| | |
|---|---|
| **Title:** | Understanding Risk Beyond Cybersecurity: Developing agency-wide Enterprise Risk Management |
| **Category:** | Enterprise IT Management Initiatives |
| **State:** | Indiana |
| **Contact:** | Graig Lubsen, Indiana Office of Technology 317-268-8071; glubsen@iot.in.gov |
| **Project Initiation Date:** | 2021 |
| **Project End Date:** | Ongoing |

## Executive Summary

In the Spring of 2021, Anushree Bag, Executive Director of Enterprise Risk and Resiliency Services, and her team at the Indiana Office of Technology (IOT) led a small team to establish the Enterprise Risk Management (ERM) framework at the centralized IT organization for the State of Indiana.

All businesses, including government agencies, need to have a plan to manage their major risks. This project established a framework and a process to effectively manage risks across the organization through the use of a common risk management framework. It followed an iterative and collaborative process to create a tangible work product, the Risk Register.

## Idea

Enterprise risk management is a holistic, disciplined approach to identifying, addressing, and managing an organization's risks. With ERM, the responsibility of risk management isn't placed on individual departments or business units, but the organization's leadership. This approach sets ERM apart from the "silo approach" of traditional risk management where each department handles their own risk.

The process (or cycle) of the enterprise risk management framework has five main parts: 1) Strategy Objectives, 2) Risk Identification, 3) Risk Assessment, 4) Risk Response, and 5) Risk Monitoring. (Figure 1)



*Figure 1*

## Implementation

As a first step, Anushree Bag met with IOT's leadership and provided introductory training on ERM, and how the adoption of ERM, through better awareness and management of the agency's risks, could a) improve the achievement of strategic goals 2) inform budget decisions and 3) help meet performance goals.

The team then met with all IOT business unit leaders and trained them on ERM fundamentals - the importance and relevance of ERM as a methodology, risk categories, ways to identify, measure, rank and prioritize risks, how to determine risk responses, how to monitor and report on risks, and other key risk terminology like risk register, heat map, and emerging risks.

In the Fall of 2021, the ERM team met once again with the business unit leaders and sought their input on what they perceived to be the most significant risks in the agency. **Previously, the only risk under consideration was cybersecurity risk, but with this enterprise-level thinking, business unit leaders reported on other risks, such as workforce management, compliance, reputation, technology debt, cloud security, etc.**

Based on the response, the ERM team developed IOT's first-generation Risk Register, which is the first of its kind in the State of Indiana.

Risks are calculated as either emerging or current, then are tabulated by type. The types are 1) strategic, 2) operational, 3) financial, 4) compliance or 5) reputational. Business leaders are then asked to score the level of impact, likelihood and velocity – the speed at which the risk affects the organization. Calculating across these three areas, a risk measurement is calculated.

