# TBM & NIST Integration

**October 4, 2023**

8am PT | 11am ET | 4pm BST | 5pm CEST

Standards Open Forum

TBM COUNCIL

**Ed Hayman**
TBM Architect &
Technical Advisor
TBM Council

**Antonio "Toney" Mitchell**
Deputy Associate CIO,
IT Strategy & Policy
Office of Personnel Management

**Mina Han**
Principal
REI Systems

**We will begin shortly!**

# Topics for Today's Session (90 mins)

**0:00 – 0:20** | TBM Council & Standards Committee Overview & 2023 Charter

**0:20 – 0:30** | NIST & TBM Alignment

**0:30 – 0:50** | Public Sector Involvement & OPM Pilot

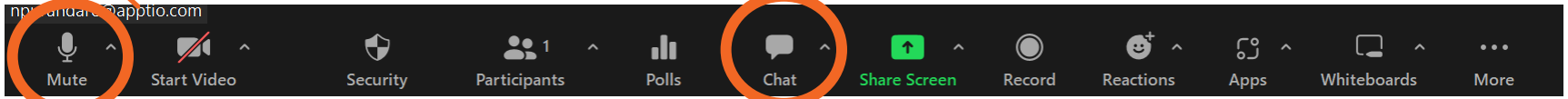
**0:50 – 1:10** | Cyber Security TCO

**1:10 – 1:25** | Closing thoughts

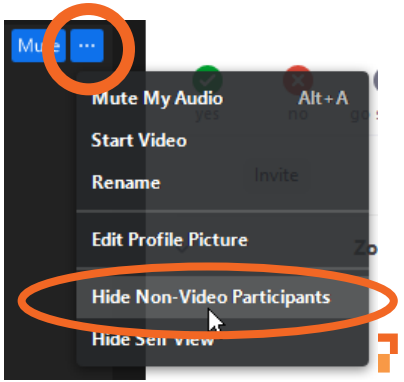
**1:25 – 1:30** | Upcoming TBM Council Activities & Wrap Up

# Zoom Meeting Recording / Questions

- This session is being recorded.
- **Please unmute your audio to ask a question – jump on in! OR you can submit questions via the Chat button in your Zoom toolbar**




- Please change your view to **Hide Non-Video Participants** by clicking on the ellipsis (“dot-dot-dot”) in your Zoom profile.






TBM COUNCIL

# Copyright ©2022 Technology Business Management Council, Ltd.



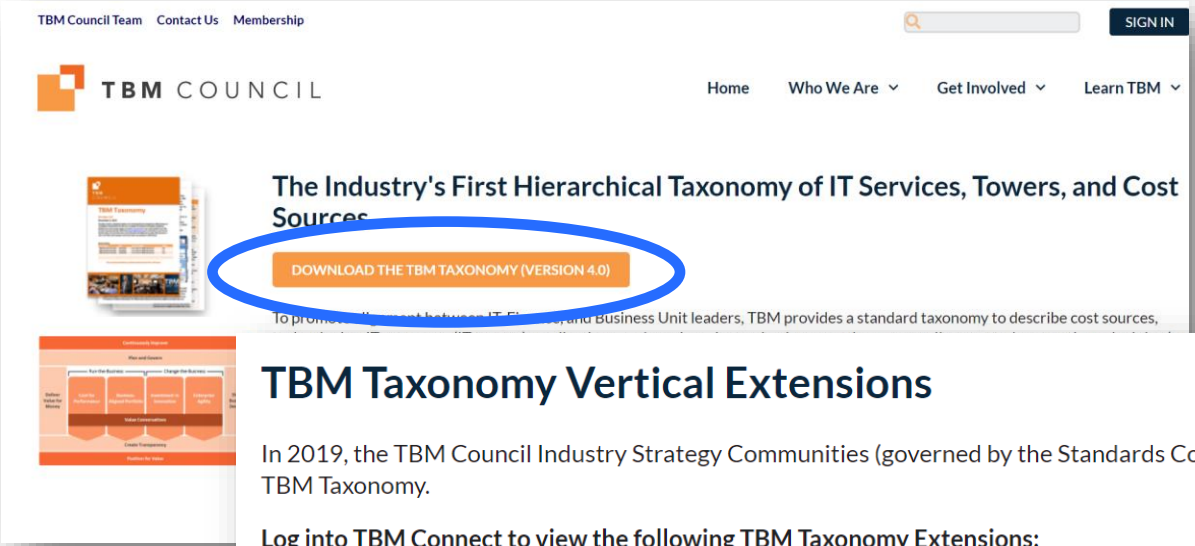
TBM COUNCIL

# TBM Standards Committee Members

- **Voting Members**
  1. Atticus Tysen, Intuit (Chair)
  2. Akin Ayemobola, USAA
  3. Brant Nyman, NCR
  4. Carl Stumpf, Nike
  5. Carollyn Gehrke, John Deere
  6. Chris Curtis, Freddie Mac
  7. John Wilson, MetLife
  8. Kelley Wendelborn, Lowe's Companies
  9. Lee Hawley, Red Hat
  10. Matthew Erickson, Hub International Limited
  11. Antonio “Toney” Mitchell, Office of Personnel Management
  12. Brian Bell, Church & Dwight
  13. Michael Mazza, Morgan Stanley
  14. Daniel Donalson, Childrens Health Dallas
  15. Adrian Thivy, Origin Energy (APAC)

- **Non-Voting Members**
  1. Jon Sober, Author, Practical Technology Business Management
  2. Kathy Rudy, ISG
  3. Laura Szakmary, US General Services Administration
  4. Matt Temple, Accenture
  5. Mina Han, REI Systems
  6. Quinn Abraham, Maryville
  7. Stephanie Roe, State of Washington
  8. Tim Pietro, Rego Consulting

# Improved Accessibility to TBM Taxonomy Materials




**Coming Soon!**
**Utilities Extension**

## TBM Taxonomy Vertical Extensions

In 2019, the TBM Council Industry Strategy Communities (governed by the Standards Committee) each created an extension to the TBM Taxonomy.

