

The background features abstract, overlapping green geometric shapes in various shades, including light lime green, medium green, and dark forest green. These shapes are primarily located on the left and right sides of the page, framing the central text.

Risk-informed Application Inventory

Review of Methods, Insights, and Critical Applications

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 and existing applications are defined/discovered/researched
- Provided the basis to apply elements of our risk assessment to our applications

Assessing Risk

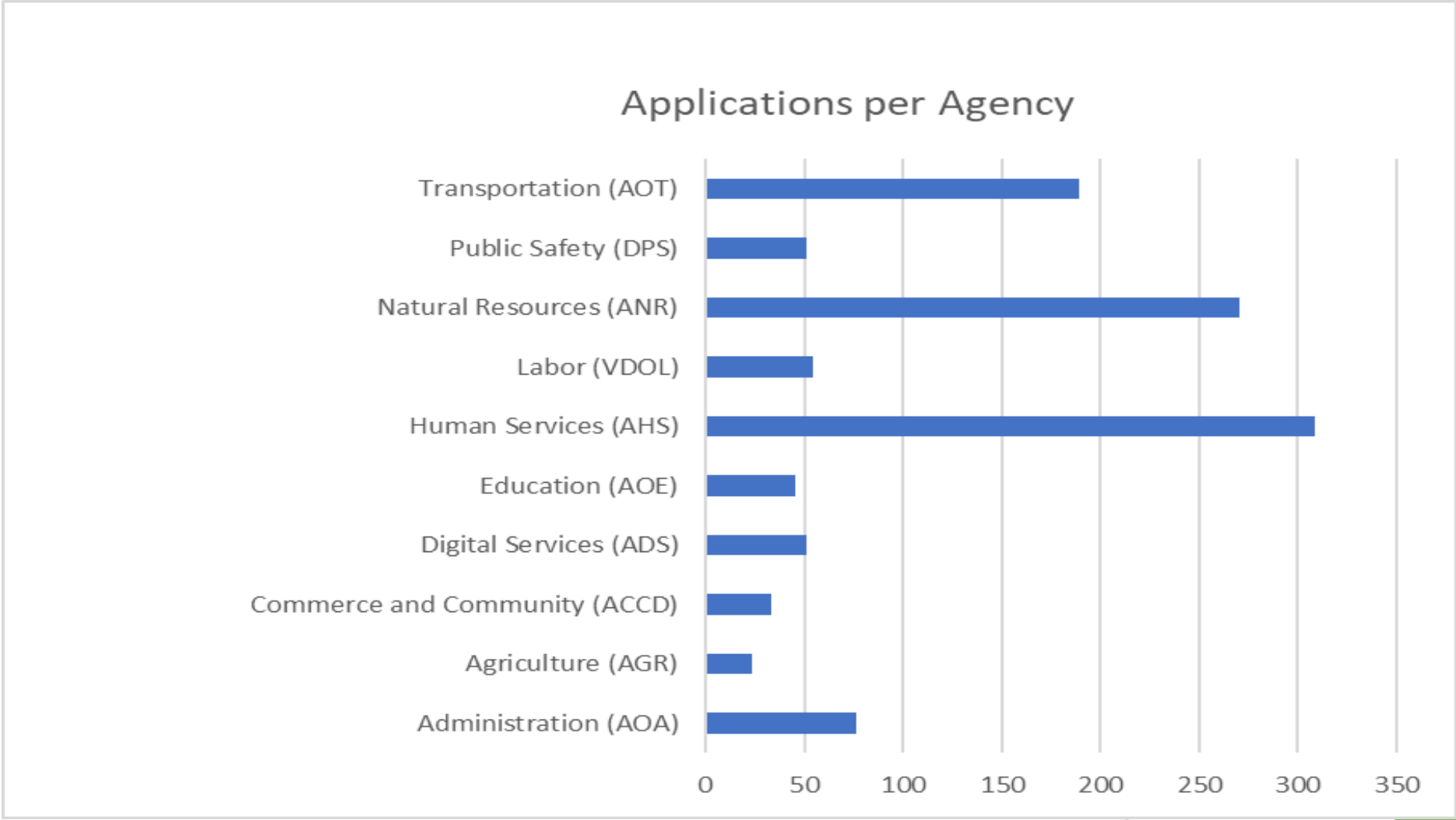
Scripted scoring with human evaluation

- **Software platform evaluated against:**
 - Latest version = 0
 - Supported version = 1
 - Extended support = 2
 - End of Life/unsupported = 3
- **Hardware OS used similar scoring to above**
- **Data was a simple test**
 - Publicly available data = 0
 - Sensitive data of any type (PII/PHI/FTI/etc.) = 3
- **Web presence was scored based on exposure**
 - No web interface = 0
