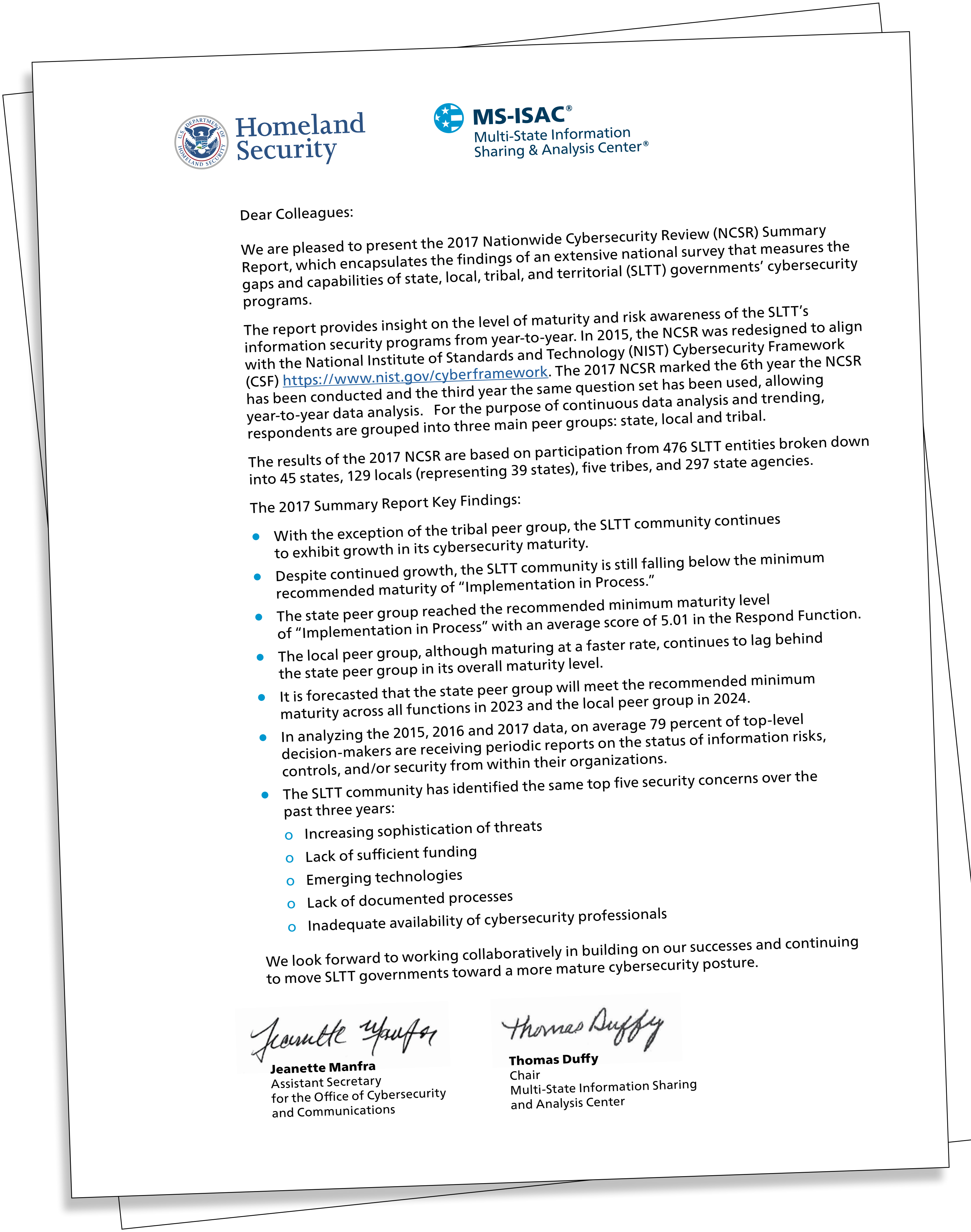
# Nationwide Cybersecurity Review:
Summary Report

2017

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®



Homeland Security

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Dear Colleagues:

We are pleased to present the 2017 Nationwide Cybersecurity Review (NCSR) Summary Report, which encapsulates the findings of an extensive national survey that measures the gaps and capabilities of state, local, tribal, and territorial (SLTT) governments' cybersecurity programs.

The report provides insight on the level of maturity and risk awareness of the SLTT's information security programs from year-to-year. In 2015, the NCSR was redesigned to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) https://www.nist.gov/cyberframework. The 2017 NCSR marked the 6th year the NCSR has been conducted and the third year the same question set has been used, allowing year-to-year data analysis. For the purpose of continuous data analysis and trending, respondents are grouped into three main peer groups: state, local and tribal.

The results of the 2017 NCSR are based on participation from 476 SLTT entities broken down into 45 states, 129 locals (representing 39 states), five tribes, and 297 state agencies.