**Log into TBM Connect to view the following TBM Taxonomy Extensions:**

GOVERNMENT | INSURANCE | BANKING | HEALTHCARE | MANUFACTURING

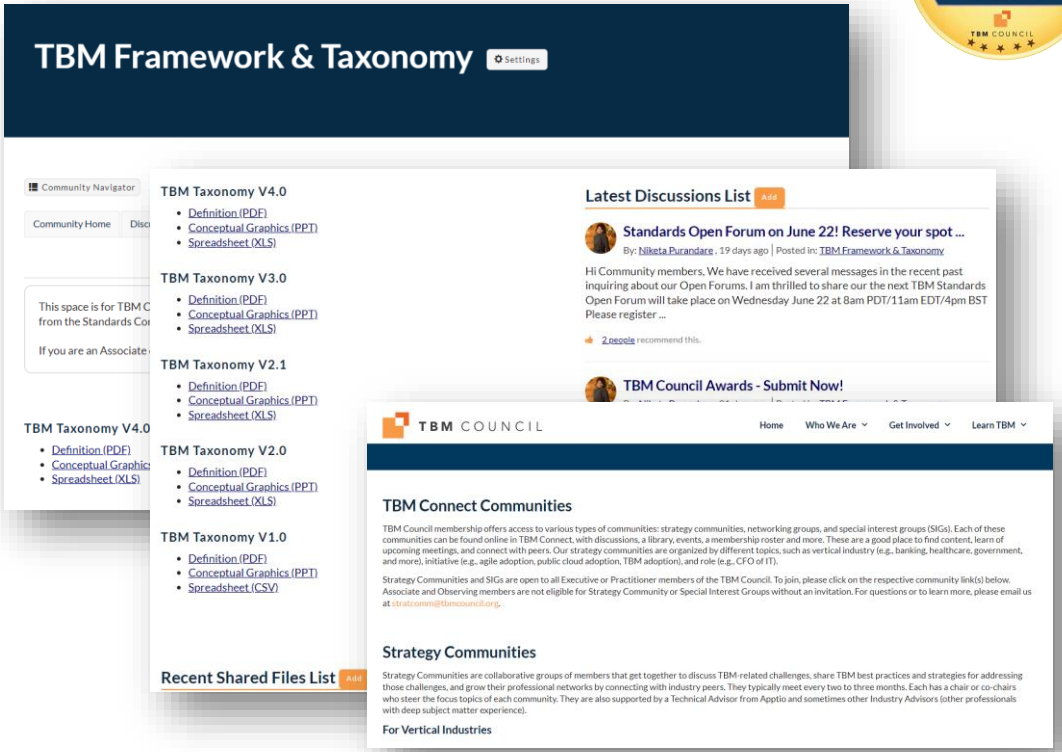
# Join the TBM Council

- Join online at http://www.tbmcouncil.org/join
  - Connect with peers from our member community
  - Attend our annual global conference and regional events and networking groups
  - Access best practices and other resources on our community site
  - Take advantage of the TBM Council's education offerings and certification program
  - Take pride in contributing to the rapidly growing discipline of Technology Business Management


# Be Sure to Engage Online

- Join on TBM Connect to:
  - Access past meetings recordings and presentations
  - Engage with the 400+ other Strategy Community members
  - Receive invitations to future meetings
  - Stay up to date with Community discussions

[Join the conversation on TBM Connect]



TBM COUNCIL

# Collaborate to discuss TBM-related challenges, share TBM best practices, and strategies

Join Now

# Standards Committee 2023 Charter

Mission:
Promote standard frameworks, processes and taxonomy for TBM; show alignment to new & existing operating models driven by evolving trends in technology.

Deliverables:

- ❑ Continued ServiceNow CSDM alignment
- ❑ TBM: Moving Beyond Costs
- ❑ Agile & TBM alignment
- ❑ TBM Taxonomy alignment to Security Framework (NIST)

# NIST Framework & TBM Taxonomy Alignment

Ed Hayman & Mina Han

# Why?

## Government agencies asked to report out on Cyber Security spend

- Requirement: break out Cyber Security spend based on NIST, a security framework
- Desire: use existing IT cost models as source of cyber security spend
- Government Strategy committee mapped the NIST Framework to TBM Taxonomy in 2022
- TBMC Standard Committee reviewed and updated in 2023

# NIST Framework

*Lifecycle to understand, manage, and reduce cybersecurity risks*

The NIST Cybersecurity Framework helps:

- Determine activities important to **assure critical operations and service delivery**
- **Prioritize investments** and **maximize impact of dollars** spent on cybersecurity
- **Improves communication, awareness, and understanding** across stakeholders by providing a common language
- Supports **acquisition needs** between a buyer/supplier

**Where to Find?**

- NIST Cybersecurity Framework
- Framework Version 1.1
- NIST Special Publication 1271, Getting Started with the Cybersecurity NIST Framework: A Quick Start Guide

# NIST – Comprehensive and Detailed Framework

**NIST draws upon security resources from several existing frameworks**

| Function | Category | Subcategory | Informative References |
|---|---|---|---|
| **IDENTIFY (ID)** | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | **CIS CSC** 1<br>**COBIT 5** BAI09.01, BAI09.02<br>**ISA 62443-2-1:2009** 4.2.3.4<br>**ISA 62443-3-3:2013** SR 7.8<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2<br>**NIST SP 800-53 Rev. 4** CM-8, PM-5 |
| | | **ID.AM-2:** Software platforms and applications within the organization are inventoried | **CIS CSC** 2<br>**COBIT 5** BAI09.01, BAI09.02, BAI09.05<br>**ISA 62443-2-1:2009** 4.2.3.4<br>**ISA 62443-3-3:2013** SR 7.8<br>**ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1<br>**NIST SP 800-53 Rev. 4** CM-8, PM-5 |
| | | **ID.AM-3:** Organizational communication and data flows are mapped | **CIS CSC** 12<br>**COBIT 5** DSS05.02<br>**ISA 62443-2-1:2009** 4.2.3.4<br>**ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 |



