

IAITAM ACE

KICKIN' ASSETS
SINCE 2002

**MANAGING END-OF-LIFE
RISK WITH IT ASSET
MANAGEMENT**



**NASHVILLE, TN
MAY 9TH - 11TH**

WANTED



MIKE TAYLOR
SENIOR MANAGER
DELOITTE & TOUCHE LLP

WANTED



LINDSEY MACKEY
MANAGER
DELOITTE & TOUCHE LLP



IAITAM ACE
KICKIN' ASSETS
SINCE 2002

IAITAM.org | ACE 2023 | Nashville TN

What is Technology Lifecycle Management (TLM)?

Technology Lifecycle Management (TLM) is an enterprise function that encompasses the planning, design, acquisition, implementation, and management of elements comprising of the IT infrastructure. It is important to the reduction of risk caused by End-of-Life (EOL) technology.

IS



The ability to identify and plan for upcoming EOL remediation activities far enough in advance to be **proactive instead of reactive**



An enterprise-wide function that requires collaboration between multiple stakeholder groups to function efficiently



A **policy, operating model, and methodology** that enables the TLM team to prioritize EOL remediation efforts in collaboration with product and application owners



IS NOT

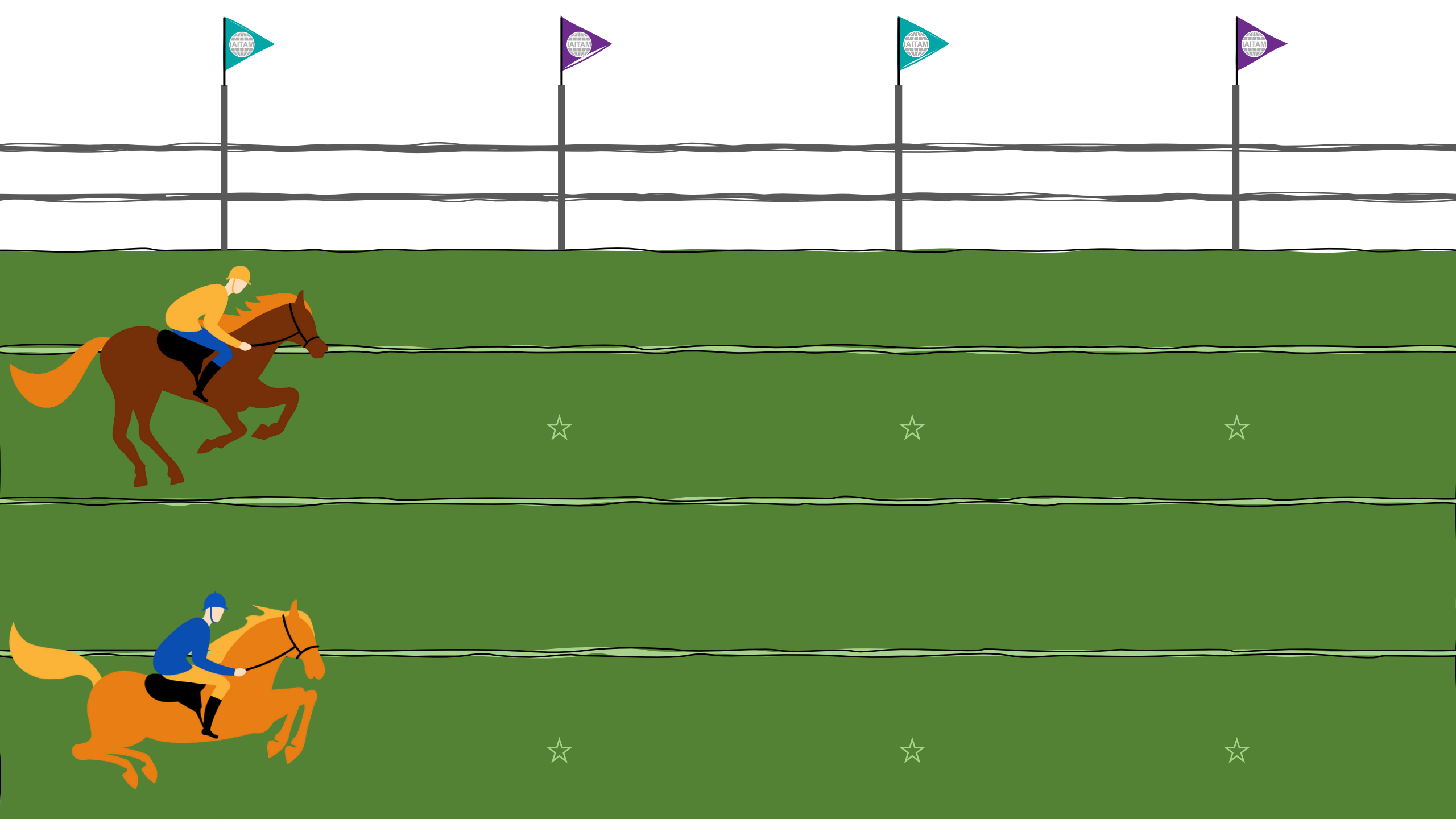


A **Technology Standards Management** capability – EOL TLM does not define technology standards for use within the enterprise, nor establish version currency of hardware or software beyond established EOL dates (N, N-1, etc.)