# Impact

The first risk generation risk register was developed in Excel and was a documentation of more than 100 risks. The top 10 were placed on a heat map (Figure 2), and presented to the IOT Agency Head, with the potential for the agency head to present it to the executive branch agencies of Indiana, and/or to the Governor's cabinet.
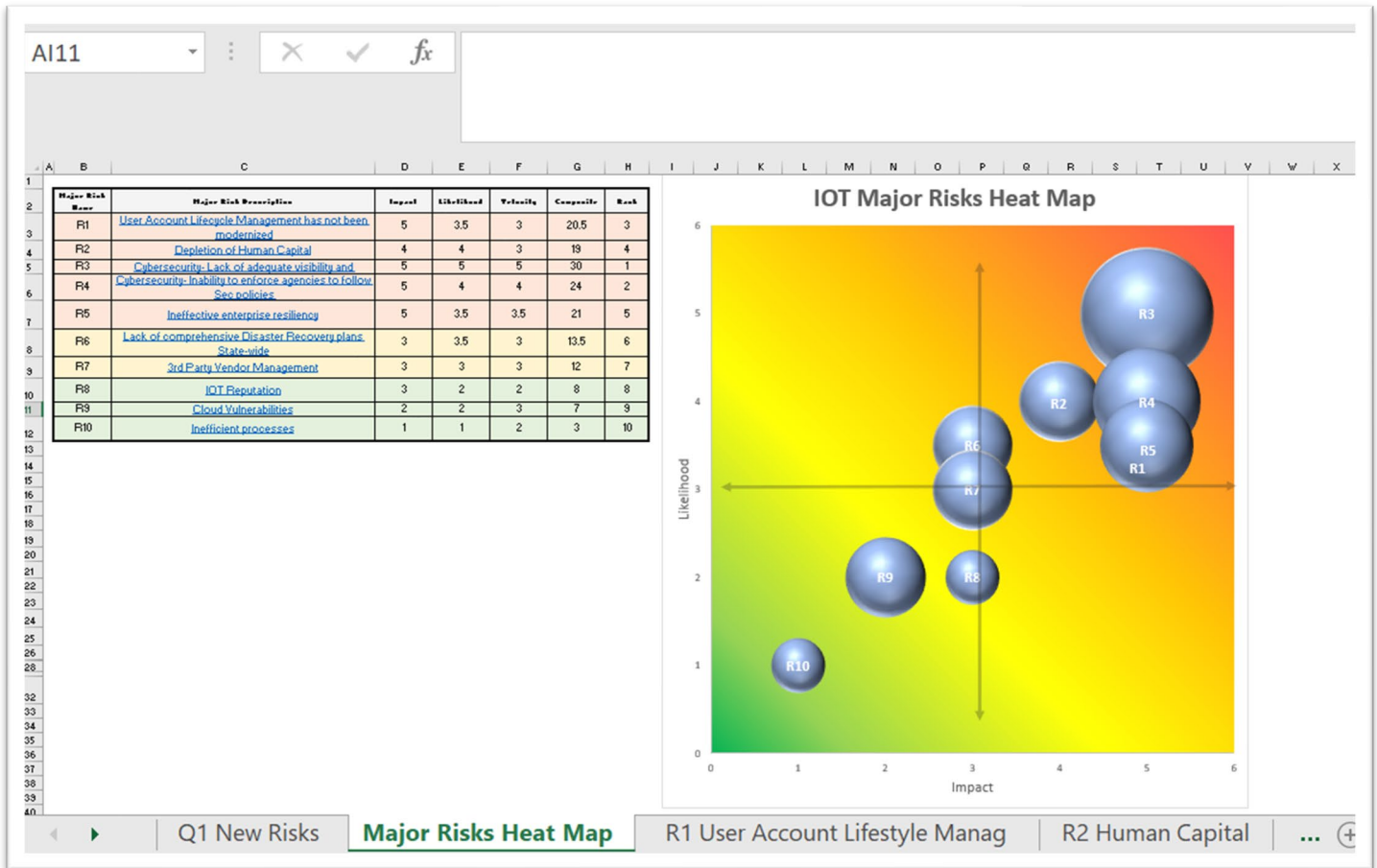


*Figure 2*

In the spring of 2022, the IOT ERM team created the second-generation risk register by importing all risks from the Excel spreadsheet to the State of Indiana's Governance, Risk & Compliance (GRC) tool - Archer. The Risk Register and heat map are now published in real time on IOT's management portal (Figure 3). Any IOT personnel can report on any risks by entering information through an online form that was developed by the IOT Communications team, and hosted on IOT's intranet, Marvin.
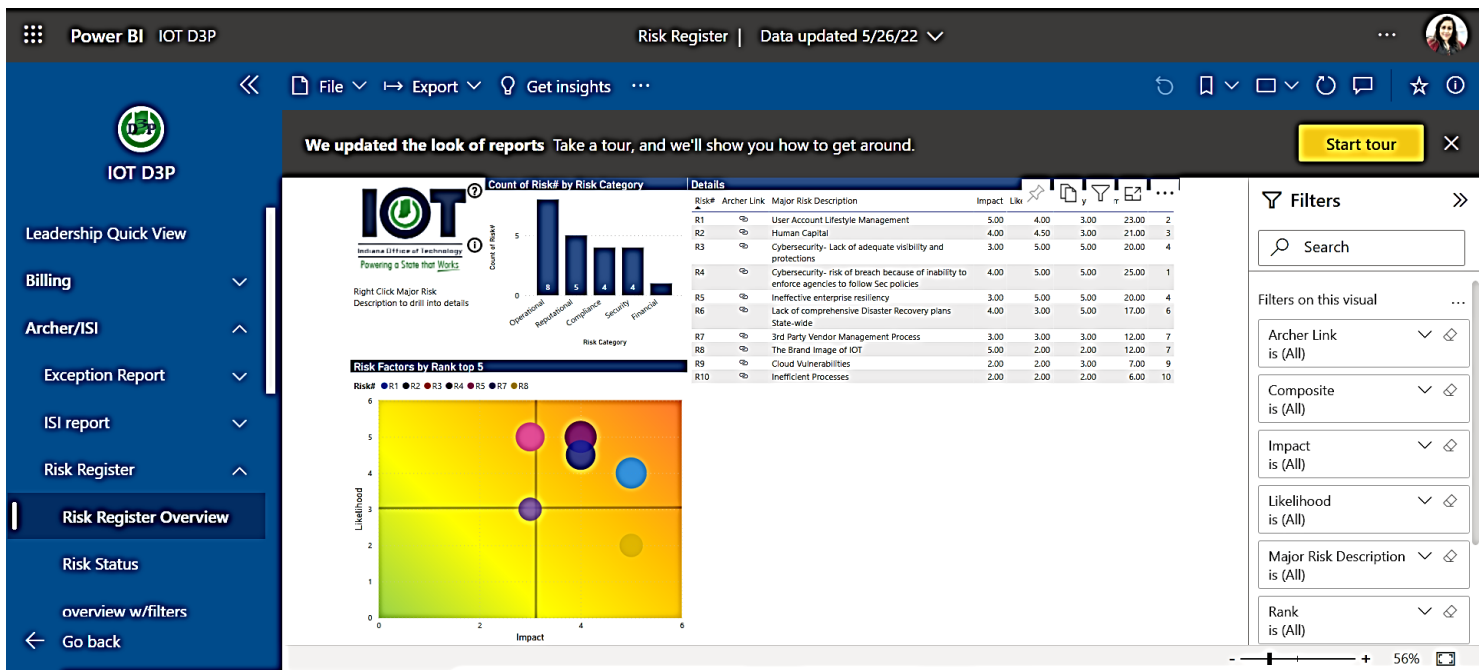
*Figure 3*