TBM COUNCIL

# NIST Components


**Identify**

Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities

**Protect**

Develop and implement the appropriate safeguards to ensure delivery of services

**Detect**

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event

**Respond**

Develop and implement the appropriate activities to take action regarding a detected cybersecurity event

**Recover**

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

# TBM Taxonomy

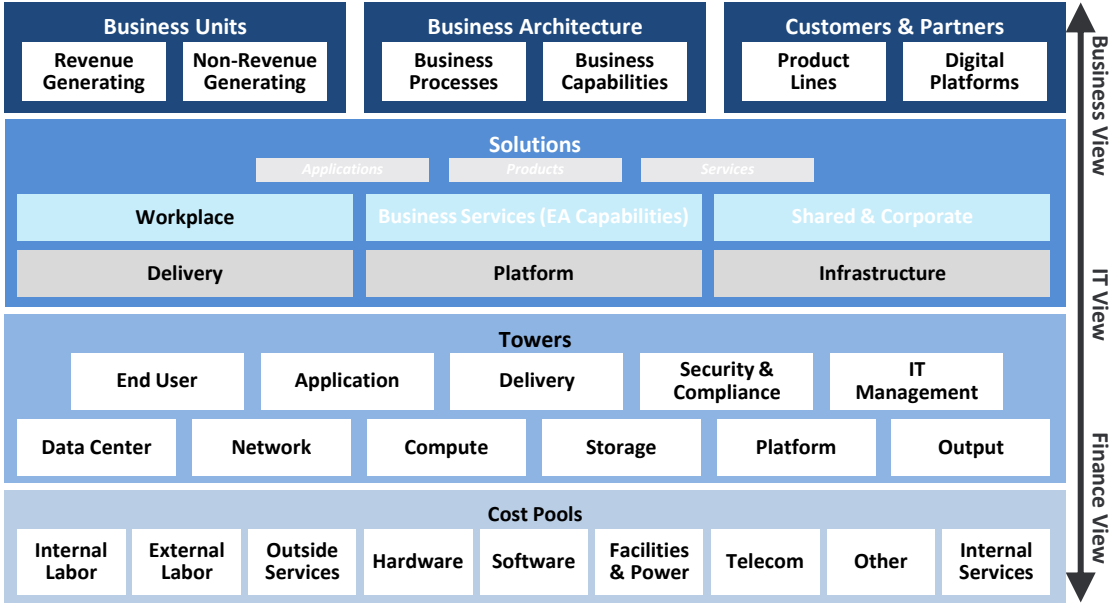
*TBM provides a standard taxonomy and framework to analyze cost sources, technologies, IT resources (Towers), applications, and solutions*

**Business:**
Describes the consumers of the solutions, the business processes and capabilities enabled, or the products/platforms provided

**Solutions:**
**(Alignment to NIST)**
Describes what IT delivers to end consumers: business leaders, end users and often external parties such as customers and partners.

**Towers:**
Describes the technology functions
supported by IT spend in terms & groupings relevant to the owners and consumers of those functions.

**Cost Pools:**
Describes the type of spending using terms and groupings relevant to both IT and finance.





TBM COUNCIL

# NIST & TBM Intersection

## *Challenges*

- **Reporting is difficult** for agencies to respond to (multiple data calls, audits, etc.)
- **Need to convey the value** of using the TBM framework
- Cybersecurity teams are more **focused on outcomes vs. cost to deliver**

## *Value*

Aligning the TBM and NIST Frameworks can:

- **Automate** data calls and audit responses
- Identify the **cost** of Cybersecurity and **how it is being used**
  - **Reduce duplication**
  - **Identify gaps**
  - **Understand capabilities**

# NIST to TBM Crosswalk

## NIST

- Identity
- Protect
- Detect
- Respond
- Recover

## TBM Security & Compliance

- Identity & Access Management
- Security Awareness
- Cyber Security & Incident Response
- Threat & Vulnerability Management
- Data Privacy & Security
- Governance, Risk & Compliance
- Business Continuity & Disaster Recovery

# Government Strategy Committee Approach

1

Gather TBM community **feedback** and guidance

Conduct **environmental scan** to gain understanding of the NIST Framework, relevant resources, how it is used, by whom, and why

Discover

2

Convene **cohort** to address issues

Identify appropriate taxonomies and **develop crosswalk mapping**:

- NIST (v1.1)
- TBM (v4.0)

