Early Warning®

EMBEDDING 2ND LINE RISK REVIEW INTO YOUR ORGANIZATION: FOCUS ON THE JOURNEY, NOT THE DESTINATION

Shelley Aul, Director, Privacy Office

1

Objectives

- Share the journey we've taken to incrementally embed 2nd line risk review into our organization and how we've matured the program over the years
- Provide an overview of our current risk review process and share lessons learned that have informed where we are today

2

Quick level set

The Three Lines of Defense

- First line – Owns and manages risks (i.e., the business)
- Second line – Oversees risks/risk and compliance (e.g., Legal, Compliance, Privacy, Security, etc.)
- Third line – Provides independent assurance (e.g., Internal Audit)

Setting the stage: 2013

- Joined EWS as the Enterprise Compliance Manager
- Hired to build the Company's Enterprise Ethics & Compliance Program
- Compliance was in the Legal Dept
- No formal policy or process for legal and compliance reviews of Company products and services
- Advice was given on an ad hoc basis and in piecemeal (e.g., in meetings, office drop ins, emails, etc.)
- Advice would get lost or misinterpreted
- Needed a more formal process to assess and document the potential legal, regulatory, compliance, contractual and policy impacts/requirements to Company products and services

Fast forward to 2015

WHAT WE DID

- Launched the Legal Compliance Impact Assessment (LCIA) process
- Created a policy requirement for LCIAs
- Embedded the LCIA into the SDLC
- Used the Company's existing GRC tool to facilitate the information gathering process
- Communicated the change and provided training to the business
- Required LCIAs for new projects and those in early development
- Put the LCIA into our annual goals

THE CHALLENGES WE ENCOUNTERED

- Received pushback from some business partners that we were creating new "hoops" to jump thru
- Concerns that "time sensitive" initiatives may be delayed
- Training end-users on the GRC tool and limitations with the tool
- Concerns that innovation work may be delayed

5

2016

WHAT WE DID

- Compliance moved out of Legal and under Risk and the Privacy Office was created within Legal
- Rebranded the LCIA to a Privacy Impact Assessment (PIA) to better align with external practices/ standards
- Created more support documents (e.g., SharePoint site, WIs, procedures)

THE CHALLENGES WE ENCOUNTERED

- The GRC was not designed for our use-case
- Our PIA questionnaire did not fit all the use-cases we were seeing
- Unnecessary work was being created when projects were going thru the PIA process that really didn't need it

6

2017

WHAT WE DID

- Transitioned to a new tool, designed for PIAs
- Added a pre-screen to cut down on unnecessary PIAs
- Created different versions of the PIA questionnaire for various use-cases
- Added PIAs to the required privacy training module

THE CHALLENGES WE ENCOUNTERED

- Felt like we (the Privacy Office) were making decisions in a vacuum needed more awareness of initiatives coming thru
- The requirements in the PIA Memo could easily get lost in the shuffle

7

2018

WHAT WE DID

- Created the Legal Review Board, consisting of members from Legal and Privacy, to review pre-screens
- Added a Legal Review, completed by an attorney in Legal, to the PIA (now the “Legal Review/PIA”)
- Added the Legal Requirements Checklist to help the business address each of the requirements in the Legal Review/PIA Memo
- Started offering voluntary training sessions throughout the year

THE CHALLENGES WE ENCOUNTERED

- The questions in the pre-screen weren’t always getting us the info we needed to triage requests
- Reporting was manual

8

2020

WHAT WE DID

- Privacy moved out of Legal and under Risk
- Formed the Legal and Privacy Review Board (LPRB)
- Replaced the pre-screen process with the Legal and Privacy Intake Form
- Rewrote the Intake Form to help the LPRB better triage initiatives and to enable reporting

THE CHALLENGES WE ENCOUNTERED

- Certain business units wanted to move faster and with more independence

2022

WHAT WE DID

- Released a Self-Assessment for predefined data use-cases to help the business move faster
- Added Intakes to our enterprise risk management goals to hold all employees accountable

THE CHALLENGES WE ENCOUNTERED

- Various risk teams have intake processes, hitting the business at different times, asking for the same information
- Need to become more agile and lean
- The business needs better visibility into the status of Intakes and Legal Review/PIAs
- Privacy needs a more efficient way to monitor new initiatives and initiatives that change over time

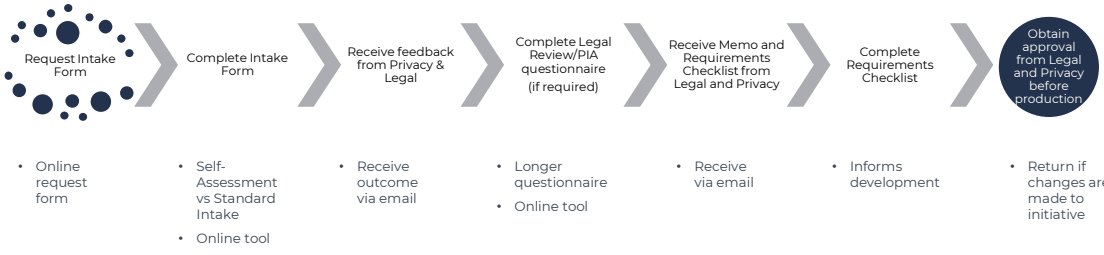
2023

WHAT WE ARE DOING

- Consolidating the various risk teams' intake forms into one consolidated risk intake form
- Redefining the policy requirement for the consolidated risk intake process
- Expanding the LPRB to include members from the other risk teams
- Moving the intake process into the Company's new GRC tool to centralize and manage risk activities, map/link data, automate processes, and increase visibility across the organization

11

Our process flow today



12

13