The 2017 Summary Report Key Findings:

- With the exception of the tribal peer group, the SLTT community continues to exhibit growth in its cybersecurity maturity.
- Despite continued growth, the SLTT community is still falling below the minimum recommended maturity of "Implementation in Process."
- The state peer group reached the recommended minimum maturity level of "Implementation in Process" with an average score of 5.01 in the Respond Function.
- The local peer group, although maturing at a faster rate, continues to lag behind the state peer group in its overall maturity level.
- It is forecasted that the state peer group will meet the recommended minimum maturity across all functions in 2023 and the local peer group in 2024.
- In analyzing the 2015, 2016 and 2017 data, on average 79 percent of top-level decision-makers are receiving periodic reports on the status of information risks, controls, and/or security from within their organizations.
- The SLTT community has identified the same top five security concerns over the past three years:
  - Increasing sophistication of threats
  - Lack of sufficient funding
  - Emerging technologies
  - Lack of documented processes
  - Inadequate availability of cybersecurity professionals

We look forward to working collaboratively in building on our successes and continuing to move SLTT governments toward a more mature cybersecurity posture.

Jeanette Manfra

**Jeanette Manfra**
Assistant Secretary
for the Office of Cybersecurity
and Communications

Thomas Duffy

**Thomas Duffy**
Chair
Multi-State Information Sharing
and Analysis Center

## Acknowledgments

The Multi-State Information Sharing & Analysis Center® (MS-ISAC®) would like to thank everyone who has previously participated and continues to participate in the Nationwide Cybersecurity Review (NCSR). Your continued support in the NCSR helps us work towards our mission of improving the overall cybersecurity posture of the nation's state, local, tribal, and territorial governments.

We would also like to acknowledge and thank the members of the MS-ISAC Metrics Workgroup for their continued support. Their knowledge, expertise, and dedication assist in the continued success of the NCSR. A special "thank you" to these individuals who contributed to this report: Gary Coverdale, Jim Cusson, Amelia Gifford, Jenna Cole, Greg Bown, Dustin Stark, Linda Erickson, and Kim LaCroix.

*This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number, 2010-PD-123-000001, Mod #13.*

*The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.*

## Table of Contents

# Executive Summary

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

NASCIO
Representing Chief Information
Officers of the States

NATIONAL
ASSOCIATION
of COUNTIES NACo

In June of 2009, the U.S. Department of Homeland Security (DHS) was directed by the United States Congress to develop a cyber-network security assessment that would measure gaps and capabilities of state, local, tribal, and territorial (SLTT) governments' cybersecurity programs. The first Nationwide Cybersecurity Review (NCSR) was conducted in 2011 by DHS. In 2013, DHS partnered with the Multi-State Information Sharing & Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop and conduct the second NCSR. Since 2013, the NCSR has been conducted on an annual basis, and 2017 marks the sixth year the self-assessment has been conducted.

The results of the 2017 NCSR are based on participation from 476 SLTT entities broken down into 45 states, 129 locals (representing 39 states), five tribes, and 297 state agencies.

The NCSR provides insight on the level of maturity and risk awareness of the SLTT's information security programs from year to year. Using the results of this Report, DHS and MS-ISAC will continue to work with our partners on improving the overall cybersecurity maturity of the SLTT community.

## *2017 NCSR Key Findings*

**With the exception of the tribal peer group, the SLTT community continues to exhibit growth in its cybersecurity maturity.** 1

**Despite continued growth, the SLTT community is still falling below the minimum recommended maturity of "Implementation in Process."** 2

**The state peer group reached the recommended minimum maturity level of "Implementation in Process" with an average score of 5.01 in the Respond Function.** 3

**The local peer group, although maturing at a faster rate, continues to lag behind the state peer group in its overall maturity level.** 4

**It is forecasted that the state peer group will meet the recommended minimum maturity across all of the functions in 2023 and the local peer group in 2024.** 5

**In analyzing the 2015, 2016, and 2017 data, on average 79 percent of top-level decision-makers are receiving periodic reports on the status of information risks, controls, and/or security from within their organizations.** 6

**The SLTT community has identified the same top five security concerns over the past three years:**

- **Increasing sophistication of threats**
- **Lack of sufficient funding**
- **Emerging technologies**
- **Lack of documented processes**
- **Inadequate availability of cybersecurity professionals**

7

## Methodology

In 2015, the NCSR was redesigned to align with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) https://www.nist.gov/cyberframework. The Framework uses existing standards, guidelines, and best practices as guidance for organizations to manage and reduce cybersecurity risk. Through the realignment of the NCSR to the NIST CSF, MS-ISAC and DHS continue to develop a common understanding of the current cybersecurity management practices across SLTT governments.