Propose

3

Analyze **gaps and overlaps**

Develop **findings and recommendations** to provide a comprehensive taxonomy

Analyze

4

**Validate** proposal with TBM Standards Committee and Community to ensure usability

**Confirm** output with POC from **NIST**

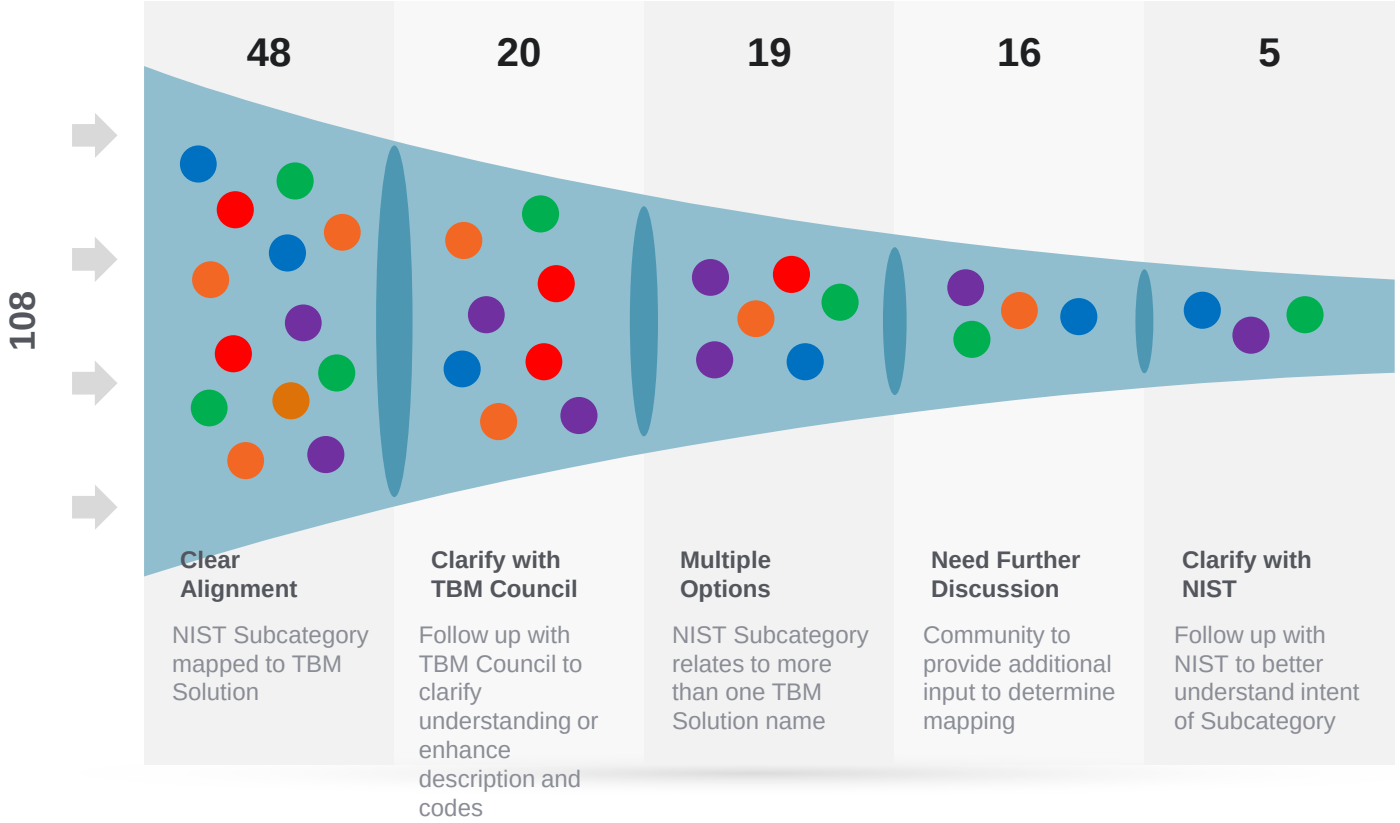
* In Progress

Validate



TBM COUNCIL

# Findings and Recommendations




**Publish Taxonomy and Crosswalk**

TBM taxonomy and crosswalk updated as needed and published

# Standard Committee sub-committee established for NIST/TBM Alignment

Sub-Committee lead

- Antonio “Toney” Mitchell, Office of Personnel Management

Members

- Mina Han, REI Systems
- Michael Mazza, Morgan Stanley
- Chris Karalis, ISG
- Jon Sober, Certified Information Systems Auditor, author Practical TBM
- Ed Hayman, Technical Advisor, Apptio

# NIST / TBM Alignment Deliverables

- Updated NIST – TBM Taxonomy Crosswalk (aka ‘mappings’)
- TBM Taxonomy v4.1
  - Updates to categories and definitions to better align to NIST
  - *Assess other taxonomy refinements*
- Cyber Security “Total Cost” model guidelines
  - Capture security-related activities specific to operational areas

# IDENTIFY Sub-Category Mappings

| Function | Category | Subcategory | TBM Service/ Solution Type | TBM Service/Solution Category | TBM Service/Solution Name |
|---|---|---|---|---|---|
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-1:** Physical devices and systems within the organization are inventoried | Delivery | Operations | IT Service Management |
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-2:** Software platforms and applications within the organization are inventoried | Delivery | Operations | IT Service Management |
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-3:** Organizational communication and data flows are mapped | Delivery | Strategy & Planning | Enterprise Architecture |
| IDENTIFY (ID) | **Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | **ID.AM-4:** External information systems are catalogued | Delivery | Operations | IT Service Management |

# PROTECT Sub-Category Mappings

| Function | Category | Subcategory | TBM Service/ Solution Type | TBM Service/Solution Category | TBM Service/Solution Name |
|---|---|---|---|---|---|
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes | Delivery | Security & Compliance | Identity & Access Management |
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-2:** Physical access to assets is managed and protected | Infrastructure | Data Center | Enterprise Data Center<br><br>Other Data Center |
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-3:** Remote access is managed | Delivery | Security & Compliance | Identity & Access Management |
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. | **PR.AC-4:** Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | Delivery | Security & Compliance | Identity & Access Management |
| PROTECT (PR) | **Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized | **PR.AC-5:** Network integrity is protected (e.g., network segregation, network segmentation) | Infrastructure | Network | All Network Security Names |

# DETECT Sub-Category Mappings

| Function | Category | Subcategory | TBM Service/ Solution Type | TBM Service/Solution Category | TBM Service/Solution Name |
|---|---|---|---|---|---|
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | **DE.AE-2:** Detected events are analyzed to understand attack targets and methods | Delivery | Security & Compliance | Cyber Security & Incident Response |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors | Delivery | Operations | Event Management |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | **DE.AE-4:** Impact of events is determined | Delivery | Security & Compliance | Cyber Security & Incident Response |
| **DETECT (DE)** | **Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood. | **DE.AE-5:** Incident alert thresholds are established | Delivery | Operations | Event Management |
| **DETECT (DE)** | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-1:** The network is monitored to detect potential cybersecurity events | Delivery | Operations | Event Management |
| **DETECT (DE)** | **Security Continuous Monitoring (DE.CM):** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. | **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events | Infrastructure | Data Center | Enterprise Data Center<br><br>Other Data Center |

