



# The Evolution of the IT Risk Assessment

March 22<sup>nd</sup>, 2017

- This presentation will last about 45 minutes.
- Today's presentation slides can be downloaded by going to <http://www.wolfpacsolutions.com/2017-webinar-archive> . Please note, not all slides will be included in the posted presentation as some of this session will consist of a live demonstration.
- You have two options for audio today. You may dial in by phone or listen through your computer.
- We will have time for Q & A at the end of the presentation. Submit your questions by using the “questions box” located on the webinar’s control panel.

## **Manuel Centeio**

WolfPAC Development

Phone: 617-261-8168

Email: [mcenteio@wolfandco.com](mailto:mcenteio@wolfandco.com)

- Recap of Last Webinar
- IT 4.0 Risk Assessments
  - Information flow
  - Methodology (calculations vs determination)
- IT 4.0 Reports / Report Writer
- Q & A



Administration Risk Management Risk Plans Risk Analytics Help & Support Log Out

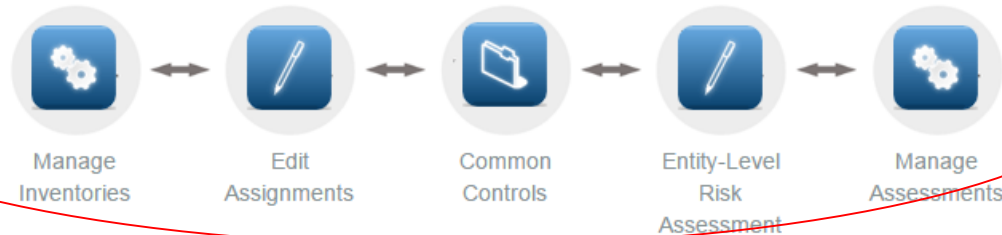
Home Risk Management Information Technology Risk Assessment (Beta)

### Welcome to the WolfPAC Information Technology Risk Assessment

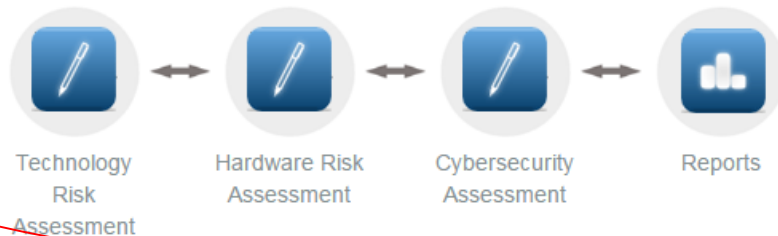
An ongoing IT Risk Assessment is fundamental to the development, implement and maintenance of an effective and comprehensive information security program. An IT Risk Assessment will identify where the organization will gain the most value from resources dedicated to the protection of information assets and will also provide a schedule to monitor the implemented information security controls.

- IT Risk Assessment Methodology
- IT User Guide
- FFIEC Cybersecurity Assessment Tool User Guide
- WolfPAC Cybersecurity Assessment Tool User Guide

### Administrative Tasks



### Information Technology Assessment



Streamlined Administrator and User capabilities  
Role Based Access

## A Consistent Five(5) Step Process.....

- ✓ **First Step: Answer the Questions** (identifies threats + threat impacts are calculated)
- ✓ **Second Step: Complete Threat Assessment** (identifies applicable controls, set threat likelihood, calculate Inherent risk)
- ✓ **Third Step: Select Controls** (check applicable controls)
- ✓ **Fourth Step: Complete Controls Assessment** (define control environment rating per threat)
- ✓ **Fifth Step: Review Assessment Results**

- Inherent Risk will be calculated using the table provided in NIST SP 800-30 Appendix I (Table I-2). See table below for additional details
- Example on slide 8 demonstrates the use of Inherent risk assessment scale table

Inherent Risk Assessment Scale Table					
Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

- In the example below considering the highest impact and likelihood score the system calculated inherent risk will be 'Very High'

(A) Threat	(B) Likelihood	(C) Calculated Impact Score	(D) Inherent Risk Analysis per Threat	(E) Inherent Risk for technology (one overall score)
Threat	Determined by user	Highest risk level from CIA	NIST SP-800-30 Appendix I table I-2	Highest score in column D
Unauthorized access to the system and/or data	Very High	Very High	Very High	Very High
Customer does not implement security settings	High		Very High	
Customer does not implement security settings	Moderate		High	
Third party connections are insecure	Low		Moderate	
Unauthorized change to system	Very Low		Low	