### *Question Set*

The NCSR question set was built upon the NIST CSF Core, with some minor alterations. The Core consists of a collection of cybersecurity-related activities organized into five main functions: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**. Each of the five functions is subdivided into 22 categories and then further into 98 sub-categories.

The NCSR leverages the 98 sub-categories as the questions for the assessment with the addition of questions pertaining to privacy controls. For assessment purposes, the sub-categories provide enough details for organizations to identify actionable steps to improve their cybersecurity maturity and the ability to utilize pre-existing cross-references to best practices, standards, and requirements.

### *Targeted Participants*

The target audience for the NCSR are personnel within the SLTT community who are responsible for cybersecurity management within their organization.

### *NCSR Individual Reports*

Upon completion of the NCSR, the participant who completed the self-assessment has access to custom individual reports that are specific to their organization. All individual self-assessments and scores are kept confidential and anonymous. The reports allow participants to develop a benchmark to gauge year-to-year progress and continuously compare themselves against their peers.

### *Participation by Entity Type*

For the purposes of continuous data analysis and trending, respondents are grouped into three main peer groups: state, local, and tribal (**Figure 1**).

### *Peer Groups Defined*

The state peer group involves participation from among the 50 state governments.

The local peer group consists of any local government entity. This includes cities, counties, parishes, boroughs, K-12 public school districts, public libraries, associations, authorities, and the like.

The tribal peer group includes participation by any federally recognized tribe. Note: Historical data for the 2015 tribal peer group is not present as 2016 marks the first year there was enough participation from tribal governments to create a separate peer group.

In 2017, the MS-ISAC was able to capture and create an additional 18 sub-sector peer groups, which are discussed in further detail in **Appendix III**. Peer groups are based on participation from a minimum of five organizations per group.

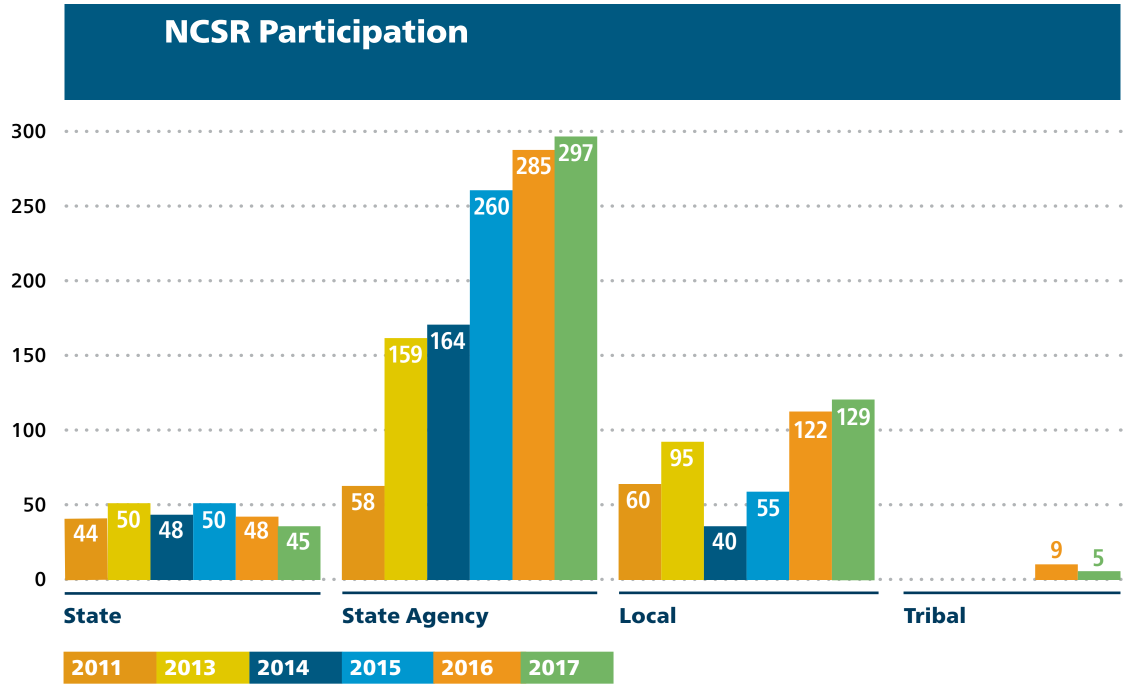


*Figure 1*

**Figure 1** represents SLTT participation in the NCSR over the years.

## NCSR Demographic Analysis

The following information was collected in doing an analysis on the demographic and post-survey responses from the 2015, 2016, and 2017 NCSRs.

