities B. Risk Appetite and Risk Tolerance

Back To Agenda

10/27/2016

INFORMATION PAPER

SUBJECT: Enterprise Risk Management (ERM) Update for the BOT-Audit, Risk Management, Compliance and Ethics Committee November 2016 Meeting

1. Purpose. To advise BOT-A committee members of significant ERM and Chief Risk Officer (CRO) activities from the past two months and those planned or anticipated for the next two months.

2. Action Recapitulation:

a. Significant ERM/CRO Activities from the Past Two Months:

- 2016-2017 ERM Top Risk Survey Launched
- University Youth Programs/Minors on Campus – Regulation Published
- Unmanned Aircraft Systems Interim Regulation Published
- Initial ERM Orientations with the Chancellor and Chief of Staff
- RIMS Regional Professional Development Workshop – Asheville
- RIMS ERM Conference – Atlanta
- University Youth Programs – Training Workshop (Nov)
- UNC System Insurance Workshop
- Re-Admissions Risk Case Reviews and University Behavioral Concerns Team Actions
- ERM Consultations and Inquiries – Various Departments
- Advising and Assisting University of Oklahoma with ERM Program Start
- Youth Programs Specialist Search Committee Actions & Hire

b. Significant ERM/CRO Activities Next Two Months:

- Top Risk Survey Results Analysis & Prioritization Exercise
- Quarterly Enterprise Risk Management Committee Meeting and Actions (Nov)
- Presentation of Top Risk Survey Results to University Leadership and BOT-ARMCE
- Prepare Prototype ERM Annual Report
- Continued Integration of Traditional Risk Management Functions into ERM Office
- Complete ERM Reference Manual/Handbook
- Re-Admissions Risk Case Reviews and University Behavioral Concerns Team Actions
- ERM Consultations/Research/Inquiries – Various Departments

3. Other: Article on Risk Appetite and Risk Tolerance Included for Thought/Discussion

ACTION OFFICER: Tim Wiseman
Assistant Vice Chancellor for ERM & Military Programs
Spilman Bldg, Room 214, 252-737-2803

Back To Agenda

The Institute of Risk Management

Risk Appetite & Tolerance Executive Summary

Crowe Horwath

Crowe Horwath Global Risk Consulting
Member Crowe Horwath International

irm

Leading the risk profession

Back To Agenda

Risk Appetite and Tolerance

Executive Summary

Supported by:

alarm
THE PUBLIC RISK MANAGEMENT ASSOCIATION

icsa. CHARTERED SECRETARIES

CIMA
Chartered Institute of Management Accountants

Chartered Institute of Internal Auditors

CIPFA The Chartered Institute of Public Finance & Accountancy

Charterhouse Risk Management

A guidance paper from
the Institute of Risk Management
September 2011

Back To Agenda

Foreword

irm

Leading the risk profession

Risk appetite today is a core consideration in any enterprise risk management approach.

As well as meeting the requirements imposed by corporate governance standards, organisations in all sectors are increasingly being asked by key stakeholders, including investors, analysts and the public, to express clearly the extent of their willingness to take risk in order to meet their strategic objectives.

The Institute of Risk Management, now in its 25th year, has a key role to play in establishing sound practices in this area and building consensus in what has, for too long, been a nebulous subject.

By providing practical advice on how to approach the development and implementation of a risk appetite framework we believe we will be helping boards and senior management teams both to manage their organisations better and to discharge their corporate governance responsibilities more effectively.

We are particularly pleased that a large number of professional bodies are supporting this work – risk is everyone's business and a common understanding and approach helps us work together to address this challenging area.

Alex Hindson
Chairman
The Institute of Risk Management

Back To Agenda

alarm
THE PUBLIC RISK MANAGEMENT ASSOCIATION

This paper will be helpful to senior managers in public service organisations who are trying to understand risk appetite in the context of their own strategic and operational decision making. In its recently published Core Competencies in Public Service Risk Management, Alarm identified the need to understand the organisation's risk appetite and risk tolerance, as part of the key function of identifying, analysing, evaluating and responding to risk. The 'questions for the boardroom', set out in this paper, could easily be translated into 'questions for the public organisation's senior executive committee' and as such may be of value to many Alarm members and their organisations.

Dr Lynn T Drennan
Chief Executive
Alarm, the public risk management association

Crowe Horwath
Crowe Horwath Global Risk Consulting
Member Crowe Horwath International

While the Financial Reporting Council has kick-started the debate on risk appetite and risk tolerance in the UK, it is a debate that resonates around the world. As an integrated global risk consulting business, I can testify to the fact that our clients are debating risk appetite. That is why we are pleased to support the work of the Institute of Risk Management in moving this debate forward. We look forward to actively engaging with IRM and others in promoting this thought-provoking document and turning risk appetite into a day-by-day reality for boards and risk management professionals around the world.

Larry Rieger
CEO, Crowe Horwath
Global Risk Consulting

Chartered Institute of Internal Auditors

The Chartered Institute of Internal Auditors welcomes this contribution from the Institute of Risk Management to the debate on risk appetite and risk tolerance. In theory, the idea of deciding how much risk of different types the organisation wishes to take and accept sounds easy. In practice, it is difficult and needs ongoing effort both from those responsible for governance in agreeing what is acceptable and from all levels of management in communicating how much risk they wish to take and in monitoring how much they are actually taking. Anything that stimulates debate on the practical challenges of risk management is to be welcomed.