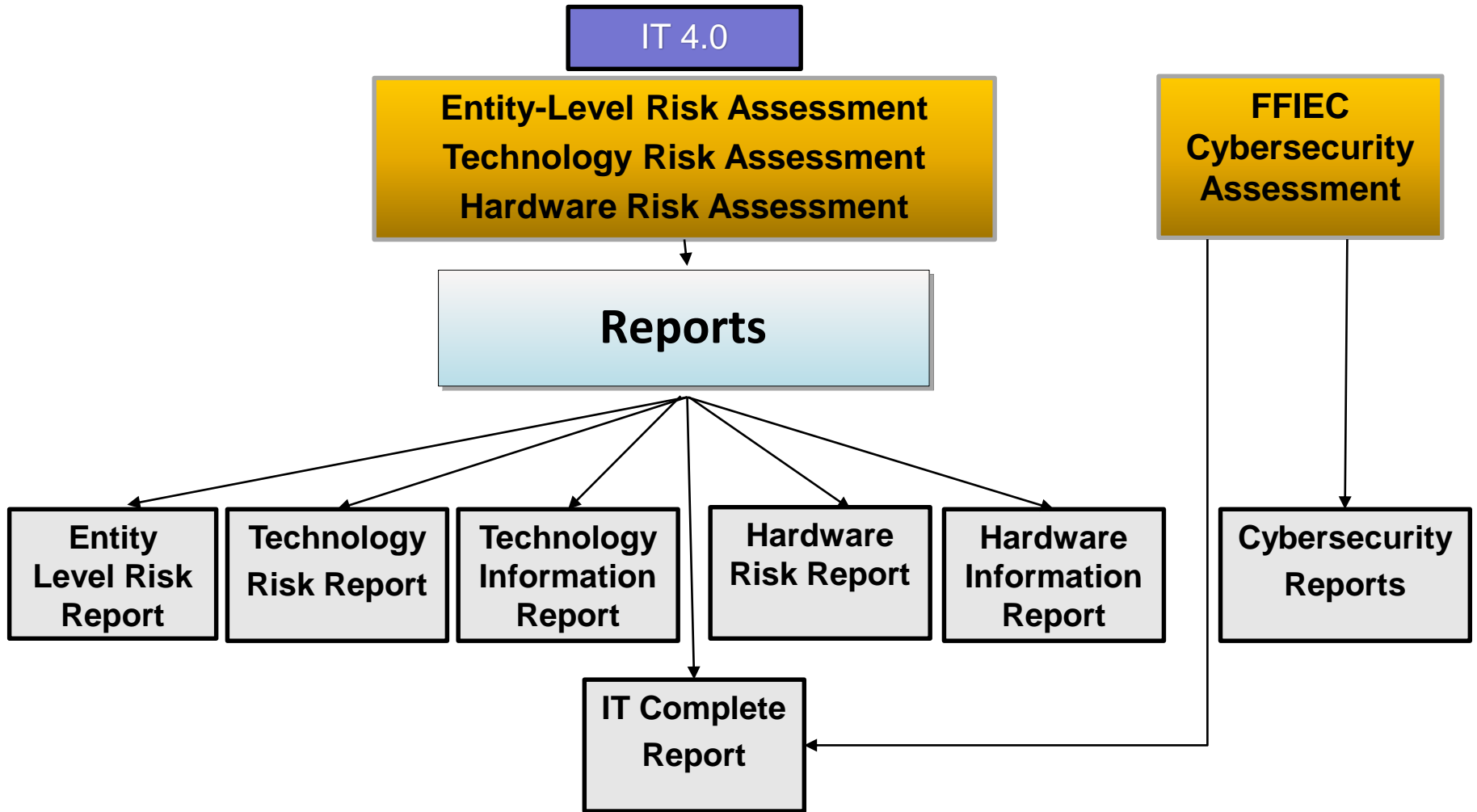
- Control environment score values will be based on OCC Bulletin from 2015-48
- Control environment rating will be assigned to each individual threat by end users

Control Environment Score (from OCC Bulletin 2015-48)	Effect on Residual Risk
Strong	Reduces IR value by 2 levels (i.e. Very High = Moderate)
Satisfactory	Reduces IR value by 1 (i.e. Very High = High)
Insufficient	No effect
Weak	No effect

- Residual risk will be assigned based on the calculated inherent risk and control environment rating using the table below.

Residual Risk Assessment Scale Table					
Control Environment Score	Inherent Risk Score				
	Very Low	Low	Moderate	High	Very High
Weak	Very Low	Low	Moderate	High	Very High
Insufficient	Very Low	Low	Moderate	High	Very High
Satisfactory	Very Low	Very Low	Low	Moderate	High
Strong	Very Low	Very Low	Very Low	Low	Moderate

- Each threat is evaluated on its own merit.
- Each control environment is evaluated on its own merit
- Combine the results for each threat to determine Residual Risk





## **Manuel Centeio**

WolfPAC Development

Phone: 617-261-8168

Email: [mcenteio@wolfandco.com](mailto:mcenteio@wolfandco.com)