

# 1. Ensure AI Transparency

- **AI Explainability**
  - To build trust among AI users, develop explainable AI that is transparent across processes and functions
- **How to Minimize unintended bias**
  - Build responsibility into your AI to ensure that the algorithms – and underlying data – are as unbiased and representative as possible.
- **How to Protect the privacy and security of data**
  - Leverage a privacy and security-first approach to ensure personal and/or sensitive data is never used unethically.

**SME: Data & Analytics team**

**Data: Open-source libraries**

## 2. Disinformation Monitoring

- **Analysis and impact of the disinformation (fake news)** Automated analysis of the scale and impact of the disinformation phenomenon on specific geographical areas/population groups/online users;
- **Prioritize reported information** An algorithm that prioritizes reported information for manual verification.

**SME: Data & Analytics team**

**Data: Twitter Social media, Open-source libraries**

## 3. Lessons Learnt

- The current process to generate lessons learned is manual, **resource intensive and time consuming**
- Utilize machine learning and artificial intelligence to better mine Project Closure database for lessons and knowledge **coming out of closure reports** to support **better programming and decision making** within UNICC .

**SME: Project Management team**

**Data: Project Closure reports**

## 4. ML enabled Security Fraud detection

### ML Algorithms to help automate

- Analysis of event, incident and log data
- Analytics on risks - opened, closed, under risk thresholds, risk owners, controls. Ultimately, measure & increase SOC team's efficiency.
- Cross validate based on data collected based on SOC and Vulnerability management
- Fill out knowledge gaps specific to Vulnerability management

**SME: Security Team**

**Data: Incident log**

# 5. Incident Management

## Incident order of priority

- Identify categories of incidents. Today we do not have a clear classification of the types of incidents
- Identify known errors by reviewing the resolution data.
- Identify recurring Service Requests for the different teams, so that we can see how they can be streamlined.

**SME: OPX team**

**Data: Incident reports**

## 5. Software license Management

- **Improve software license management.** Current license management is manual and reactive.
- The process is not efficient, effective nor fully reliable.
  - ISAE3000 audit run in October 2016.
  - External audit recommendations from Connect Sphere (“Add software assets and licenses to the AMS DB and link to the CMDB. [...]”)

**SME: OPX team**

**Data: Incident reports**