Indiana is the first state to have a formal ERM program, and Anushree was invited to meet with the National Association of Chief Information Officers (NASCIO) Executive Committee, where she presented a business case on why State Government should consider adopting ERM as a strategic priority. The presentation was well received and NASCIO created a ballot-based ERM and sent it to all State CIOs at the end of 2021.

Based on responses to the ballot, NASCIO published the Top 10 Risks report in March 2022 (Figure 4).

STATE CIO TOP 10 ENTERPRISE RISKS

2022 Priority State Enterprise Risks

**RISK 1**
Cybersecurity Risk

**Cybersecurity Risk:** data protection; insider threats; third-party practices as outsourcing increases; determining what constitutes "due care" or "reasonable"; ransomware; identity theft; unauthorized access to state government services

**RISK 2**
Technology Risk

**Technology Risk:** IT infrastructure management; IT maturity; information asset management; cloud portfolio; artificial intelligence and machine learning; block chain; identity theft

**RISK 3**
Operational Risk

**Operational Risk:** policies; procurement; vendor management; physical security; business continuity; disaster recovery; unauthorized access to a service

**RISK 4**
External Risk

**External Risk:** supply chain; utility disruption; inflation; economic risks; global pandemic; force majeure; workplace violence

**RISK 5**
Enterprise Project Management Risk

**Enterprise Project Management Risk:** failed projects; late projects; irrelevant projects; lack of effective independent verification & validation (IV&V) ; lack of qualified project management discipline; lack of self-correcting governance; procurement process risks

**RISK 6**
Compliance Risk

**Compliance Risk:** federal regulatory audits; state regulatory audits; contract compliance assurance; administrative regulations

**RISK 7**
Financial Risk

**Financial Risk:** budget management; valuation; liquidity; inadequate economic resilience

**RISK 8**
Reputational Risk

**Reputational Risk:** data breaches; fraud; disputes/lawsuits; scandal

**RISK 9**
Strategic Risk

**Strategic Risk:** related to support of local government; investing in innovation

**RISK 10**
Workforce and Labor Risk

**Workforce and Labor Risk:** human capital management; labor shortage; IT staffing and vendor personnel risk; recruitment and retention of employees

NASCIO

www.nascio.org

*Figure 4*

The ERM team now meets with business owners twice a year to seek and document updates to the risk register and the top 10 risks. Anushree was invited to co-facilitate an ERM workshop at NASCIO mid-year and has demonstrated ERM to several State of Indiana agencies.

Indiana is leading the process of developing ERM programs in state government, nationally, and as a direct outcome of this project, the Indiana Office of Technology now has an established enterprise risk management framework.