# RESPOND Sub-Category Mappings

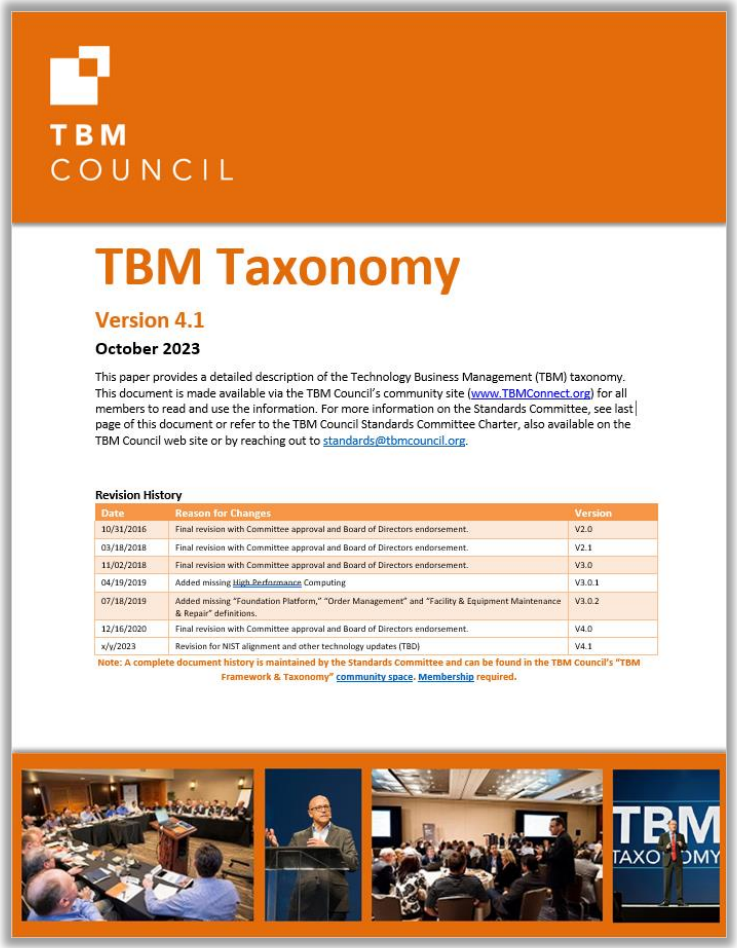
| Function | Category | Subcategory | TBM Service/ Solution Type | TBM Service/Solution Category | TBM Service/Solution Name |
|---|---|---|---|---|---|
| RESPOND (RS) | **Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents. | **RS.RP-1:** Response plan is executed during or after an incident | Delivery | Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-1:** Personnel know their roles and order of operations when a response is needed | Delivery | Security & Compliance | Security Awareness |
| RESPOND (RS) | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-2:** Incidents are reported consistent with established criteria | Delivery | Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-3:** Information is shared consistent with response plans | Delivery | Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-4:** Coordination with stakeholders occurs consistent with response plans | Delivery | Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). | **RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness | Shared & Corporate<br><br>Delivery | Corporate Communications<br><br>Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | **RS.AN-1:** Notifications from detection systems are investigated | Delivery | Security & Compliance | Cyber Security & Incident Response |
| RESPOND (RS) | **Analysis (RS.AN):** Analysis is conducted to ensure effective response and support recovery activities. | **RS.AN-2:** The impact of the incident is understood | Delivery | Security & Compliance | Cyber Security & Incident Response |

# IDENTIFY Sub-Category Mappings

| Function | Category | Subcategory | TBM Service/ Solution Type | TBM Service/Solution Category | TBM Service/Solution Name |
|---|---|---|---|---|---|
| RECOVER (RC) | **Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. | **RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident | Delivery | Security & Compliance | Business Continuity & Disaster Recovery |
| RECOVER (RC) | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-1:** Recovery plans incorporate lessons learned | Delivery | Security & Compliance | Business Continuity & Disaster Recovery |
| RECOVER (RC) | **Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities. | **RC.IM-2:** Recovery strategies are updated | Delivery | Security & Compliance | Business Continuity & Disaster Recovery |
| RECOVER (RC) | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | **RC.CO-1:** Public relations are managed | Shared & Corporate | Risk, Audit & Compliance | Breach Management & Remediation |
| RECOVER (RC) | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | **RC.CO-2:** Reputation is repaired after an incident | Shared & Corporate | Corporate Communications | Stakeholder Relations<br><br>Government Relations<br><br>External Communications |
| RECOVER (RC) | **Communications (RC.CO):** Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). | **RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams | Delivery | Security & Compliance | Business Continuity & Disaster Recovery |

# TBM Taxonomy 4.1 Update

- Definition updates to drive better clarity and alignment with NIST categories
- Primarily focused on Security & Compliance Sub-Tower and Service Categories
- Other “operational” towers covered in a supplemental document



TBM COUNCIL

## TBM Taxonomy

### Version 4.1

**October 2023**

This paper provides a detailed description of the Technology Business Management (TBM) taxonomy. This document is made available via the TBM Council’s community site (www.TBMConnect.org) for all members to read and use the information. For more information on the Standards Committee, see last page of this document or refer to the TBM Council Standards Committee Charter, also available on the TBM Council web site or by reaching out to standards@tbmcouncil.org.

**Revision History**

| Date | Reason for Changes | Version |
|---|---|---|
| 10/31/2016 | Final revision with Committee approval and Board of Directors endorsement. | V2.0 |
| 03/18/2018 | Final revision with Committee approval and Board of Directors endorsement. | V2.1 |
| 11/02/2018 | Final revision with Committee approval and Board of Directors endorsement. | V3.0 |
| 04/19/2019 | Added missing High Performance Computing | V3.0.1 |
| 07/18/2019 | Added missing “Foundation Platform,” “Order Management” and “Facility & Equipment Maintenance & Repair” definitions. | V3.0.2 |
| 12/16/2020 | Final revision with Committee approval and Board of Directors endorsement. | V4.0 |
| x/y/2023 | Revision for NIST alignment and other technology updates (TBD) | V4.1 |

**Note: A complete document history is maintained by the Standards Committee and can be found in the TBM Council’s “TBM Framework & Taxonomy” community space. Membership required.**