 - Internal web access only = 1
 - External, vendor owned (SaaS) = 2
 - Public facing, State owned = 3
- **Each application total score falls between 0 - 12**

Example scoring

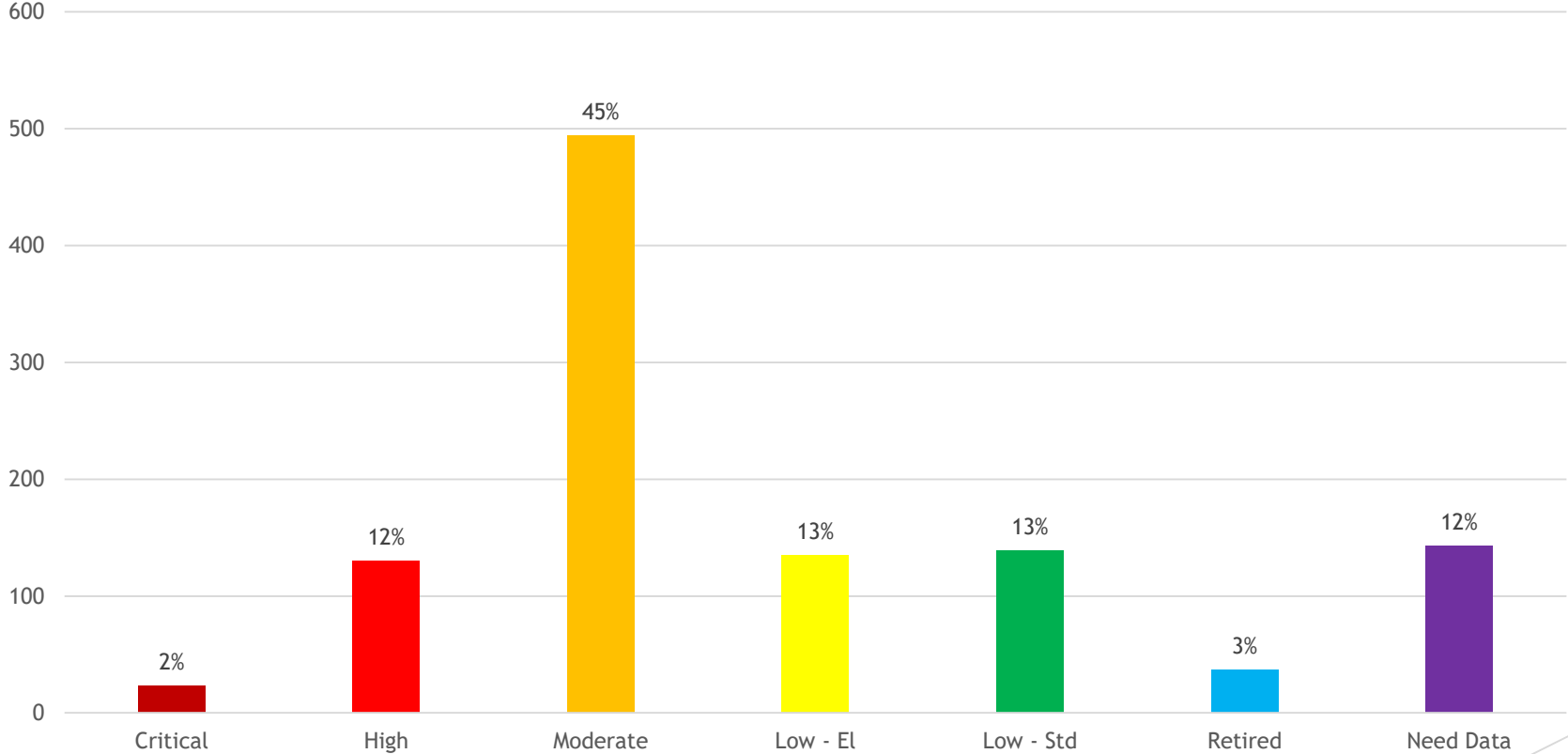
- ▶ The Agency of Widgets has an application that allows people to find the right widget to support their local businesses. The service has been stable and so, left to run largely unchanged over the last 6-8 years.
 - ▶ The service is provided by a SQL server, with a web interface. All the data is publicly available, and the public can log into it and search for local businesses in the desired category. When built, it had the latest web interface, database, and server platform.
 - ▶ Specs - SQL server 2012, IIS 8, 2012r2 server, available at “localwidgets.vermont.gov”
 - ▶ Scoring breakdown (7 - Moderate)
 - ▶ Software platform - 2 (extended support)
 - ▶ Hardware operating system - 2 (extended support)
 - ▶ Data type - 0 (public)
 - ▶ Web presence - 3 (State hosted, public searchable)

