

**RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.  
Learn.  
Secure.

Capitalizing on  
Collective Intelligence

# Reboot Your IT Threat Risk Assessment (TRA) Process in Twenty Minutes

SESSION ID: GRC-R04A

**Ola Lawal**

Manager, IT Compliance & Risk  
Enbridge Inc.  
@supolawal





# Introduction

- ◆ Threat Risk Assessment (TRA) Process
  - ◆ Scope - IT projects
  - ◆ Main Objective - Assess risks early on in the SDLC
- ◆ Challenges
  - ◆ Too many projects to be assessed
  - ◆ Funding for detailed assessments
  - ◆ How do we focus on the areas of greatest risk?
  - ◆ How can we demonstrate “real” business value?

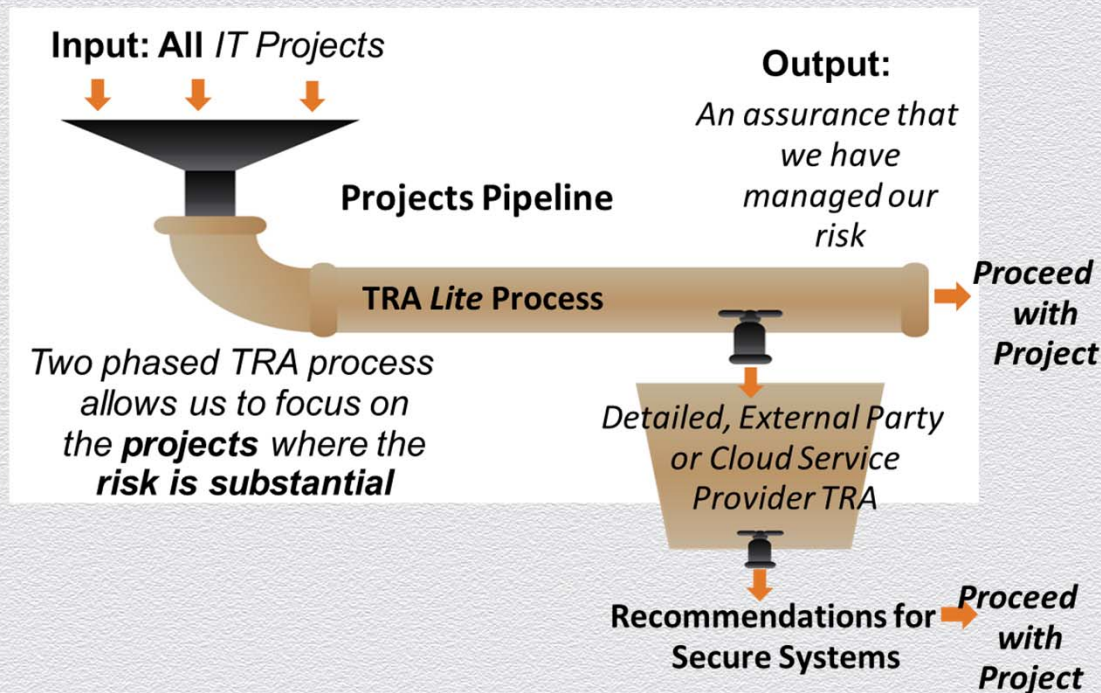


## What We Did – A Reboot!

- ◆ Five main activities to address our challenges
  - ◆ Focused more on business processes using a two step process
    - ◆ TRA Lite
      - ◆ Detailed (or external party, cloud provider, etc.) TRA
  - ◆ Provided as much information upfront as possible
  - ◆ Automated the process (as much as possible)
  - ◆ Engaged the business in risk treatment
  - ◆ Report report report!!!



# A Two Step Process



- ◆ 5 Detailed Review Triggers
  - ◆ Regulatory compliance
  - ◆ Sensitive data
  - ◆ External party/Public facing
  - ◆ Critical infrastructure
  - ◆ First of its kind



# Information Upload

- ◆ Relevant Information
  - ◆ Roles and responsibilities (Project managers, architects, sponsors, etc.)
  - ◆ How to request service
  - ◆ How long does it take to complete a TRA
  - ◆ How to plan for a detailed assessment (costs, timelines, etc.)
- ◆ Marketing Materials
  - ◆ FAQs & Service Brochure
  - ◆ Lunch & Learns (program & project managers)



# Automated Processes

- ◆ Service requests
- ◆ Information Gathering
- ◆ Response/Recommendations
  - ◆ Observations
  - ◆ Risk response framework
    - ◆ Risk ratings
    - ◆ Acknowledgement & treatment
    - ◆ Signoff for risk acceptance



# Engage The Business

- ◆ Risk Response Framework
  - ◆ Risk treatment is a business process
- ◆ Risk Treatment
- ◆ No action is not acceptable
  - ◆ Accept risks, mitigate now or mitigate in the future
- ◆ Book Ends
  - ◆ Follow up before project wraps up
  - ◆ Real business value is in implementing recommendations



# Report, Report, Report!!!

- ◆ Metrics
  - ◆ Total number of TRAs (TRA lites, detailed, etc.)
  - ◆ Number of recommendations (addressed, accepted, etc.)
  - ◆ Planned vs. Adhoc
- ◆ Trends (“real” business value)
  - ◆ Future plans
  - ◆ Risk appetite



## What a Successful TRA Reboot Looks Like

- ◆ More requests (beyond just projects)
- ◆ More hall Way chats
- ◆ More questions
  - ◆ Recommendations
  - ◆ What are the trends
- ◆ Report requests
- ◆ Performance feedback





# **RSA<sup>®</sup>CONFERENCE2014**

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Questions?

For Further information:

[Ola.Lawal@Enbridge.com](mailto:Ola.Lawal@Enbridge.com)

(403) 718 3579