

# Joint Information Technology Oversight Committee

Prepared by:

Kevin G. Moore Jr., Director

December 3, 2021



# Risk Based Software Inventory

*(Updated Results)*



# Inventory Methodology

Legislative IT primarily followed the methodology created by the Agency of Digital Services (ADS) as outlined in a previous presentation. The process is simple yet effective for producing a dataset which we can readily learn from.

*(See below screenshot.)*

## Method Used

Clean, efficient, explainable

- Use of a simple method was key to understanding how to compare apples to apples
- Risk assessed across four primary categories
  - Software platform
  - Hardware operating system
  - Data type
  - Web presence
- Assigning a numerical score and providing a visual representation for “at a glance” understanding
- Bonus:
  - Scoring process allowed a single set of eyes to evaluate for consistency
  - Allowed for the identification of insufficiently documented applications
- Living document that is updated as new applications are defined/discovered
- Provided the basis to apply elements of our risk assessment to our applications

Source: Scott Carbee, CISO, ADS (July 23, 2021)



# Scoring Criteria

The scoring system in use by Legislative IT is based almost entirely upon the system developed by ADS's software assessment framework. The scoring criteria assesses 4 categories as follows:

## Operating System Score [0-3]:

- 0 – Up to date current version, within Publisher support.
- 1 – Non-current version, still within Publisher support.
- 2 – Non-current version, still within Publisher **extended** support.
- 3 – Operating system is End of Life or Unsupported by the Publisher.

## Software Score [0-3]:

- 0 – Up to date current version, within Publisher support.
- 1 – Non-current version, still within Publisher support.
- 2 – Non-current version, still within Publisher extended support.
- 3 – Software is End of Life or Unsupported by the Publisher.

## Data Score [0-3]:

- 0 – All data on information system is public.
- 1 – The information system contains “Administratively sensitive” information.
- 3 – System contains legally protected sensitive information, Such as PII, PHI, FTI or other information of a comparable sensitivity.

*Note: The ADS framework only use the 0 and 3 criteria to denote if the system has sensitive information, to make this metric more meaningful to the General Assembly the 1 “Administratively Sensitive” score was added.*

## Web Presence [0-3]:

- 0 – Application does not have a web interface.
- 1 – Application has an internal web interface.
- 2 – Application has an External web interface, managed by publisher.
- 3 – Application has an external web interface, managed by State.

*Each application will score from 0 to 12, 0 indicating the lowest risk and 12 the highest.*



# Analysis

## Data Points

**Total Data Points:** 16,956 (previously 4086)

**Unique pieces of software:** 181 (previously 217)

**Unique Software Versions:** 328 (previously 332)

**Software Terms Replaced:** 0 (no change)

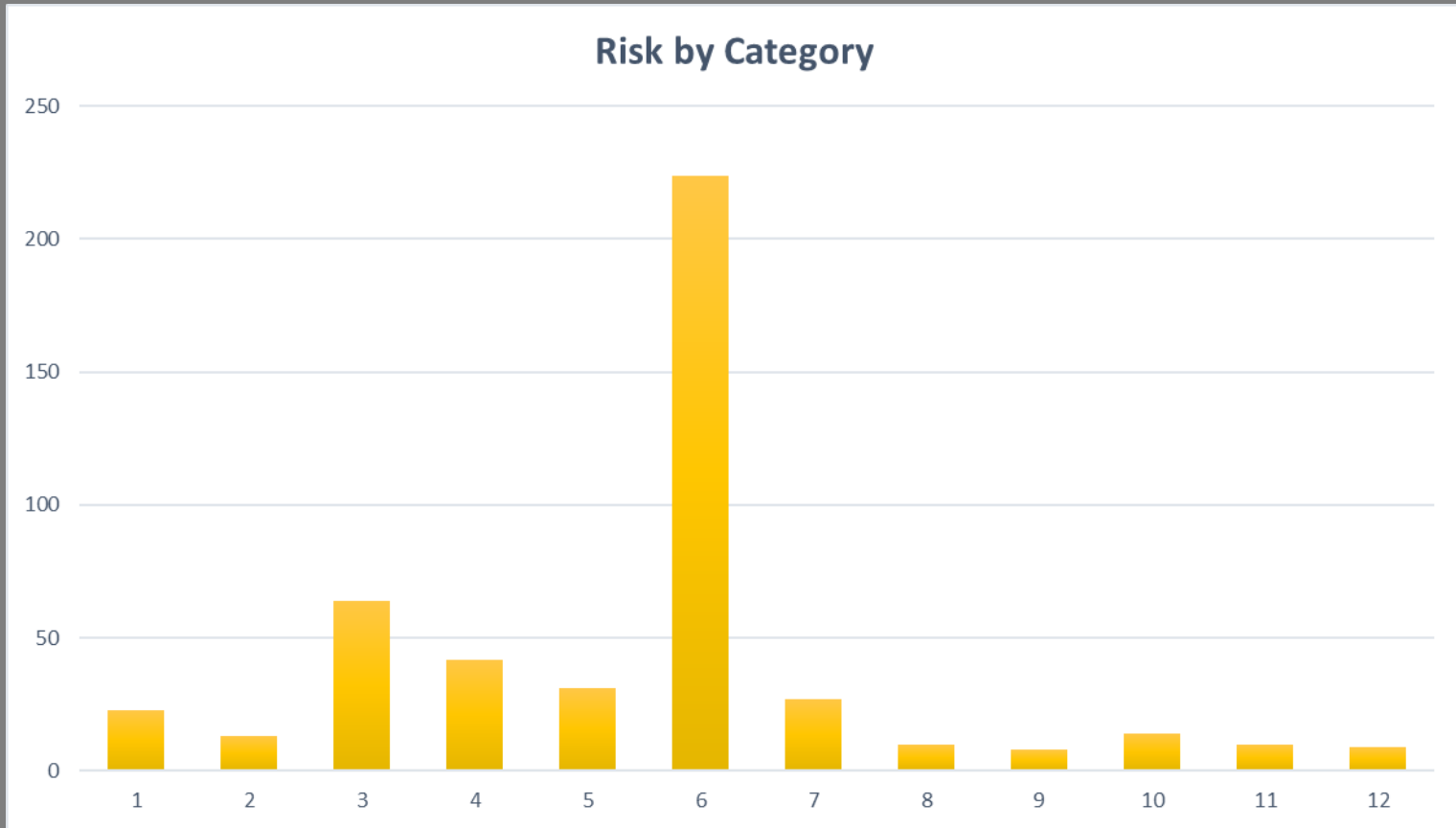
**Software Terms Ignored:** 3387 (previously 3277)