Jackie Cain
Policy Director
Chartered Institute of Internal Auditors

CIPFA The Chartered Institute of Public Finance & Accountancy

CIPFA is pleased to endorse this work by IRM on risk appetite and tolerance which provides welcome leadership on a challenging subject for both the public and private sectors. We look forward to taking the debate further with our membership in pursuit of our commitment to sound financial management and good governance.

Diana Melville
Governance Adviser
Chartered Institute of Public Finance and Accountancy

Back To Agenda

CIMA
Chartered Institute of Management Accountants

All successful organisations need to be clear about their willingness to accept risk in pursuit of their goals. Armed with this clarity, boards and management can make meaningful decisions about what actions to take at all levels of the organisation and the extent to which they must deal with the associated risks. But defining and implementing risk appetite is work in progress for many. CIMA therefore warmly welcomes this new guidance from the Institute of Risk Management as a sound foundation for developing best practice on this critical topic.

Gillian Lees
Head of Corporate Governance
Chartered Institute of Management Accountants (CIMA)

icsa
CHARTERED SECRETARIES

This document is an important contribution to a key area of board activity and helpfully addresses one of the issues highlighted in the Financial Reporting Council's Guidance on Board Effectiveness. ICSA is pleased to support the work started here by the Institute of Risk Management, and looks forward to a well-informed debate and some useful conclusions.

Seamus Gillen
Director of Policy
Institute of Chartered Secretaries and Administrators (ICSA)


Charterhouse
Risk Management

This paper sends out a clear statement that the principle of risk appetite emanating from the board is the only effective way to initiate an ERM implementation. Charterhouse Risk Management is delighted to be associated with the launch of this paper after contributing to the consultation process. Our own experience with clients confirms that this approach is not only critical, but that the whole process must be undertaken with a practical rather than theoretical vigour. This is an essential ingredient of our delivery capability. References to 'appetite' and 'hunger' only reinforce the living nature of the required approach.

Neil Mockett
CTO
Charterhouse Risk Management

Back To Agenda

Introduction

The UK Corporate Governance Code states that *"the board is responsible for determining the nature and extent of the significant risks it is willing to take in achieving its strategic objectives."*

The intent of this document is to provide high level guidance to directors and senior executives on how to address this part of the Code, which essentially requires consideration of the subjects of 'risk appetite' and 'risk tolerance'.

This summary will tell you:

- what you need to know
- what you need to do, and
- where can you turn for more detailed guidance

It became apparent during the development of our paper that there is considerable interest in this topic in the public sector as well as the private sector, and also beyond the UK. So, while some specifics might differ, we feel that the underlying principles hold true for all sectors and all geographical locations.

We have prepared this guidance under the overall direction of a working group of the Institute of Risk Management. Our work has produced this executive summary, which is designed to provide an overview of the subject for general use, particularly by board members, and a more detailed version which is primarily designed to assist those whose task it is to advise boards on these matters. The detailed version of our guidance is available for free download from IRM's website*.

Following the financial collapse, precipitated by banks which we all assumed were outstanding at managing risk, which was after all their raison d'être, first the Walker Report, and then the review of Corporate Governance by the FRC highlighted the need for boards to re-evaluate just how good they are at managing risk. As a consequence Risk Appetite and Risk Tolerance are now on the agenda for all listed companies. Importantly, our work has shown that this interest extends outside the listed sector to organisations in all walks of life. But managing risk appetite represents a massive challenge: risk professionals have been divided as to how to determine risk appetite and there is precious little in terms of useful guidance.

* Risk Appetite and Tolerance – Guidance Paper available from www.theirm.org/publications/risk_appetite.html

Back To Agenda

We do not regard this guidance as the last word on the subject:

thinking will continue to develop and, if, as we hope, this booklet is superseded before too many reporting seasons come and go, then we will know that the concept of risk appetite is beginning to take root.

It is our view that risk appetite, correctly defined, approached and implemented, should be a fundamental business concept that could make a substantial difference to how businesses and organisations are run. We fully expect that the initial scepticism about risk appetite will be gradually replaced as boards and executive directors gain greater insight into its usefulness. We also anticipate that analysts will soon be asking chief executives, chairmen and finance directors about risk appetite. After all, this subject is at the heart of the organisation: risk-taking, whether private, public or third sector, whether large or small, is what managing an organisation is about. The approach of the new UK Corporate Governance Code represents an opportunity to place risk management, and in particular risk appetite, right at the centre of the debate on effective corporate governance and the role of the board in running organisations.

Richard Anderson
Deputy Chairman,
Institute of Risk Management

Members of the Working Group

Richard Anderson,
Deputy Chairman of IRM and Managing Director of Crowe Horwath Global Risk Consulting

Bill Aujla,
CRO at Etisalat

Gemma Clatworthy,
Senior risk consultant at Nationwide Building Society

Roger Garrini,
Audit manager at Selex Galileo

Paul Hopkin,
Director of IRM and technical director of AIRMIC

Steven Shackleford,
Senior academic in audit and risk management at Birmingham City University

John Summers,
Chief advisor – risk at Rio Tinto

Carolyn Williams,
Head of thought leadership at IRM

Back To Agenda

About IRM

The Institute of Risk Management (IRM) is the world's leading enterprise risk management education Institute. We are independent, well-respected advocates of the risk profession, owned by practising risk professionals. We provide qualifications, short courses and events at a range of levels from introductory to board level and support risk professionals by providing the skills and tools needed to deal with the demands of a constantly changing, sophisticated and challenging business environment. We operate internationally with members and students in over 90 countries, drawn from a variety of risk-related disciplines and a wide range of industries in the private, third and public sectors.

