RISK & COMPLIANCE

Luke Deavenport & Andrew Hettick

Sprinting to the Future with Agile Auditing

KEYS CONFERENCE

1

DISCLAIMER

- **This presentation is for information only.**
  Evaluate risks before acting based on ideas from this presentation.
- **This presentation contains the opinions of the presenters.**
  Opinions may not reflect the opinions of Tandem.
- **This presentation is proprietary.**
  Unauthorized release of this information is prohibited.

2

Luke Deavenport

CISA, CISSP, SSCP

Audit & Security Consultant

Andrew Hettick

CISA, CISSP, SSCP

Information Security Officer

3

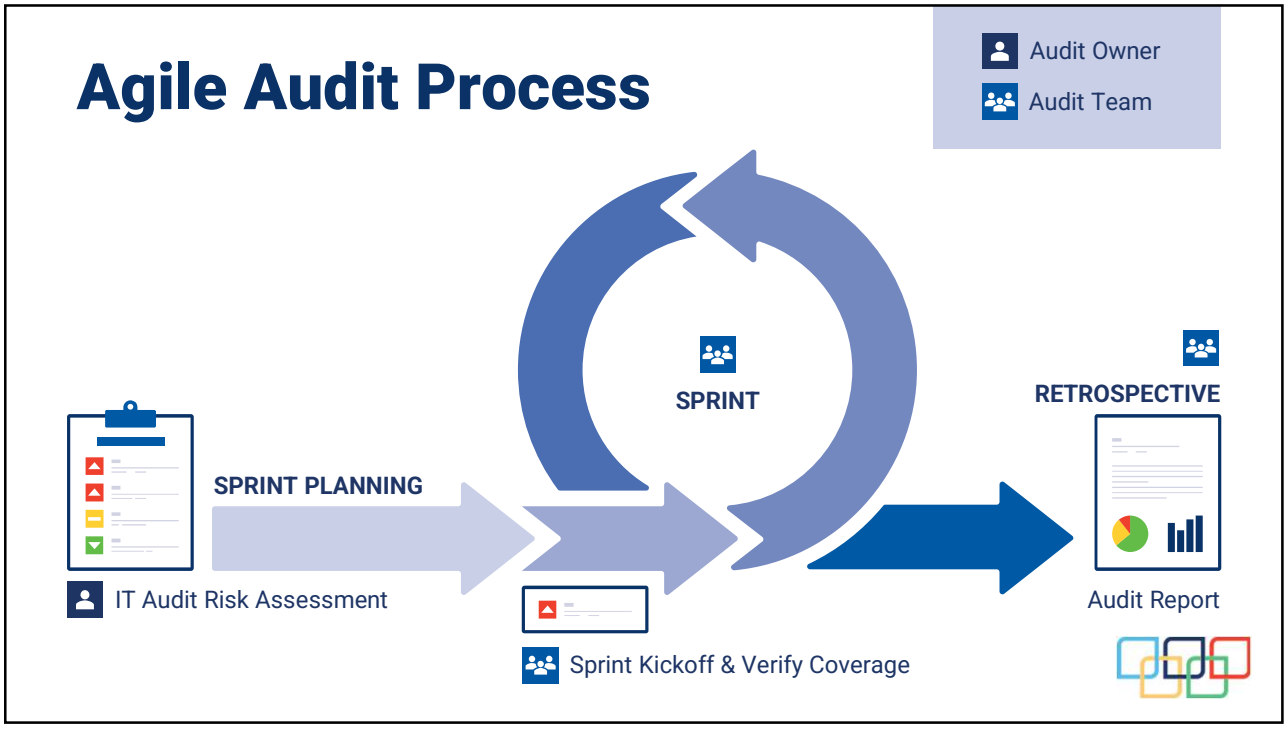
Agenda

1. Defining the Agile Audit Process
2. Agile Auditing Benefits
3. IT Audit Risk Assessment
4. Hands-on Activity
5. Agile Auditing Details

4

Defining the Agile Audit Process

5



6

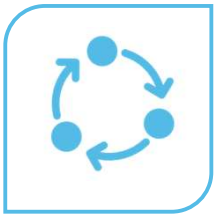
Are any of you doing agile audits?