# Public Sector Involvement & OPM Pilot

Antonio “Toney” Mitchell

# Pilot Objectives

1. Create **better transparency for better reporting**
2. Understanding data is the **cornerstone of making informed decisions and extracting valuable insights**
3. Approaching **consistency and compliance**

# OPM Pilot Approach

## Pilot Kickoff

- Articulate scope and potential outcomes
- Identify current data sets and tools
- Propose roadmap for pilot completion

## Data Mapping

- Obtain FY23-25 Cybersecurity budget data
- Utilize TBM Taxonomy mapping to align with the NIST Framework
- Finalize FY23-25 Cybersecurity NIST & TBM mappings

## Data Utilization

- Cybersecurity IT investment management
- OCIO visualization toolsets & applications
- Future OMB, GAO, OIG data request

## Decision Making

- Socialization of Cybersecurity compliance costs within the enterprise
- Enhance Cybersecurity benchmarking, trend analyses, forecasting and tradeoffs
- Articulate chargeback and showback fees for future budget requests

# Pilot Benefits

**Efficiency**

Easier to analyze, reducing the time and effort required to clean and prepare data for insights and reporting

**Accuracy**

Identify and rectify discrepancies and errors in data, leading to higher data accuracy and trust, which is crucial for reliable reporting and forecasting

**Management**

Communicate the value of IT to stakeholders by focusing on cost transparency, delivery of value, identification of the total cost of IT and shaping the demand for IT services

**Decision Making**

Extend TBM analysis to provide actionable recommendations to enable data-driven IT decisions

**Compliance**

Maintain compliance with Executive & Legislative Cybersecurity mandates

- Quick data response based **on TBM framework or NIST framework**
- Leverage for **Budget reporting or additional federal reporting**

# Expected Outcomes

01 **Identify and confirm** Enterprise Cybersecurity portfolio costs per the NIST and TBM Frameworks

02 Use data in the **formulation** of the Cybersecurity Service Catalog

03 **Generate value conversations** regarding Cybersecurity trends, policy mandates, and risks

04 **Simplify** annual **Cyber Budget Data Request (BDR)** reporting

# Next Steps

1. TBM community to provide feedback on areas needing further discussion
2. Complete proof of concept (PoC) to test applicability of crosswalk and expand to others
3. Coordinate with TBM Council Standards Committee and NIST
4. Publish final mapping and PoC results

# Identifying Cyber Security Costs

Ed Hayman & Mina Han

# SOLUTIONS (v4.0)

TBM COUNCIL
Standards Committee

## Delivery

Security & Compliance is a primary area

### Strategy & Planning

- Technology Business Management
  - *IT Planning*
  - *IT Finance & Costing*
  - *IT Billing*
  - *Business Value*
  - *Metrics & Benchmarking*
  - *Strategy Management (new)*
  - *Service Portfolio management*
  - *Service Catalog management*
  - *Service Level management*
  - *Availability management*
- Innovation & Ideation
  - *New technology solutions*
  - *Incubation services*
- Enterprise Architecture
  - *Business architecture*
  - *Information architecture*
  - *Application architecture*
  - *Infrastructure architecture*
- Program, Product & Project Management
  - *Portfolio investment planning*
  - *Project planning & delivery*
  - *Continuous planning & delivery*
- Business Solution Consulting
  - *Business Relationship management*
  - *Business Process analysis*
  - *Technology solution analysis*
  - *Demand management*
- IT Vendor Management
  - *Vendor Selection / Negotiation*
  - *Procurement*

### Development

- Design & Development
  - *Custom build*
  - *Package configuration*
  - *SaaS configuration*
- System Integration
  - *On-prem application integration*
  - *SaaS integration*
- Modernization & Migration
  - *App re-architecture*
  - *Data migration*
  - *Infra re-architecture*
- Testing
  - *Functional testing*
  - *Integration testing*
  - *Performance testing*
  - *Usability testing*

### Support

- Service Desk
  - *Central help desk*
  - *Deskside support*
  - *Tech bar support*
  - *IT knowledge management*
  - *Request fulfillment*
- Application Support
  - *Tier 2 app support (by app)*
  - *Tier 3 app support*
- IT Training
  - *Off-the-shelf productivity training*
  - *Business application training*
- Central Print
  - *Bill/invoice print*
  - *Publications*
  - *Automated post processing*

### Operations

- IT Service Management
  - *Incident management*
  - *Problem management*
  - *Change management*
  - *Asset management (CMDB)*
- Event Management
  - *Network monitoring*
  - *System monitoring*
  - *Application monitoring*
  - *Usage analytics*
  - *Logging analytics*
- Scheduling
  - *Batch processing*
- Capacity Management
  - *Storage capacity*
  - *Compute capacity*
  - *Data Center capacity*
- Deployment & Administration
  - *Software distribution*
  - *Config administration*
  - *Patch management*

### Security & Compliance

- *Identity & Access Management*
  - Authentication/Authorization
  - Identity Management
  - Identity Governance & Administration
  - Privileged Access Management
  - Certificate Management
- *Security Awareness*
  - Security Training
  - Security Advisory
  - Security Policies and procedures
- *Cyber Security & Incident Response*
  - Cyber Security Monitoring
  - Security Incident Response
- *Threat & Vulnerability Management*
  - Application Vulnerability Management
  - Infrastructure Vulnerability Management
  - Network/Endpoint Security
- *Data Privacy & Security*
  - Data Classification & identification
  - Data loss prevention
  - Data encryption
  - Database security
- Governance, Risk & Compliance
  - *Risk management*
  - *Policy management*
  - *Policy tracking*
  - *Data governance*
- Business Continuity & Disaster Recovery
  - *Business continuity policies*
  - *Business resiliency plans*
  - *DR procedures & exercises*
  - *DR facilities*
  - *Office continuity facilities*

However, many other areas provide security related support

# TBM Taxonomy & NIST Supplement (v0.2)

- Summary of NIST framework and purpose
- Summary of TBM Taxonomy
- Benefits of using TBM & NIST to Understand Cyber Security Costs
- Cyber Security TCO and Cost Allocation Approaches
- Security related activities by Tower / Service Category

TBM COUNCIL

## TBM Taxonomy & NIST

### Version 0.2 (DRAFT)

**October 2023**

This paper provides a summary overview of the NIST cyber security framework with a detailed mapping of cyber security activities and technologies organized under the TBM Taxonomy. The purpose is to help organizations understand the costs vs. risk profile of their technology investments related to cyber security. This document is made available via the TBM Council's community site (www.TBMConnect.org) for all members to read and use the information. For more information on the Standards Committee, see last page of this document or refer to the TBM Council Standards Committee Charter, also available on the TBM Council web site or by reaching out to standards@tbmcouncil.org.