About the Author

Richard Anderson, the principal author of this booklet, is Deputy Chairman of IRM. Richard is also Managing Director of Crowe Horwath Global Risk Consulting in the UK. A Chartered Accountant, and formerly a partner at a big-4 practice, Richard has also run his own GRC practice for seven of the last ten years. Richard has been professionally involved with risk management since the mid-nineties and has broad industry sector experience. He wrote a report for the OECD on Corporate Risk Management in the banking sector in the UK, the USA and France. He is a regular speaker at conferences and contributes to many journals on risk management and governance issues.

"It is interesting, but not surprising, that whilst a significant proportion of financial organisations who have formally articulated a risk appetite statement have been compelled to do so by regulatory requirements, non-financial organisations have developed risk appetites in order to assist in the achievement of strategic goals."

Source: Jill Douglas,
Head of Risk,
Charterhouse Risk Management

Back To Agenda

Risk appetite – principles and approach

It is often said that no company can make a profit without taking a risk. The same is true for all organisations: no organisation, whether in the private, public or third sector can achieve its objectives without taking risk. The only question is how much risk do they need to take? And yet taking risks without consciously managing those risks can lead to the downfall of organisations. This is the challenge that has been highlighted by the latest UK Corporate Governance Code issued by the Financial Reporting Council in 2010.

The following key principles have underpinned our work on risk appetite:

1. Risk appetite can be **complex.** Excessive simplicity, while superficially attractive, leads to dangerous waters: far better to acknowledge the complexity and deal with it, rather than ignoring it.
2. Risk appetite needs to be **measurable.** Otherwise there is a risk that any statements become empty and vacuous. We are not promoting any individual measurement approach but fundamentally it is important that directors should understand how their performance drivers are impacted by risk. Shareholder value may be an appropriate starting point for some private organisations; stakeholder value or 'Economic Value Added' may be appropriate for others. We also anticipate more use of key risk and control metrics which should be readily available inside or from outside the organisation. Relevant and accurate data is vital for this process and we urge directors to ensure that there is the same level of **data governance** over these metrics as there would be over routine accounting data.

Back To Agenda

3 Risk appetite is **not a single, fixed concept.** There will be a range of appetites for different risks which need to align and these appetites may well vary over time: the temporal aspect of risk appetite is a key attribute to this whole development.

4 Risk appetite should be developed in the context of an organisation's **risk management capability**, which is a function of **risk capacity** and **risk management maturity**. Risk management remains an emerging discipline and some organisations, irrespective of size or complexity, do it much better than others. This is in part due to their risk management culture (a subset of the overall culture), partly due to their systems and processes, and partly due to the nature of their business. However, until an organisation has a clear view of both its risk capacity and its risk management maturity it cannot be clear as to what approach would work or how it should be implemented.

5 Risk appetite must take into account differing views at a **strategic, tactical** and **operational** level. In other words, while the UK Corporate Governance Code envisages a strategic view of risk appetite, in fact risk appetite needs to be addressed throughout the organisation for it to make any practical sense.

6 Risk appetite must be **integrated** with the control culture of the organisation. Our framework explores this by looking at both the **propensity to take risk** and the **propensity to exercise control.** The framework promotes the idea that the strategic level is proportionately more about risk taking than exercising control, while at the operational level the proportions are broadly reversed. Clearly the relative proportions will depend on the organisation itself, the nature of the risks it faces and the regulatory environment within which it operates.

Back To Agenda

Risk and control

We think that this dual focus on taking risk and exercising control is both innovative and critical to a proper understanding of risk appetite and risk tolerance. The innovation is not in looking at risk and control – all boards do that. The innovation is in looking at the interaction of risk and control as part of determining risk appetite. Proportionately more time is likely to be spent on risk taking at a strategic level than at an operational level, where the focus is more likely to be on the exercise of control. One word of caution though, we are not equating strategy with board level and operations with lower levels of the organisation.

A board will properly want to know that its operations are under control as much as it wants to oversee the development and implementation of strategy. In the detailed paper we have included a few suggestions as to how boards might like to consider these dual responsibilities. Above all, we are very much focused on the need to take risk as much as the traditional pre-occupation of many risk management programmes, which is the avoidance of harm.

Hungry for risk?

The word *"appetite"* brings connotations of food, hunger and satisfying one's needs. We think that this metaphor is not always helpful in understanding the phrase *"risk appetite"*. When those two words appear together we think it is more appropriate to think in terms of *'fight or flight'* responses to perceived risks. Most animals, including human beings, have a *'fight or flight'* response to risk. In humans this can be over-ruled by our cognitive processes. Our interpretation of risk appetite is that it represents a corporate version of exactly the same instincts and cognitive processes. However, since these instincts are not "hardwired" in our corporate "nervous and sensory" systems we use risk management as a surrogate.

Back To Agenda

Risk appetite and performance

Our view is that both risk appetite and risk tolerance are inextricably linked to performance over time. We believe that while risk appetite is about the pursuit of risk, risk tolerance is about what you can allow the organisation to deal with.