A **Patch Management** capability – security and version patching are handled by the appropriate technology and application teams





Common TLM challenges

LACK OF GOVERNANCE

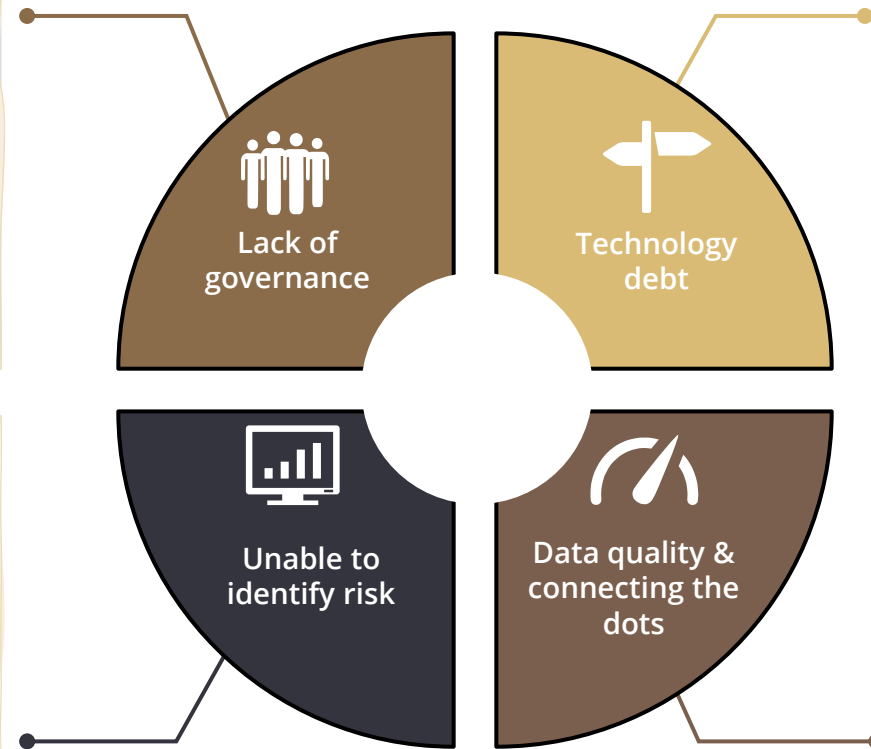
Missing, incomplete, or inconsistent policies, processes, and standards and organizational silos prevent TLM from being effective.

Lack of governance leads to lack of policy and process enforcement. Governance should be extended to the management and remediation of data.

UNABLE TO IDENTIFY RISK

EOL hardware and software is often not considered when managing IT risk.

Inability to maintain an up to date and accurate inventory and combine that with service and application models creates an inability to assess and manage risk.



TECHNOLOGY DEBT

Companies defer technology refreshes to minimize impact and accumulate technical debt and increased complexity over time.

Hardware refreshes are driven by modernization projects and can lack budget for both resources and working capital to maintain systems on a planned basis after project reaches specific milestones.

DATA QUALITY & CONNECTING THE DOTS

Many companies are unable to manage EOL even with a TLM capability in place because the asset, CMDB (Configuration Management Database), or EOL data is not accurate or timely.

Even those with good sources of data may fail to connect the dots and aggregate, normalize, and reconcile data in a way that facilitates good TLM outcomes.



What does good look like?