**Revision History**

| Date | Reason for Changes | Version |
|---|---|---|
| 10/04/2023 | Draft version in preparation for RFC at TBM Conference 2023 | 0.2 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Note: A complete document history is maintained by the Standards Committee and can be found in the TBM Council's "TBM Framework & Taxonomy" community space. Membership required.

# Cyber Security TCO and Cost Allocations

## Cost Center Identification

- **Direct Costs**: Identify departments or teams specifically dedicated to cybersecurity, such as the Information Security or Cybersecurity departments. All expenditures from these centers, including salaries, tools, licenses, and overhead, are direct costs.
- **Indirect Costs**: Identify other departments that have roles in security but not as their primary function, such as the technology operations departments or the application development and support teams. Apportion a percentage of their costs based on the estimated amount of time or resources they dedicate to security-related activities.

# Cyber Security TCO and Cost Allocations

## Labor Cost Allocation

- **Time Tracking**: Implement tools or systems to track the time employees spend on security-related tasks. This can be done through specialized time-tracking software, work management software, or integrated task management systems.  To implement, create security-specific activities.
- **Role-based Estimation**: For positions where time-tracking might be challenging, allocate costs based on role or job description. For instance, if a system administrator spends approximately 20% of their time on security patches and updates, then 20% of their compensation can be allocated to security costs.

# Cyber Security TCO and Cost Allocations

## Vendor/Supplier Cost Allocation

- **Direct Vendor Costs**: List all vendors supplying cybersecurity solutions, software, or services. The entirety of these costs can be directly allocated.
- **Shared Service Costs**: For vendors that supply a mix of services, some of which are security-related, break down their invoices or cost structures to determine the portion associated with cybersecurity. This might involve discussions with the vendor or a deep dive into the contract terms.

# Cyber Security TCO and Cost Allocations

- **Project-based Allocation:** For projects that enhance security (like the implementation of new security tools), allocate all related costs, including the associated labor and vendor costs, to cybersecurity expenditures.

- **Training & Awareness Programs:** All costs associated with security training, seminars, workshops, and awareness campaigns should be included. This should cover both external training fees and the internal time employees spend engaged in these activities.

- **Incident Response & Recovery Costs:** In the unfortunate event of a security breach or incident, all related costs, including forensic investigations, recovery operations, PR efforts, and potential legal fees, should be categorized under cybersecurity costs.

# Mapping TBM Operatio

## TBM & Operational Activities

### Virtual Servers

- **Hypervisor Security**: Harden and secure the hypervisor l unauthorized access and vulnerabilities.
- **Virtual Network Isolation**: Segregate virtual networks to surface.
- **Snapshot Security**: Secure and manage snapshots to pr unauthorized data access.
- **Guest OS Hardening**: Harden the guest operating systen virtual machines.
- **Encryption**: Implement disk and data-at-rest encryption fo
- **Resource Monitoring**: Keep track of resource utilization t anomalies that might indicate a security issue (e.g., a DoS
- **Vulnerability Scanning**: Regularly scan virtual machines vulnerabilities.

### Security-related Activities

Specific security-related activities and operational tasks can be used to map labor effort and vendor products and services to the NIST categories. The following sections identify specific types and examples of security and security-related activities for each of the TBM Taxonomy Towers and/or Service Categories and has been mapped to the NIST framework.

### Infrastructure

#### Compute

Managing security for different computing environments—be it physical servers, virtual servers, or serverless compute platforms—requires specialized attention and activities. Below is a list of security activities typically associated with the operational support of these environments.

#### Physical Servers

- **Physical Access Control**: Restrict and monitor physical access to servers using biometrics, card readers, or other secure authentication methods.
- **Environmental Controls**: Maintain temperature and humidity controls to protect physical servers.
- **Hardware Firewalls**: Implement hardware firewalls to protect the network perimeter where physical servers are located.
- **Firmware Updates**: Regularly update the server firmware to patch vulnerabilities.
- **Hardware Integrity Checks**: Regularly inspect server hardware for signs of tampering or failure.
- **Log Monitoring**: Monitor system logs for unauthorized or suspicious activities.
- **Backup Power Supplies**: Implement uninterruptible power supplies (UPS) and generators to ensure continuous operation.

#### Virtual Servers

- **Hypervisor Security**: Harden and secure the hypervisor layer against unauthorized access and vulnerabilities.
- **Virtual Network Isolation**: Segregate virtual networks to limit the attack surface.
- **Resource Monitoring**: Keep track of resource utilization to detect anomalies that might indicate a security issue (e.g., a DoS attack).
- **Snapshot Security**: Secure and manage snapshots to prevent unauthorized data access.
- **Guest OS Hardening**: Harden the guest operating systems running on virtual machines.
- **Vulnerability Scanning**: Regularly scan virtual machines for security vulnerabilities.
- **Encryption**: Implement disk and data-at-rest encryption for virtual servers.

#### Serverless Compute

- IAM Policies: Use Identity and Access Management (IAM) to define roles and permissions tightly.
- Code Review: Implement secure coding practices and review codes for vulnerabilities.
- API Gateway Security: Utilize secure APIs and implement rate limiting, authentication, and encryption.
- Event-Driven Security: Monitor and filter the events that trigger serverless functions.
- Data Validation: Implement proper input and output validation for serverless functions.