Organisations have to take some risks and they have to avoid others. The big question that all organisations have to ask themselves is: just what does successful performance look like? This question might be easier to answer for a listed company than for a government department, but can usefully be asked by boards in all sectors.

The illustrations on these pages show the relationship between risk appetite, tolerance and performance. Diagram 1 shows the expected direction of performance over the coming period. Diagram 2 illustrates the range of performance depending on whether risks (or opportunities) materialise. The remaining diagrams demonstrate the difference between:

- all the risks that the organisation might face (the *"risk universe"*- Diagram 3)
- those that, if push comes to shove, they might just be able to put up with (the *"risk tolerance"* - Diagram 4) and
- those risks that they actively wish to engage with (the *"risk appetite"* - Diagram 5).

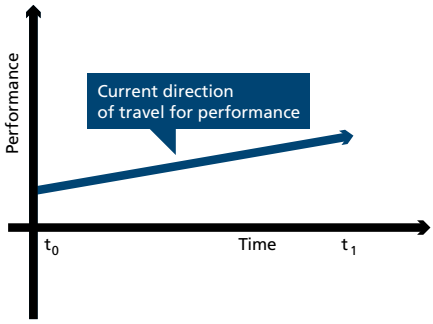

Diagram 1

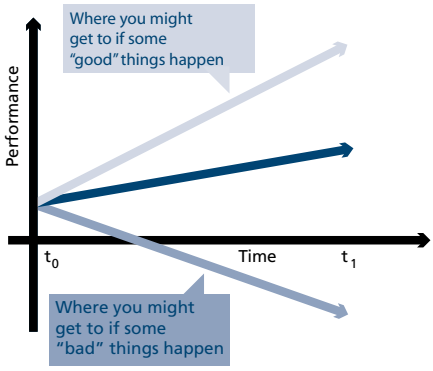

Diagram 2

Back To Agenda

We believe that the appetite will be smaller than the tolerance in the vast majority of cases, and that in turn will be smaller than the risk universe, which in any case will include *"unknown unknowns"*.

Risk tolerance can be expressed in terms of absolutes, for example *"we will not expose more than x% of our capital to losses in a certain line of business"* or *"we will not deal with certain types of customer"*.

Risk appetite, by contrast is about what the organisation does want to do and how it goes about it.

It therefore becomes the board's responsibility to define this all-important part of the risk management system and to ensure that the exercise of risk management throughout the organisation is consistent with that appetite, which needs to remain within the outer boundaries of the risk tolerance. Different boards, in different circumstances, will take different views on the relative importance of appetite and tolerance.

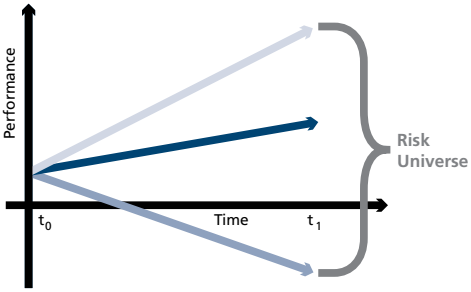

Diagram 3

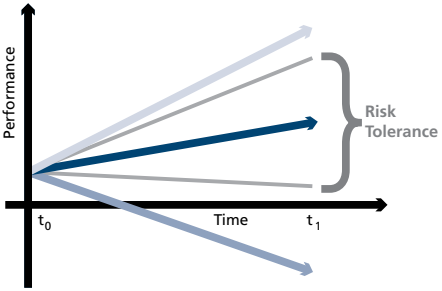

Diagram 4

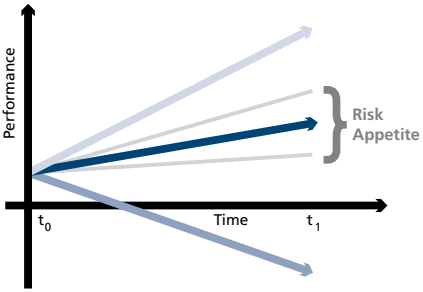

Diagram 5

Back To Agenda

Putting it into practice

We have sought to develop an approach to risk appetite that:

1. is theoretically sound (but the theory can quickly disappear into the background)
2. is practical and pragmatic: we do not want to create a bureaucracy, rather we are looking to help find solutions that can work for organisations of all shapes and sizes, and
3. will make a difference.

Boardroom debate - we suspect that in the early days particularly, a successful approach to reviewing risk appetite and risk tolerance in the boardroom will necessarily lead to some tensions. In other words we think that it should make a difference to the decisions that are made, otherwise it will diminish into a mere tick-box activity – and nobody needs any more of those in the boardroom. It is essential that the approach that we are setting out in the detailed guidance can and should be tailored to the needs and maturity of the organisation: it is not a one-size-fits-all approach.

Consultation - in our paper we have set out an illustrative process for the development of an approach to risk appetite. This includes appropriate consultation with those external and internal stakeholders, with whom the board believes it appropriate to consult on this matter. It also includes a review process by the board, or an appropriate committee of the board, and finally it includes a review process at the end of the cycle so that appropriate lessons can be learned.

Risk Committees - in his 2009 Review of Corporate Governance in UK Banks and Other Financial Industry Entities, Sir David Walker recommended that financial services organisations should make use of board risk committees. The Economic Affairs Committee of the House of Lords recently suggested that large organisations in other sectors should also consider creating such committees.* We think that the creation and monitoring of approaches to risk appetite and risk tolerance should be high on the agenda of these committees. In the detailed document, we have included a brief section on the role of the board or risk committee: we are suggesting that governance needs to be exercised over the framework at four key points: approval, measurement, monitoring and learning.