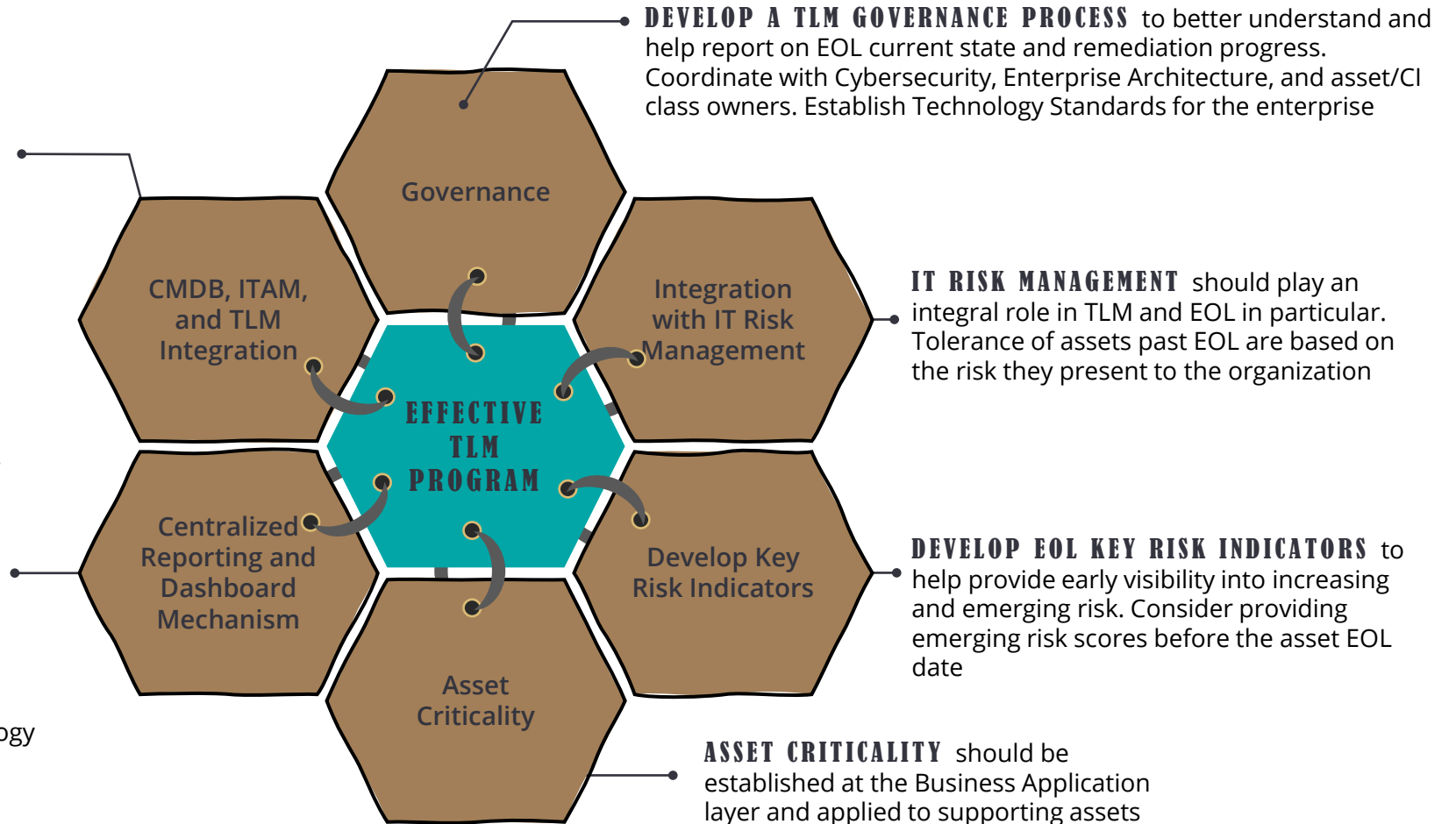
A effective TLM program should contain each of the components below

MANAGEMENT OF IT ASSETS AND CMDB CIS SHOULD BE IN AN INTEGRATED SOLUTION

so that assets are managed over the full asset lifecycle, from planning to disposal, and product lifecycles are established before vendor EOL dates but after assets are fully depreciated. This alignment to TLM allows for accurate scoring and evaluation of existing technology