Early Analysis



Early Analysis

Risk by Category



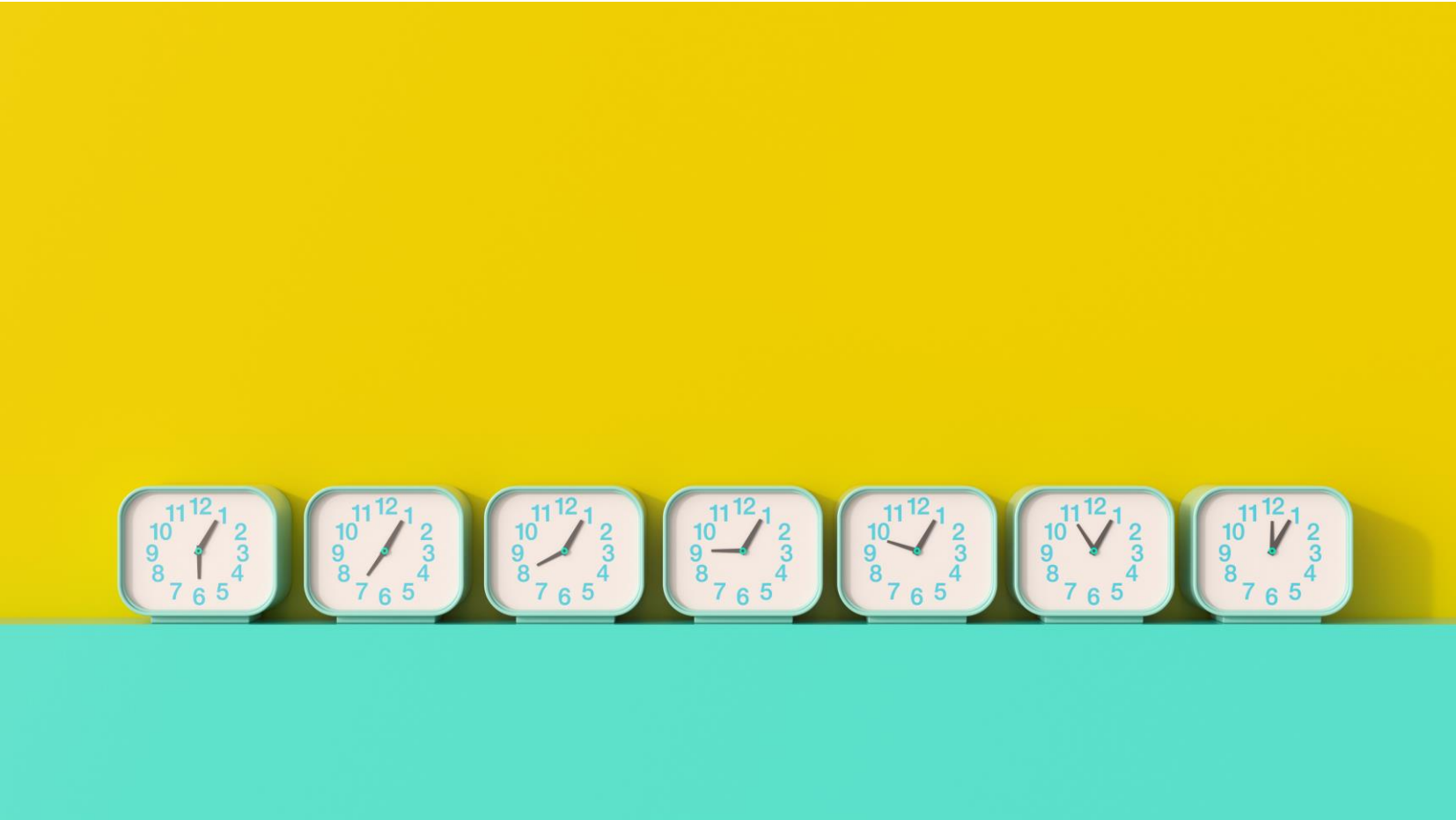
Key Themes Regarding Critical Rated Applications