7

Agile Auditing Benefits

8

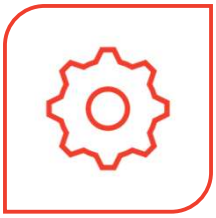
Agile Auditing Benefits



Multiple Reviews of High-Risk Areas

Audit New Controls Sooner

Distributes Audit Burden



Verify Finding Fixes Quickly

9

IT Audit Risk Assessment

10

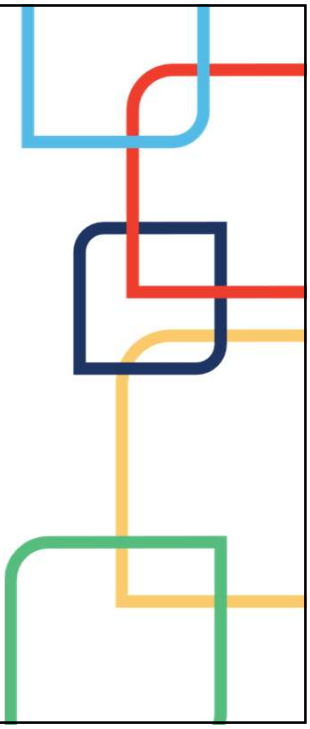
Purpose

IT Audit Risk Assessment

1. Identifies areas of most concern
2. Determines best use of audit resources
3. Helps determine if agile auditing is beneficial for you

11

Why did IT Audit Risk Assessments become more well known?



12

Background

IT Audit Risk Assessment

InTREx includes a request list item for an IT Audit Risk Assessment

InTREx Information Technology Risk Examination

Review items relating to internal or external IT audit, such as:

- Examination reports and workpapers
- Pre-examination memoranda and file correspondence
- IT audit charter and policy
- IT audit schedule
- IT audit risk assessment
- Cybersecurity self-assessments
- Internal and external IT audit reports

13

Risk Assessment Differences

IT Audit Risk Assessment

Information Security Risk Assessment	IT Audit Risk Assessment
Analyze threats to your organization	Determine frequency to audit each area
Controls are applied to mitigate those risks	Validate the effectiveness of applied controls

14

Create Your Own IT Audit Risk Assessment

15

Handout

IT Audit Risk Assessment

- Fill in the Frequency for each criticality level

Criticality	Definition	Frequency
Insignificant	A deficiency in this area has the potential to cause **negligible** adverse effects on the organization.	Situationally Based Only
Low	A deficiency in this area has the potential to cause **limited** adverse effects on the organization.	
Medium	A deficiency in this area has the potential to cause **serious** adverse effects on the organization.	
High	A deficiency in this area has the potential to cause **severe** adverse effects on the organization.	
Extreme	A deficiency in this area has the potential to cause **catastrophic** adverse effects on the organization.	

16

Handout

IT Audit Risk Assessment

- Example

Criticality	Definition	Frequency
Insignificant	A deficiency in this area has the potential to cause **negligible** adverse effects on the organization.	Situationally Based Only
Low	A deficiency in this area has the potential to cause **limited** adverse effects on the organization.	18 - 24 Months
Medium	A deficiency in this area has the potential to cause **serious** adverse effects on the organization.	12 Months
High	A deficiency in this area has the potential to cause **severe** adverse effects on the organization.	6 Months
Extreme	A deficiency in this area has the potential to cause **catastrophic** adverse effects on the organization.	3 Months

17

Handout

IT Audit Risk Assessment

- Fill in the Criticality ratings
- Medium is a good default

Audit Area	Criticality
IT Infrastructure Management	
IT Audit Independence	
Business Continuity Planning	
Cyber Incident Response	
IT Oversight, Strategy & Policy	
IT Staffing, Security Training & Company Culture	
IT Risk Management & Risk Assessment	
Vendor Management	
Access & Data Management	
Physical Inspections	
Cyber Monitoring, Alerting & Review	
External Vulnerability Scanning	
Internal Vulnerability Scanning	

18

Handout

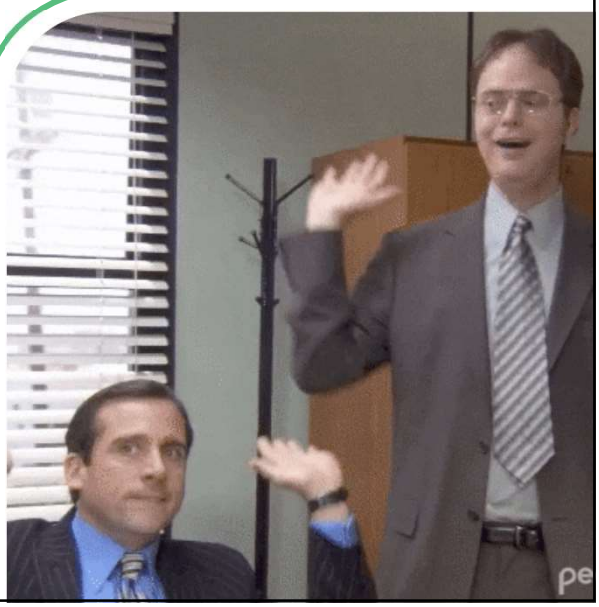
IT Audit Risk Assessment

- Example

Audit Area	Criticality
IT Infrastructure Management	Medium
IT Audit Independence	Low
Business Continuity Planning	Medium
Cyber Incident Response	Medium
IT Oversight, Strategy & Policy	Medium
IT Staffing, Security Training & Company Culture	Insignificant
IT Risk Management & Risk Assessment	Medium
Vendor Management	Medium
Access & Data Management	High
Physical Inspections	Low
Cyber Monitoring, Alerting & Review	Medium
External Vulnerability Scanning	Extreme
Internal Vulnerability Scanning	High

19

You now have your own IT Audit Risk Assessment!