* House of Lords Economic Affairs Committee. (2011) Second Report - Auditors: Market concentration and their role

Flexibility - all of this needs to be carried out with the basic precept in mind that risk appetite can and will change over time (as, for example, the economy shifts from boom to bust, or as cash reserves fall). In other words, breaches of risk appetite may well reflect a need to reconsider the risk appetite part way through a reporting cycle as well as a more regular review on an annual cycle. Rapid changes in circumstances, for example as were witnessed during the financial crisis in 2008-9, might also indicate a need for an organisation to re-appraise its risk appetite or at least the application of its risk appetite framework. In a fast changing economic climate, it is especially important for firms to have not only a clearly defined strategy, but also a clearly articulated risk appetite framework so that they are able to react quickly to the challenges and opportunities presented during such times.

Back To Agenda

Five tests for risk appetite frameworks

In summary, there are five tests that Directors should apply in reviewing their organisation's risk appetite framework:

1. Do the managers making decisions understand the degree to which they (individually) are permitted to expose the organisation to the consequences of an event or situation? Any risk appetite framework needs to be practical, guiding managers to make risk-intelligent decisions.
2. Do the executives understand their aggregated and interlinked level of risk so they can determine whether it is acceptable or not?
3. Do the board and executive leadership understand the aggregated and interlinked level of risk for the organisation as a whole?
4. Are both managers and executives clear that risk appetite is not constant? It may change as the environment and business conditions change. Anything approved by the board must have some flexibility built in.
5. Are risk decisions made with full consideration of reward? The risk appetite framework needs to help managers and executives take an appropriate level of risk for the business, given the potential for reward.

We believe that by following the guidance set out in detail in our document, directors will be able to be confident that they can pass all of those five tests.

> *"The risk appetite statement is generally considered the hardest part of any Enterprise Risk Management implementation. However, without clearly defined, measurable tolerances the whole risk cycle and any risk framework is arguably at a halt."*
>
> Jill Douglas, Head of Risk, Charterhouse Risk Management

Back To Agenda

Questions for the boardroom

Below we set out some questions that we think boards may want to consider, as part of an iterative process over time, as they develop their approaches to risk appetite and which will enable them to remain at the forefront of the discussion. One clear outcome from our consultation exercise was that, despite the expected variation in views on the technical aspects of risk appetite, there was a common acceptance of these questions as a useful starting point for board discussion.

Background

1. What are the significant risks the board is willing to take? What are the significant risks the board is not willing to take?
2. What are the strategic objectives of the organisation? Are they clear? What is explicit and what is implicit in those objectives?
3. Is the board clear about the nature and extent of the significant risks it is willing to take in achieving its strategic objectives?
4. Does the board need to establish clearer governance over the risk appetite and tolerance of the organisation?
5. What steps has the board taken to ensure oversight over the management of the risks?

Back To Agenda

Designing a risk appetite

6 Has the board and management team reviewed the capabilities of the organisation to manage the risks that it faces?

7 What are the main features of the organisation's risk culture in terms of tone at the top? Governance? Competency? Decision making?

8 Does an understanding of risk permeate the organisation and its culture?

9 Is management incentivised for good risk management?

10 How much does the organisation spend on risk management each year? How much does it need to spend?

11 How mature is risk management in the organisation? Is the view consistent at differing levels of the organisation? Is the answer to these questions based on evidence or speculation?

Constructing a risk appetite

12 Does the organisation understand clearly why and how it engages with risks?

13 Is the organisation addressing all relevant risks or only those that can be captured in risk management processes?

14 Does the organisation have a framework for responding to risks?

Implementing a risk appetite

15 Who are the key external stakeholders and have sufficient soundings been taken of their views? Are those views dealt with appropriately in the final framework?

16 Has the organisation followed a robust approach to developing its risk appetite?

17 Did the risk appetite undergo appropriate approval processes, including at the board (or risk oversight committee)?

18 Is the risk appetite tailored and proportionate to the organisation?

19 What is the evidence that the organisation has implemented the risk appetite effectively?

Back To Agenda

Governing a risk appetite

20 Is the board satisfied with the arrangements for data governance pertaining to risk management data and information?

21 Has the board played an active part in the approval, measurement, monitoring and learning from the risk appetite process?

22 Does the board have, or does it need, a risk committee to, inter alia, oversee the development and monitoring of the risk appetite framework?

The journey is not over - final thoughts

23 What needs to change for next time round?

24 Does the organisation have sufficient and appropriate resources and systems?

25 What difference did the process make and how would we like it to have an impact next time round?

Back To Agenda

Crowe Horwath Global Risk Consulting
Contact: Richard Anderson
E richard.anderson@crowehorwathgrc.net

Charterhouse Risk Management Ltd
Contact: Andy Jenkinson
E andy.jenkinson@charterhouse-group.com

The Institute of Risk Management
6 Lloyd's Avenue
London EC3N 3AX

T +44(0)20 7709 9808
E enquiries@theirm.org
W www.theirm.org

Leading the risk profession

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 10, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Hiromi Sanders, Assistant Director, Office of Research Compliance Administration
Agenda Item	V.
Item Description	Research Compliance
Comments	
Action Requested	Information
Disposition	
Notes	

Back To Agenda

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 11, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Kel Normann, Committee Chair
Agenda Item	VI.
Item Description	Other Business
Comments	
Action Requested	
Disposition	
Notes	

Back To Agenda

HCCA HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

November 2016

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG

The Evolution of Healthcare Law and Compliance

an interview with Sara Kay Wheeler
2015–2016 SCCE/HCCA Board President
Partner, King & Spalding

See page 16

Back To Agenda

by Michelle C. Evans, MPA, CHC, CHPC and Kenneth A. DeVille, PhD, JD

HIPAA Privacy walkthroughs: The convergence of policy, education, and monitoring

» HIPAA Privacy "walkthroughs" are a proactive means of supporting the elements of an effective compliance program.