IMPLEMENT A SINGLE TECHNOLOGY SOLUTION for proactive notifications and real-time dashboards for business owners:

- EOL reports by Service/Application criticality
- EOL reports for pending assets by class and date
- EOL reports for assets past EOL
- IT Risk reports for EOL assets
- Consolidated for reporting and management of both IT and OT assets as required
- Visualize spend required to support EOL technology

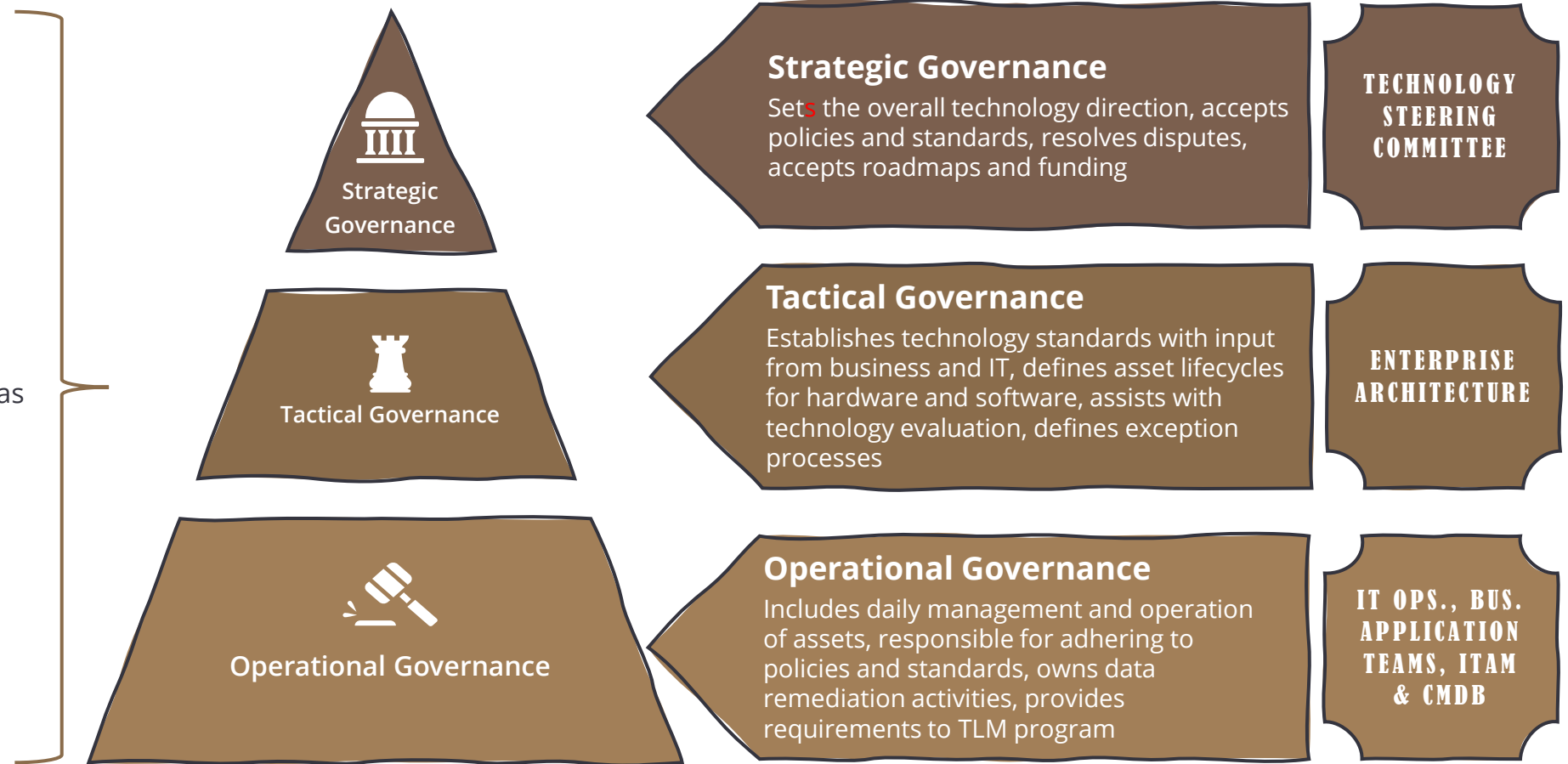


What does good look like – TLM governance top to bottom

Objective: Create enterprise-wide policies, standards, and processes for IT Asset Management that covers the full asset lifecycle, with monitoring and enforcement mechanisms to maintain them

