

# Joint Information Technology Oversight Committee

Prepared by:

Kevin G. Moore Jr., Director

September 30, 2021



# Risk Based Software Inventory

*(Preliminary 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.*



# Early Analysis

Data Points

**Total Data Points: 4086**

**Unique pieces of software: 217**

**Unique Software Versions: 332**

**Software Terms Replaced: 0**

**Software Terms Ignored: 3277**

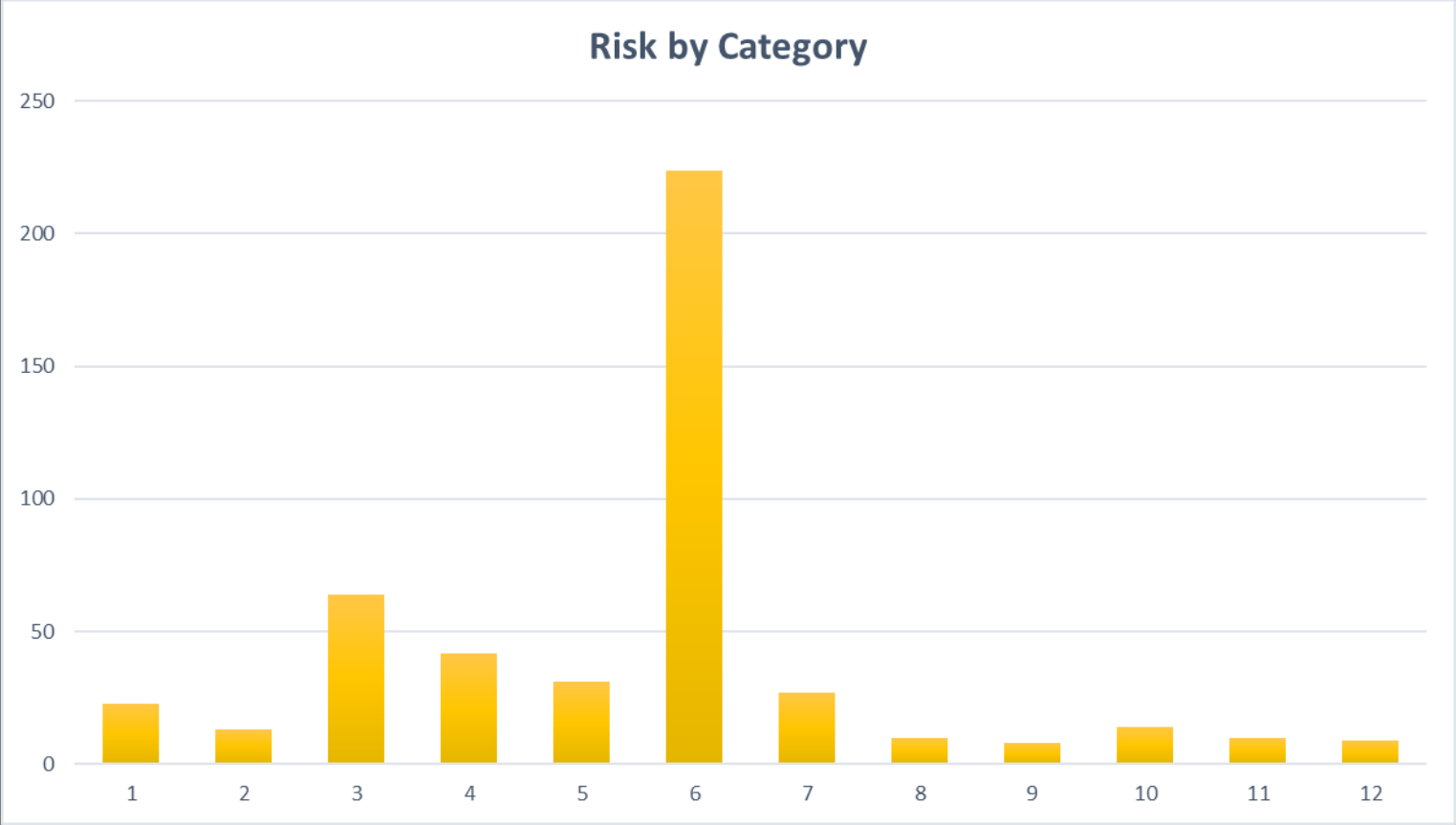
**Software Items not rated: 33**

**Unique OS and Software Version Pairings: 492**



# Early Analysis

Application Risk by Category



Data as of September 29, 2021



# What have we learned, so far?

- This exercise provided a good deal of insight into areas in need of improvement.
- Similar to ADS, the riskiest applications were well known to Legislative IT, but we now have a clearer understanding of how they compare to other applications in use.
- The value provided by this exercise has prompted us to make this process permanent and more dynamic. Doing so allows us to continue to capture this information without the same demand on staff time.



# 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