» Annual HIPAA walkthroughs are a potential means of identifying HIPAA violations and departures from regulations and can enhance training.

» Checklists should focus on the issues that are of greatest risk and regulatory concern for the particular clinic setting.

» Announced, "no fault" visits emphasize that walkthroughs are primarily a collaborative process.

» Post-walkthrough reports should include specific directions on regulatory requirements as well best practice recommendations.

Michelle C. Evans *(evansmi@ecu.edu) is Director, Office of Institutional Integrity/ECU HIPAA Security Officer and* ***Kenneth A. DeVille*** *(devillek@ecu.edu) is Chief Institutional Integrity Officer/HIPAA Privacy Officer at East Carolina University in Greenville, NC.*

Compliance departments and compliance officers often struggle with the multifaceted yet interlocking nature of their mission. They must understand and communicate the technical and sometimes nuanced requirements of applicable state and federal regulations. They must develop institution and practice-specific policies that support and promote compliance with those regulations. Institutional actors from leadership, middle management, and providers, to operational staff must be educated on these regulations and policies. But mere education on regulatory requirements and policies is insufficient.

The concrete, day-to-day implications of regulations and policies must be communicated to leadership, staff, and providers in such a way that they can be applied in real-life practice settings. Employees must understand how policies and regulations apply in *their* work settings. This mandate can be especially challenging in larger medical centers and practices in which there are frequently multiple, even dozens of, individual clinics, offices, and departments in which the range of work flows may present an array of different compliance challenges. Finally, the existence of policies and formal education on those policies is insufficient if employees do not follow established standards and guidance. Compliance officers are responsible for monitoring adherence to applicable policies across varying practice settings and taking corrective action where appropriate.[1] All of these goals must be addressed in a context of limited human and financial compliance resources.

Evans

DeVille

Regular HIPAA Privacy "walkthroughs," or "walking rounds," are a recognized means of effectively and efficiently protecting patients, supporting the elements of an effective compliance program, and helping

ensure adherence to HIPAA Privacy standards.[2] HIPAA Privacy walkthroughs require, in one sense, little more than a compliance officer physically touring clinics, offices, and departments and evaluating the various facilities and work sites, observing work flows, and talking to staff and providers. Ideally, the compliance reviewer will refer to a prepared checklist identifying key regulatory requirements, institutional policy directives, and recommended guidance and confirm by observation and interviews whether those concerns are addressed in everyday, real-life practice. HIPAA walkthroughs are a potential means of identifying HIPAA violations and departures from regulations. But a carefully structured and appropriately executed program can yield additional, and perhaps far more important, benefits that justify and exceed the resources required to conduct them on a regular basis.

First steps

Different covered entities will have a varying range of clinic and office settings, but the basic approach to initiating a walkthrough program is likely to look relatively similar. The authors serve an institution that treats patients in approximately 40 to 50 different clinics and practice settings. Walkthroughs may also be conducted in other non-clinic settings (e.g., financial service offices) that handle or process protected health information (PHI). But the essential features of a walkthrough program will be comparable in varying types of covered entities, even if the treatment settings are not.

The first step in initiating an ongoing walkthrough program should be the development of a checklist that will allow observation of staff and provide those who work in clinics with applicable regulatory, policy, and best practice guidance. The existence of the checklist is important early in the process, because it aids the Compliance or Privacy Office's review by focusing its goals and developing the most effective approach and strategies in conducting the actual walkthroughs. The development of a checklist as a first step will also allow others in the institution to understand more fully the nature of the exercise before it is launched.

The walkthrough checklist

The development of a checklist to guide the HIPAA walkthroughs is a relatively straightforward exercise. The checklist should contain practice-related references to regulatory requirements, key institutional policies, and specific concerns related to the organization and medical work of the clinics that will be reviewed. Although walkthroughs are designed primarily as a means of evaluating risks and compliance with privacy concerns, there is also an opportunity to include scrutiny of many important HIPAA Security risks as well. A HIPAA Compliance Office can easily produce its own "home grown" checklist from scratch, but there are numerous model checklists available from various organizations and many academic healthcare centers that can be adapted for use.

The checklist can be formatted in any number of ways. But, it is useful to create a spreadsheet that includes the specific privacy or security concern or activity, an indication whether or not the expectation is met by the clinic's organization and practices, and a space for observations and recommendations by the compliance reviewer for follow up, if any is required. The checklist developed and employed by the authors contains approximately 70 items for inspection and scrutiny, but a workable checklist could contain either more or less depending on need and/or the risks of the institution. The categories and subject matter should focus on the issues, practices, and requirements that are of greatest

risk and regulatory concern for the particular clinic settings.