ESTABLISHED TLM GOVERNANCE

- Policies, processes, and standards should be enterprise wide to reduce work done in silos
- Engage IT and the business as part of the governance process
- Include data governance in the model with clear roles and responsibilities for data quality remediation



What does good look like – key stakeholder groups

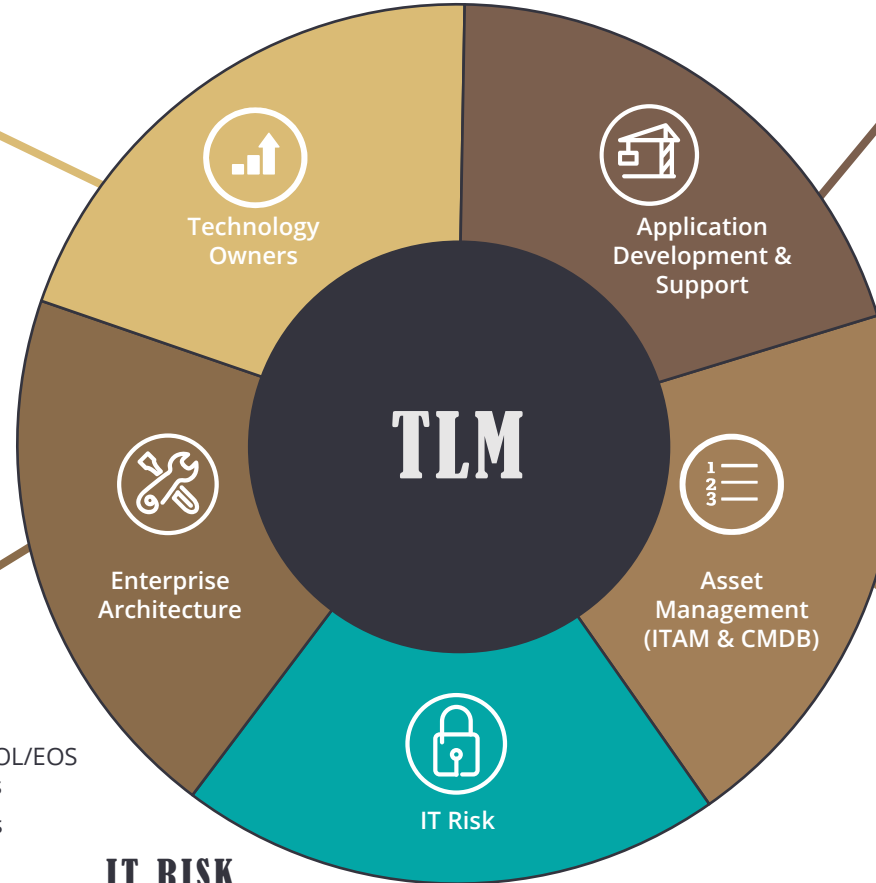
Objective: Establish collaboration across the enterprise to establish standards, determine lifecycles, and define exception processes for EOL remediation with input from business and IT.

TECHNOLOGY OWNERS

- Coordinate with TLM to generate EOL remediation plans based on technology roadmaps
- Manage impacts from accepted Exception requests
- Assist driving adherence to TLM EOL and technology standards
- Collaborate with TLM to determine:
 - Current asset ownership
 - Missing EOL dates for enterprise technology assets and/or components

ENTERPRISE ARCHITECTURE

- Establish a Technology Adoption Framework Program
- Implement and manage a formal Technology Standards Management program as a Federated model
- Collaborate with IT Enterprise to establish IT asset lifecycle EOL/EOS (End-of-Support) targets not driven by vendor-supplied dates
- Identify, establish and enforce IT asset lifecycle requirements



APPLICATION DEVELOPMENT & SUPPORT

- Manage EOL remediation activities for application components within the application stack
- Maintain ownership and required configuration items (CI) for all their applications in the CMDB
- Coordinate with appropriate hardware support teams for hardware end-of-life remediation

ASSET MANAGEMENT (ITAM & CMDB)

- Enable automated discovery to streamline monitoring and reporting of EOL Compliance
- Improve TLM required data, missing EOL data, addressed by CMDB and ITAM teams with collaboration from vendors and TLM