20

IT Audit Schedule

21

IT Audit Schedule

Practical Tips

- Use the IT Audit Risk Assessment document
- Assign highest criticality areas first
- Work through less critical areas
- Ensure number of sprints matches frequency

22

Handout

IT Audit Schedule

- Fill in the Target Sprint section

Audit Area	Criticality	Target Sprint
IT Infrastructure Management	Medium	
IT Audit Independence	Low	
Business Continuity Planning	Medium	
Cyber Incident Response	Medium	
IT Oversight, Strategy & Policy	Medium	
IT Staffing, Security Training & Company Culture	Insignificant	
IT Risk Management & Risk Assessment	Medium	
Vendor Management	Medium	
Access & Data Management	High	
Physical Inspections	Low	
Cyber Monitoring, Alerting & Review	Medium	
External Vulnerability Scanning	Extreme	
Internal Vulnerability Scanning	High	

23

Handout

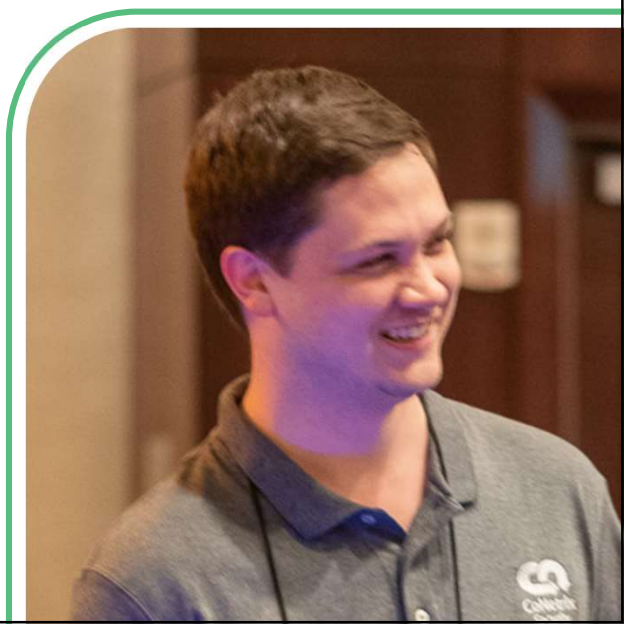
IT Audit Schedule

- Example

Audit Area	Criticality	Target Sprint
IT Infrastructure Management	Medium	Q2
IT Audit Independence	Low	Not this year
Business Continuity Planning	Medium	Q3
Cyber Incident Response	Medium	Q4
IT Oversight, Strategy & Policy	Medium	Q1
IT Staffing, Security Training & Company Culture	Insignificant	Not this year
IT Risk Management & Risk Assessment	Medium	Q2
Vendor Management	Medium	Q3
Access & Data Management	High	Q2, Q4
Physical Inspections	Low	Q4
Cyber Monitoring, Alerting & Review	Medium	Q1
External Vulnerability Scanning	Extreme	All
Internal Vulnerability Scanning	High	Q1, Q3

24

You now have your own IT Audit Risk Assessment and schedule!



25

"I can't change the direction of the wind, but I can adjust my sails to always reach my destination."