# Mapping TBM Operational Activities to NIST

## TBM & Operational Activities

### Common to All Environments

- **Auditing and Compliance**: Regularly audit environments for compliance with relevant regulations like GDPR, HIPAA, or PCI-DSS.
- **Security Training**: Train operational staff in best practices for each specific environment.
- **Multi-Factor Authentication (MFA)**: Require multiple forms of authentication before granting access.
- **Data Encryption**: Implement encryption for data-at-rest, data-in-transit, and, where possible, data-in-use.
- **Patch Management**: Regularly update all software components to patch known vulnerabilities.
- **Anti-Malware Solutions**: Deploy anti-malware solutions tailored for the specific compute environment.
- **Regular Backups**: Back up data and configurations regularly and ensure that backups are also secure.
- **Network Monitoring**: Continuously monitor network traffic for suspicious activities.
- **Incident Response**: Develop and regularly update an incident response plan tailored for each compute environment.
- **Disaster Recovery**: Have a disaster recovery plan in place and regularly test it to ensure effectiveness.

## NIST

- Identity
- Protect
- Detect
- Respond
- Recover

# Next Steps

- Refine and finalize deliverables for TBM Conference
- Publish and make available for “Request for Comment” in Austin
- Encourage TBM practitioners to seek security partners in your organization to review and provide input
- Review new NIST 2.0 Framework and provide feedback

TBM Conference

FinOps CloudyCon

23

# TBM Taxonomy Alignment to NIST Framework

Wednesday, Oct 25 | 4:00 pm | 45 Minutes

Register Today!

Get 20% off with TBM Council Member code
**MEMBER20**

www.tbmconference.org

# TBM Executive Foundation Course & Certification

A 4-day (16 hour) course and certification exam providing the essential knowledge that drives business transformation within IT by running a successful TBM program.

Sign up at www.tbmcouncil.org/events

## Recommended For:

- Heads of IT Finance (CFOs of IT, VP/Director of IT finance)
- TBM Program Directors (including aspiring program directors)
- Members of the Office of the CIO (OCIO)
- IT Vice Presidents (tower or silo leaders)
- Senior FP&A professionals supporting IT departments
- IT program and portfolio management (PPM/PMO) leaders
- Service management leaders
- IT strategy and transformation professionals
- Senior IT project managers
- IT governance and risk management professionals
- Independent consultants providing TBM, ITSM, IT4IT, GRC and related offerings

## What You Will Learn:

- The need for TBM and how it drives significant cost optimization and more effective business-technology management practices
- How to build a TBM program in your organization, including essential roles, responsibilities and skillsets
- The essential tools of TBM, including the framework, taxonomy, model, and metrics
- The key TBM disciplines including creating transparency, delivering value for money, shaping demand and planning for value
- The four value conversations of TBM and their associated management metrics
- How to drive continuous improvement with TBM
- How to apply the tools and disciplines of TBM beyond IT

DOWNLOAD THE COURSE SYLLABUS

# TBM Council Research

The TBM Council is committed to continuous research aimed at benefiting Council members and advancing TBM best practices, standards, education, and future activities and priorities.

## We value your feedback; It has an impact!

Surveys serve as the primary means of data collection and research, and they are administered through a variety of channels, including the TBM Council community platform, newsletters, LinkedIn, and online and in-person events like our yearly TBM Conference.

## Annual State of TBM Report

Each year we survey over 500+ respondents globally to assess the maturity, adoption, and impact of TBM. The survey covers a range of topics including, strategic planning, investment and transformation priorities, budgeting and financial controls, Cloud strategies, Agile delivery, and more.

Starting from 2023, comprehensive results will be available exclusively to Council members. These results include executive summaries, key findings, year-over-year trends, and recommendations.

2022 State of TBM Executive Summary

## Event Polls & Surveys

Available to both online and in-person event participants, these surveys target specific topics and areas of interest. They also collect feedback on agenda, content, and delivery.

## Engagement Surveys

Exclusive to practitioner and executive Council members, these monthly surveys focus on activities, capabilities, and practices across tech financials, Cloud, Agile/Portfolio Management, and more

## Council Pulse Surveys

Exclusive to practitioner and executive Council members, these quarterly surveys aim to assess the factors influencing membership, Council activity satisfaction, and promotions

## Topic Specific Polls & Surveys

Ad-hoc surveys targeting mixed audiences to gather specific data on topics like TBM salaries.

**For further information and to participate in these surveys, please visit tbmcouncil.org**

# Upcoming Events

TBM COUNCIL

About | Get Involved | Learn TBM | Showcase

Browse Events

Upcoming Events

On-Demand

**TBM EXECUTIVE PRIMER**

Technology Business Management (TBM) mer

3:00 PM me

the framework drive value the world's ions.

**TBM EXECUTIVE PRIMER**

Technology Business Management (TBM) Executive Primer

October 11 at 6:00 AM
Pacific Daylight Time

Virtual

Get introduced to the framework of disciplines that drive value conversations for the world's leading organizations.

**TBMCONNECT**

New Member Webinar

October 12 at 7:30 AM
Pacific Daylight Time

Virtual

In this webinar, we will review the history of the TBM Council, benefits of membership, and how you can become involved. TBM Council Membership is required to register. Become a member.

**TBM EXECUTIVE PRIMER**

Technology Business Management (TBM) Executive Primer – French

October 19 at 12:30 AM
Pacific Daylight Time

Virtual

Découvrez le cadre des disciplines qui guident les conversations de valeur d'organisations mondiales de premier plan

REGISTER NOW

**TBM Conference 23**
FinOps CloudyCon new

TBM Conference 2023

October 24 - October 27

Austin, TX

Join us and thousands of your peers from across the globe for TBM inspiration, education, and connection – all so you can continue to innovate to compete.

REGISTER NOW

**TBM-CLOUD PRIMER**

TBM-Cloud Primer

October 31 at 8:00 AM
Pacific Daylight Time

Virtual

Discover how leading enterprises use Technology Business Management (TBM) to manage the impact of public cloud consumption on applications, products, and services.

REGISTER NOW

# THANK YOU!