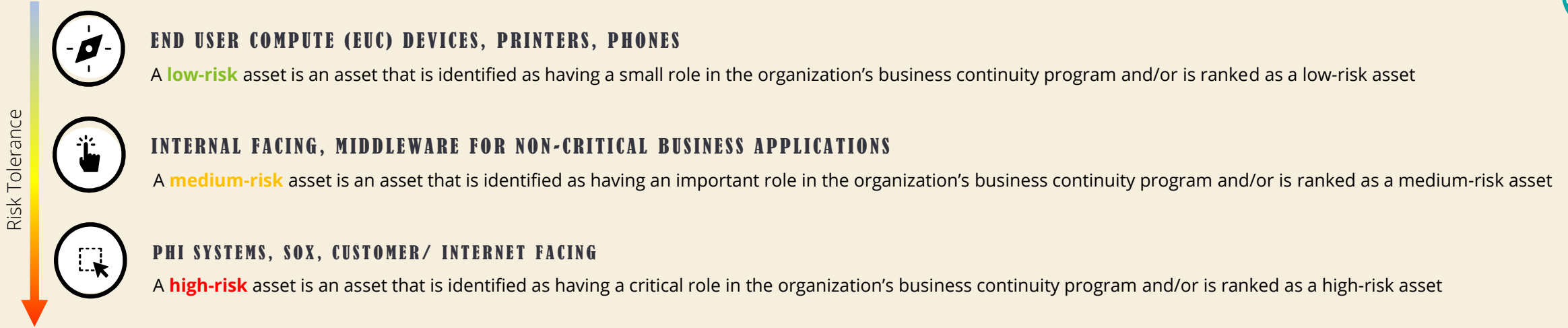
IT RISK

- Identify, quantify, and record risks generated by failure to remediate end-of-life technology
- Manage the risk remediation process, which includes the approval of exceptions



What does good look like - integrate TLM with IT Risk Management (ITRM)

Objective: Ability to assess the operational, financial, and information security risks created by end-of-life assets in the environment



FINANCIAL RISK

Post-warranty support purchased through Original Equipment Manufacturer (OEM), or Third-Party Maintenance is expensive and can exceed cost of replacement with non-EOL asset with OEM warranty/support

OPERATIONAL RISK

IT Assets may no longer be able to efficiently support daily operational activities as the organization and supported applications grow and change. Chance of failure increases as assets pass their Mean Time Between Failure (MTBF) ratings, which can cause application and service disruptions. In addition, ability to repair an EOL asset is more difficult, which can extend outages