- ▶ Unsupported operating systems
- ▶ Unsupported software platforms
- ▶ Public facing and accessible web pages
- ▶ Contain sensitive data
- ▶ The critical applications get highest risk rating across all categories
- ▶ Tend to be in-house/contractor developed or modified OR
- ▶ Highly integrated and expensive software solutions

Other Factors

- ▶ Complexity - With multiple technologies and custom code built into the applications it can be a monumental task to upgrade even simple components
 - ▶ For example: A required version of a web platform will not run on a modern server OS. If Server OS is updated, application effectively stops working.
- ▶ Custom code - Code may have been developed years ago by a contractor or since-departed State employee. Hiring a new developer to modernize the code is generally unfeasible.
 - ▶ Example: A system programmed 15 years ago with .NET code is effectively not upgradeable due to the legacy processes that bog a system down
- ▶ Cybersecurity considerations - Security as a part of design has only begun to take hold over the last few years. Before that, where security was concerned, add-ons were created to protect the systems...farther back, the notion of security was anathema to the writing of code and system design. Interoperability thorough system trust (and user trust) was the prevailing pattern.
 - ▶ Explained: The State uses “add-on” security quite effectively. Firewalls, intrusion detection/prevention, multi-factor authentication...all these support and enhance the security of our legacy products, but they are not as effective as a securely designed system.

Placeholder



What Did We Learn?

Having an objective basis to focus on improvement adds to efficiency

- Most of the riskiest applications were already known
- The list allows us to share and communicate our position on risk to the enterprise as well as risk to the Agencies
- Long-term inventory management will require a purpose-built system
 - Consolidation of various inventories
 - Iterative process
- Future iterations will allow us to refine our criteria to track and ascertain progress
 - Standardization of data elements
 - De-duplication of applications across Agencies
 - Deep dives on applications with little documentation to assess risks

Future State

Risk management hinges on progress and consistency

- Use the scoring criteria to drive updates, upgrades, and system replacement
- Transform data into consolidated inventory (single source)
- Move data from the flat file format to Archer GRC (governance/risk/compliance) system for better standardization, scoring, and reporting.
- Add additional dimensions of risk criteria to enhance the risk profile (criticality, RTO/RPO, resourcing, etc.)