General walkthrough checklist topic areas might include:

- Information regarding the HIPAA Privacy Office
- Notice of Privacy Practices
- Exchange of PHI
- Physical inspection
- Printers, copies, and fax machines
- Computers and workstations
- Personnel issues
- Privacy procedures and workflows
- Mail
- Disposal of PHI

The checklist should include an evaluation of specific clinical practices under each general subject area. For example, clinic employees should understand the role of the Privacy Office, know how to contact it for questions and concerns, and report privacy concerns to a manager or privacy officer as appropriate. Do employees know where to reference institutional HIPAA policies? Are employees correctly using authorization forms or directing PHI requests to the Release Office? Walkthroughs are also an excellent opportunity to evaluate the requirements related to the Notice of Privacy Practices (NPPs). Are NPPs posted in all clinical registration areas, and are English, Spanish, or other translated copies made available as needed? Do employees understand the contents of the NPP, and are NPPs collected and signed by patients as regulations require?

Walkthrough interviews present an opportunity to determine if employees understand the importance of exchanging only that PHI which is "minimally necessary." Visual observations and interviews help determine if employees protect patient privacy when interacting with patients and other staff. Telephone protocols and practices can be scrutinized. Physical inspection of the premises can provide broad insight into the protection of patient privacy and security. Is PHI kept in locked cabinets and behind secured doors when appropriate? How are whiteboards employed? Are employee desks cleared of PHI when unattended? Are printers, copiers, and fax machines in secure areas? Does the clinic have and follow appropriate protocols when using printers, copiers, fax machines, and receiving and sending mail? Important personnel and security issues might include the wearing of required ID badges, the appropriate use of passwords, and appropriate workstation practices. Is PHI disposed of in properly authorized ways? Is PHI placed in trash cans? Are locked shred bins available? Is electronic PHI properly destroyed? All such inquiries are important indicators of whether the clinic and its employees are appropriately protecting patient privacy.

Notifying leadership and middle management

After the development of the walkthrough checklist, we advise the early engagement of as many institutional contacts as possible in preparing a walkthrough program. Depending on the institutional structure, the board of directors, deans, department chairs, the director of Nursing, the head of Clinical Financial Services, and/or other individuals in leadership should be informed of the project and its goals. Notifying leadership may not be necessary, but rather it ensures that they are not taken by surprise by the activities. Moreover, early buy-in and support from leadership will help blunt potential resistance and enhance cooperation from middle management staff and providers when they learn of the walkthrough program. In large institutions, leadership can identify the appropriate middle management contacts who may likely offer beneficial suggestions that may enhance the effectiveness of the project. This may also

help build support and trust, or allay fears, when the walkthroughs are initiated. In addition, notification to middle management can help mute resistance and enhance cooperation with the walkthroughs at the clinic level, if any issues materialize. The ultimate goal, however, is that transparency and prior notice will encourage staff and providers to view the exercise as a collaborative learning process, rather than a top-down, confrontational investigation.

In some institutions, it might be advantageous to present the planned walkthrough program to select committees for their information and input. The preliminary plans for the project might be outlined for nursing leadership committees, physician practice committees, patient services committees, clinical services committees, or other groups that may play a central role in the operational aspects of the practice or institution.

At the authors' institution, the project was forecasted at the HIPAA steering committee. Although the HIPAA steering committee typically focuses on policy-level decisions and guidance, committee discussion of the walkthrough program provided a means of further publicizing the activity in the institution. As importantly, it helped illustrate for the committee how policy issues are translated to the operational setting and underscore the committee's understanding of the work of the Privacy compliance team.

Engaging staff at the clinic level

The authors recommend that the inaugural walkthrough visits are scheduled in advance and that the clinic personnel know specifically what practices will be scrutinized and evaluated. It is also advisable that the initial walkthrough visits are clearly designated as "no fault," educational exercises. There are obvious disadvantages to announced/no-fault walkthroughs. Such visits are clearly not true monitoring exercises. Clinic personnel, if they choose, have ample notice to use the checklist to prepare their clinics for the walkthrough and might revert to previous unwise and inappropriate practices once the walkthroughs have been completed. Our experience, however, suggests that this is not ordinarily the case.

Announced/no fault walkthroughs highlight the educational and collaborative component of the exercise.

But the advantages of the "no fault" approach, especially on the inaugural round of walkthroughs, are substantial. The goal of Privacy walkthroughs is not only monitoring; it is also communication and education. Announced/no fault walkthroughs highlight the educational and collaborative component of the exercise. One of the key advantages of a walkthrough is that clinic staff who have been exposed to only formal HIPAA education can now receive clinic-specific operational advice and insight. Clinic staff can see explicitly how the sometimes abstract and formal regulations and policies have a real-life, clinical component. Announced/no fault visits are more likely to enhance transparent communication between compliance staff and clinic staff and providers. Clinic staff are more forthcoming with answers and are more likely to ask questions when there is a collaborative trust established.

Walkthroughs: Round one

The actual walkthrough should consist of one or two Privacy compliance personnel touring a clinic facility with one or two clinic managers.

This approach allows very concrete discussions about the contents of the walkthrough checklist and potential brainstorming on operational alternatives that would better meet regulations and protect patient privacy. These conversations, which sometimes occur during the walkthrough itself, create the opportunity to discuss such issues as the finer points of incidental disclosures or the appropriate way to balance operational convenience against enhanced patient privacy protections. Brief post walkthrough meetings invariably provide additional opportunities for HIPAA questions, concerns, and ideas from clinic management staff, both related and unrelated to the content of the walkthrough itself. Also, these post walkthrough debriefings allow compliance personnel to reinforce the philosophy and tenor of the exercise.