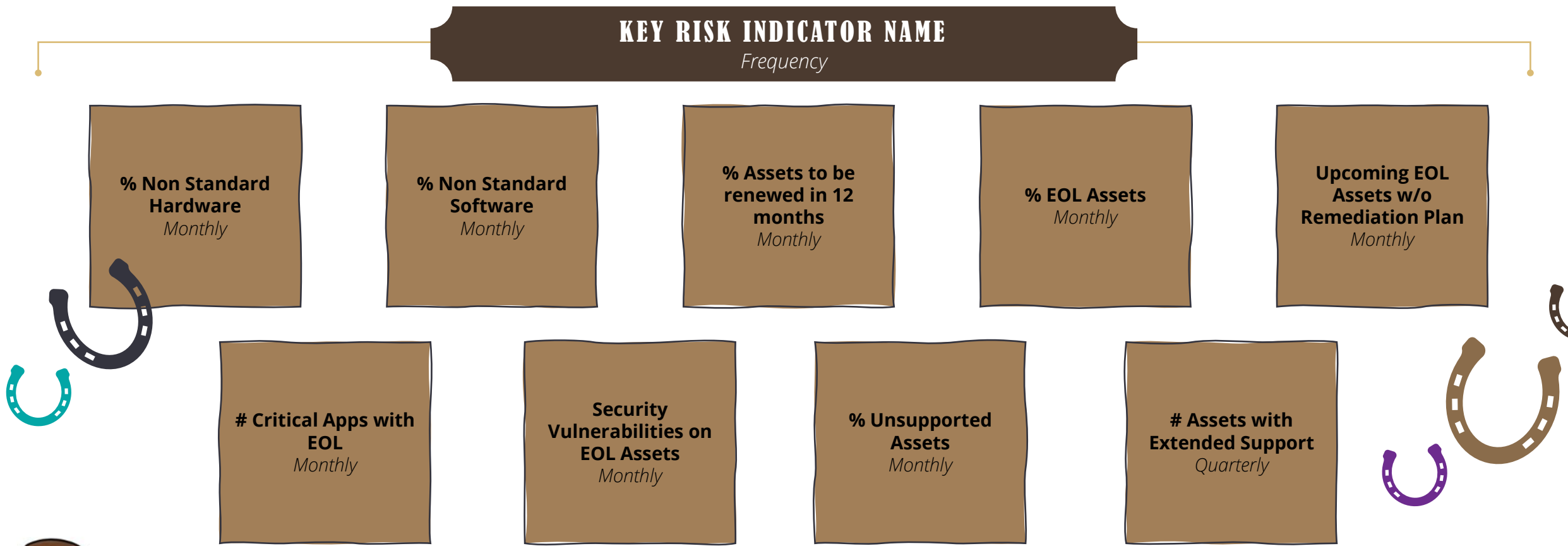
CYBER SECURITY RISK

IT Asset will no longer receive patches, bug fixes and upgrades. An estimated 1 in 3 of breaches today are a result of unpatched vulnerabilities. By allowing assets to reach EOL, where support is no longer available, organizations expose themselves to unknown vulnerabilities and greater risk



What does good look like - key risk indicators

Objective: Establish metrics and key risk indicators (KRI) that enables the organization to assess the effectiveness of the TLM program and its impact on the business



KRIs listed are a subset of recommended indicators. This is not an exhaustive list.



What does good look like – technology standards

Objective: Implement a technology standards management program that provides key benefits for the Technology Lifecycle Management capability and to the overall enterprise.

TECHNOLOGY STANDARDS MANAGEMENT

- **Map enterprise capability requirements to technology standards in collaboration with business and IT stakeholders**
 - **Establish strategic direction and technology standards** for hardware, software, and additional technology components for deployment within the enterprise
 - **Define and manage the process for evaluating new or emerging technologies**, along with the **exception process** for non-standard technology requests and a maintained library of evaluation results
 - **Identify, establish, and enforce IT asset lifecycle requirements** for many IT related hardware and software products in collaboration with TLM, external vendors and suppliers, and enterprise stakeholders
 - **Develop a product rationalization framework** through coordination with business stakeholders
- **Implement a governance framework** managed by EA, with representation from Tech Owners, App Owners, IT Procurement, IT Risk, and TLM to manage and enforce the technology acquisition process

BENEFITS FOR TLM

- Reducing the likelihood of disparate technologies through establishment of a technology standards management program and enforcing IT asset lifecycle requirements, will help improve TLM's ability to plan and execute on EOL remediation
- Centralizing the technology standards catalog and exception process for acquiring non-standard technologies will help enable the consistent definition of technology ownership responsibilities as they pertain to the technology lifecycle

BENEFITS FOR THE ENTERPRISE

- Improved management and tracking of IT assets
- Decreased security risk by updating assets in a timely manner
- Reduced operational risk and technology debt by aligning operational and developmental efforts to supported standards or accepted exceptions while prioritizing M&A assets
- Reduced technology sprawl will result in lower support costs for the enterprise
- Standardized, collaborative process to identifying and evaluating emerging technologies
- Improved ability to track technology dependencies in the application stack



Illustrative TLM maturity roadmap – 3 Years and beyond

YEAR ONE

- Define technical debt scope for TLM (EOL) and align with Senior Leadership by:
 - Coordinating with IT Service Management (ITSM) teams to improve data completeness and quality
 - Pursuing opportunities for automation
 - Identifying and updating technology asset data for those missing EOL dates to improve TLM's ability to identify EOL assets
- Implement a formal technology currency standard model, managed by TLM (EOL)
 - Version management (N, N-1)
- Incorporate cloud migration into remediation planning and standards

YEAR TWO

- Develop an IT Risk-managed EOL remediation exception process for a formal risk assessment
- Enhance EOL remediation performance of TLM metrics and prioritization
- Establish a technology adoption framework program, managed by EA

YEAR THREE

- Review and reassess TLM goals and objectives to determine additional areas for improvement
- Continue identifying strategic opportunities for improving TLM maturity through automation, improved reporting, etc.



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