Jimmy Dean

26

Agile Auditing Details

27

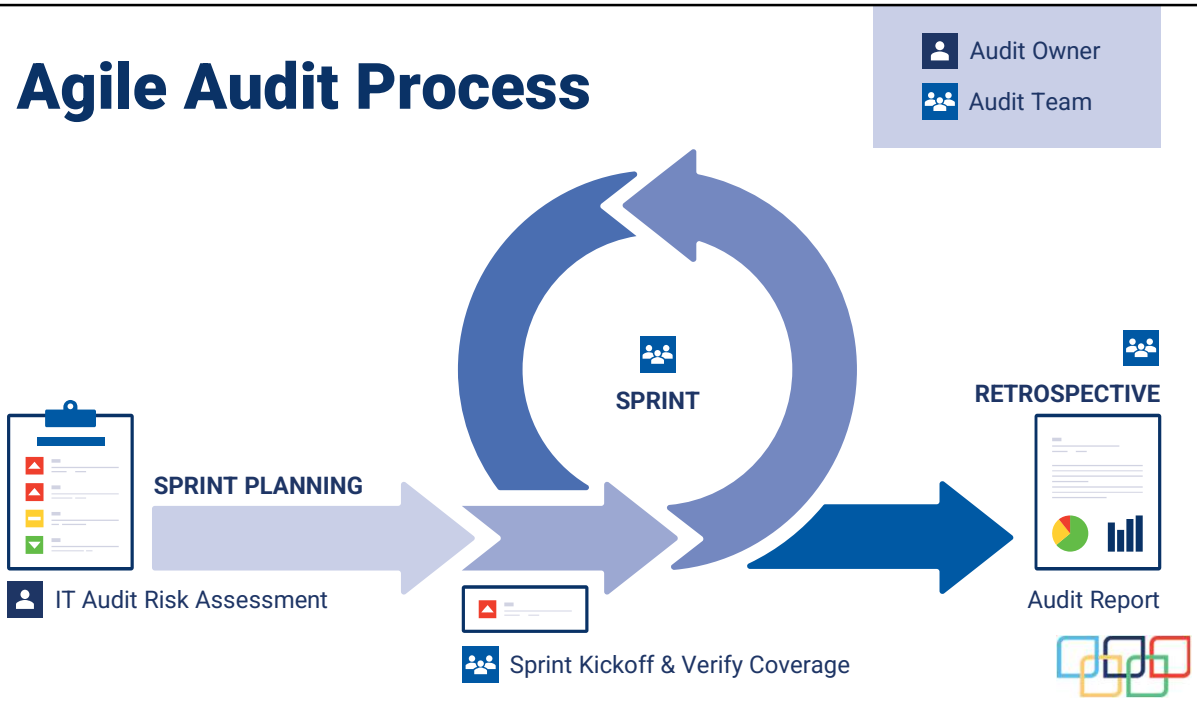
Audit Differences

Agile Audit

Traditional IT Audit	Agile IT Audit
Annual	Quarterly
Consistent scope	Adjust the scope

28

Agile Audit Process



29

Kick-Off Meeting

Agile Audit

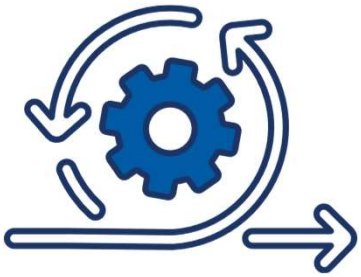
- Review the IT Audit Risk Assessment
- Confirm the scope
- Create the Request List Items
- Schedule the following, as needed:
  - Interview times
  - Data collection
  - Onsite physical inspection

30

Sprint!

Agile Audit

- Conduct the audit
  - Review scan results
  - Auditor reviews documentation provided
  - Interviews
  - Supplemental documents may be requested
  - Exit meeting
- Receive the report along with supplemental documentation



31

Sprinting Tips

Agile Audit

- Cover the critical and high areas first.
- Use extra time to dig deeper in the audited areas.
- Bring up areas of concern regularly.
- Keep the board informed.

32

Retrospective Meeting

Agile Audit

- Discuss the audit report
- Review the items completed
- Adjust the future sprints

33

Annual Work Papers

Agile Audit

- Annual deliverables of the content audited from the previous 4 quarters
- Summary of each quarter
- Report for board and examiners
- Audit rating

34

Key Takeaways

1. Better understanding on agile auditing concept
2. Leaving with your own IT Audit Risk Assessment
3. Equipped to decide if agile auditing is good for you

35

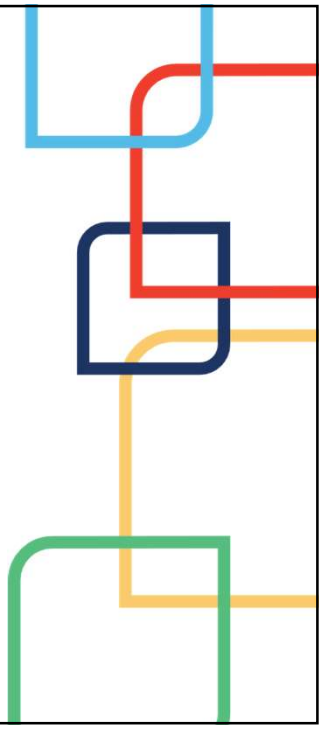
Other Resources

Agile Auditing Booklet

https://conetrix.com/agile-audit

36

Questions?



37

"If everyone is moving forward together, then success takes care of itself."

Henry Ford

38

THANKS FOR JOINING!

Sprinting to the Future with Agile Auditing

Luke Deavenport & Andrew Hettick

KEYS CONFERENCE

39