Following the post-walkthrough debriefings, the Privacy Office should provide email or hardcopy reports to the nurse managers and patient access managers, or whoever directly participated in the process, to outline the areas of concern, if any. Telephonic, written, or onsite follow-up may be appropriate, depending on the nature of the issue. These summary reports should include recommendations on specific regulatory requirements (e.g., posting of institutional NPPs) and best practice recommendations that would decrease the risk of breaches of patient PHI (e.g., improved workstation placement). Failure to meet explicit regulatory provisions (e.g., failure to post the NPP) should always generate high-priority follow-up inquiries to ensure that the clinic makes the necessary changes in a timely fashion. In contrast, best practice recommendations may be viewed as an ideal goal and revisited in subsequent discussions and walkthroughs.

Annual walkthroughs: Round two and beyond

Walkthroughs *can* be designed as a type of one-time gap analysis in which institutional needs are assessed and remedied. However, we believe the walkthrough mechanism should be repeated at least annually in order to facilitate ongoing education and dialogue. Although launching the walkthrough program involves a significant expenditure of effort and compliance staff time in Year 1, subsequent iterations of the clinic visits will be less burdensome. Annual repeat walkthroughs as an established component of the Privacy Office's ongoing compliance program will allow the exploration of new issues and expose new staff and new workflows to the reviews.

> …best practice recommendations may be viewed as an ideal goal and revisited in subsequent discussions and walkthroughs.

Our experience with repeat annual walkthroughs has been gratifying. Most clinic managers were familiar with the process and the issues illustrated on the checklist from previous years. Fewer issues of concern were identified on follow-up visits, even a year hence.

As the Privacy Office's face-to-face contact with clinic employees has increased, so has its understanding and appreciation for wide range of clinical workflows, many of which are unique to a clinic or practice. This concrete understanding has aided the office in generating additional best practice recommendations, improved consultations,

and highlighted those situations that call for a new or revised institutional policy. The results of the HIPAA walkthroughs have also provided insight to the Privacy Office on the ways in which the new employee and annual HIPAA training can be enhanced and improved. Moreover, intimate knowledge of clinic workflows, gained from the walkthrough experience, has helped Privacy Office staff understand and unravel potential violation issues entirely unrelated to the walkthrough program. Many of the clinical staff recognized the compliance reviewers. The familiarity with the compliance staff, born of the walkthrough reviews, has led to many inquiries throughout the year to the Privacy Office, queries that may not have been made otherwise. Compliance officers everywhere seek to make all employees part of the compliance team—to make compliance everyone's business. Walkthrough programs can advance that goal.

It may be useful to escalate the scrutiny of the reviews as a walkthrough program evolves from year to year. For example, the walkthroughs conducted in Year 2 of the process could be scheduled for a specific month of the year—but conducted without notice. In Year 3 and beyond, walkthroughs might be conducted without notice at varying times of the year.

Once established, the walkthrough process might evolve in other ways as well. For example, walkthroughs might be conducted anonymously and without the presence of the clinic's clinic manager, nurse manager, or patient access services manager accompanying the compliance officer on his/her review. Such approaches are obviously more likely to present a more accurate picture of the clinic's typical operations and actual employee practices, because they do not allow the staff an opportunity to prepare the clinic for the visit. Walkthroughs could be conducted during different times of the day, including after office hours when staff have left the clinic and their workstations. The "no fault" spirit of the walkthroughs might be phased out as well as the program becomes institutionalized. Compliance reviews could cite individuals or clinics that put the privacy and security of patient information seriously at risk and violate institutional policy or applicable regulations. Completed checklists, results of the walkthrough, and recommendations from the compliance reviewers could be shared with a broader audience (i.e., middle management or leadership).

On one hand, these variations on the initial approach of the walkthroughs would increase their efficacy as a monitoring tool. In this respect, such changes would be beneficial and serve one goal of an effective compliance program. On the other hand, increased monitoring and the punitive character of the program would likely undermine the walkthrough's value as a collaborative exercise in which clinic staff and providers in the field work closely with the Privacy Office to develop effective procedures, processes, and practices to protect patient privacy. The more punitive the program, the less likely it will be to promote openness and cooperation. This unfortunate reality represents a delicate balance, the resolution of which should be made on an institution-by-institution basis. In the end, a Privacy compliance officer may have other effective ways to monitor employee behavior and, therefore, feel free to retain the walkthrough as an opportunity to meet staff as partners in a collaborative exercise to do the right thing and protect patient privacy.

1. DHHS, Office of Inspector General: "Elements of an Effective Compliance Program" in OIG Compliance Program for Individual and Small Group Physician Practices. 65 (194) F.R. 59434, October 5, 2000. Available at http://1.usa.gov/1np3hDY
2. Debbie Troklus and Greg Warner: *Compliance 101*, Third Edition (HCCA 2011), p. 66.

East Carolina University
Board of Trustees
Audit, ERM, Compliance and Ethics Committee
November 11, 2016

Session	Audit, ERM, Compliance & Ethics Committee
Responsible Person	Kel Normann, Committee Chair
Agenda Item	VII.
Item Description	Closed Session
Comments	
Action Requested	
Disposition	
Notes	

Back To Agenda