**Software Items not rated:** 0 (previously 33)



# Where we were...

Application Risk by Category

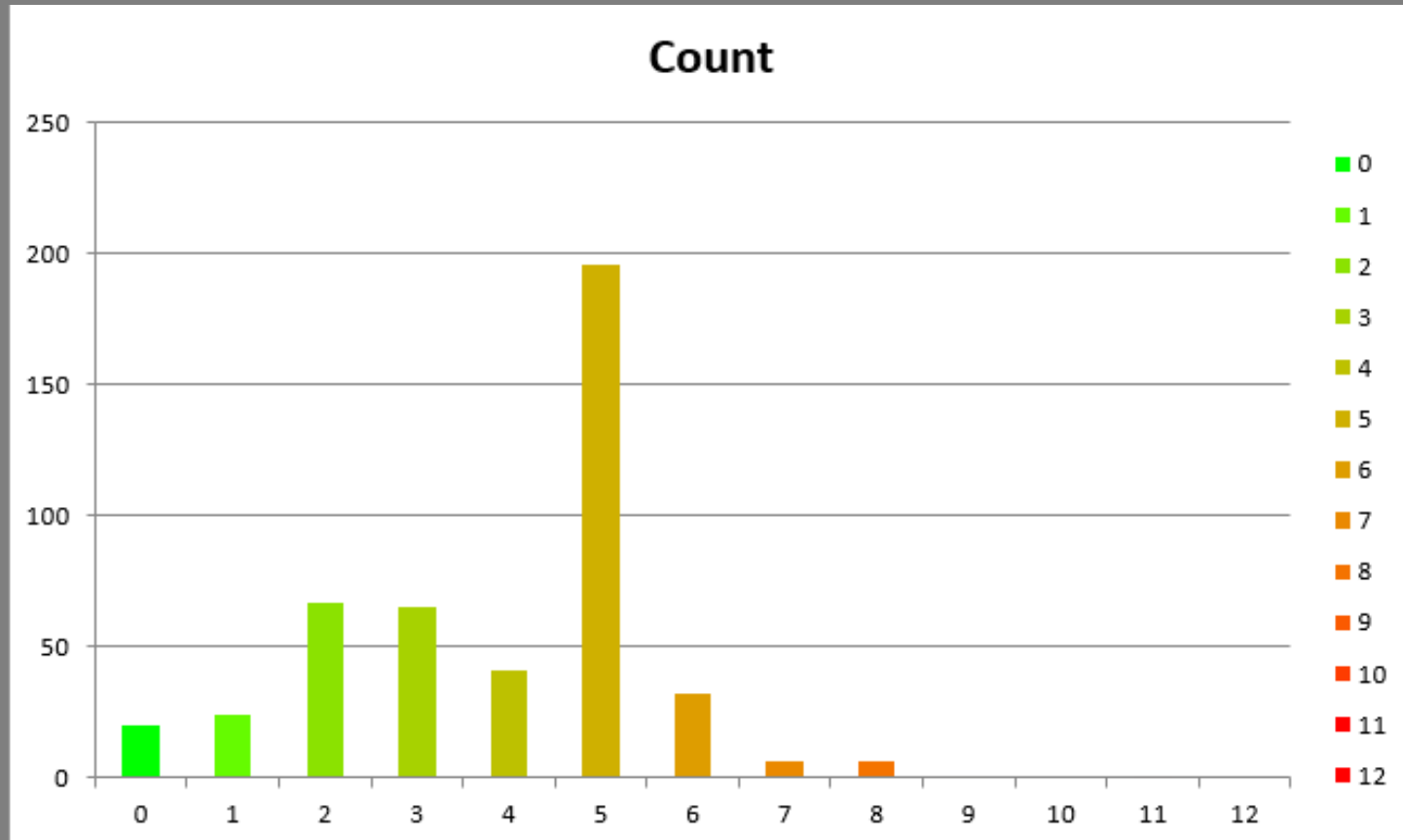


*Data as of September 30, 2021*



# Analysis as of Dec. 2, 2021

Application Risk by Category



Data as of December 2, 2021



# What have we learned, so far?

- This exercise continues to provide a good deal of insight into areas in need of improvement.
- However, the riskiest applications continue to be well known to Legislative IT.
- Scoring improvements between captures shows positive progress.





# Future Goals

- **Complete dataset with complete scores**
- **Establish automated routines to collect up-to-date data for future analysis**
- **Use data to make informed decisions related to system improvements**



Questions?



Office of Legislative  
Information Technology