**Do your top-level decision-makers receive periodic (at least annual) reports on the status of information risks, controls, and/or security from the departments, divisions, and/or agencies within your organization?**

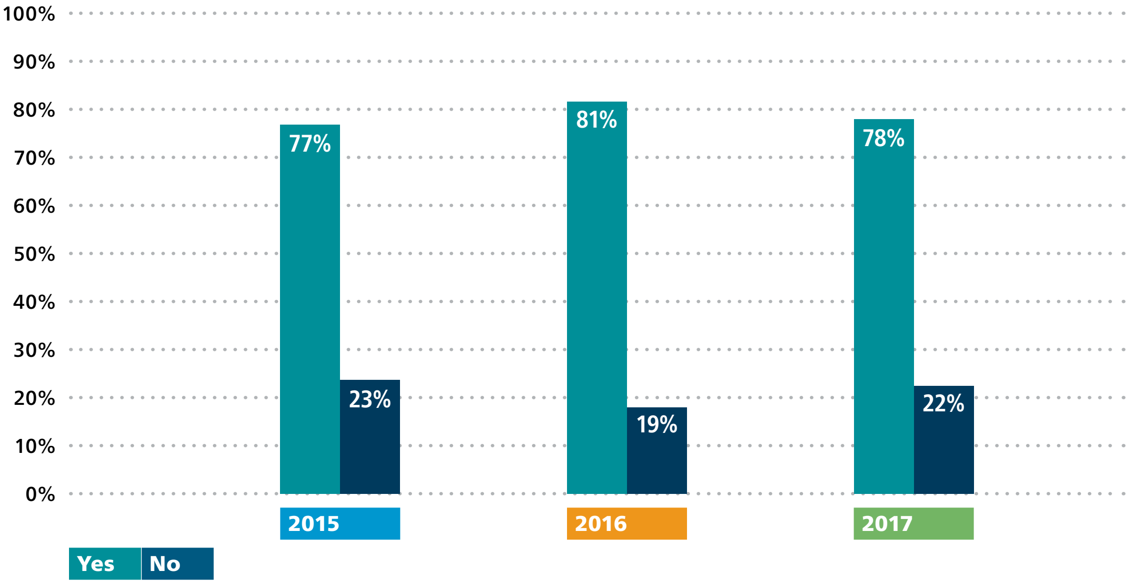


*Figure 2*

According to **Figure 2**, on average, 79 percent of top-level decision-makers are receiving periodic reports.

**Has your organization adopted or established a set of cybersecurity executive mandates, laws, statutes, approved legislation, policies, or standards to help guide the implementation of information security controls across your organization?**

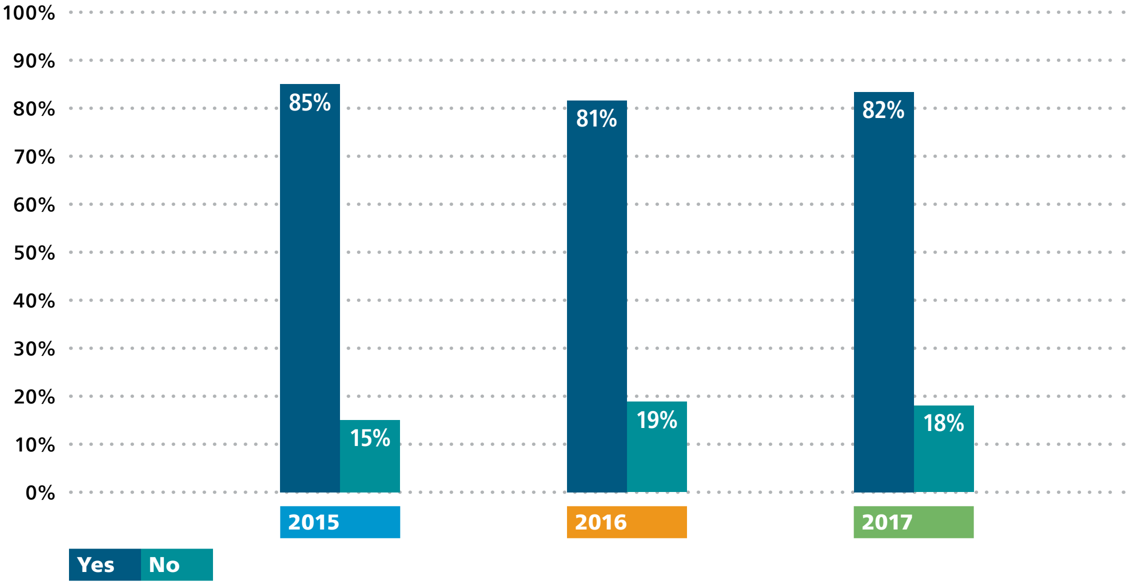


*Figure 3*

According to **Figure 3**, on average, 83 percent of respondents have adopted and/or established cybersecurity standards or policies within their organizations.

**What part of your IT operation is outsourced?**

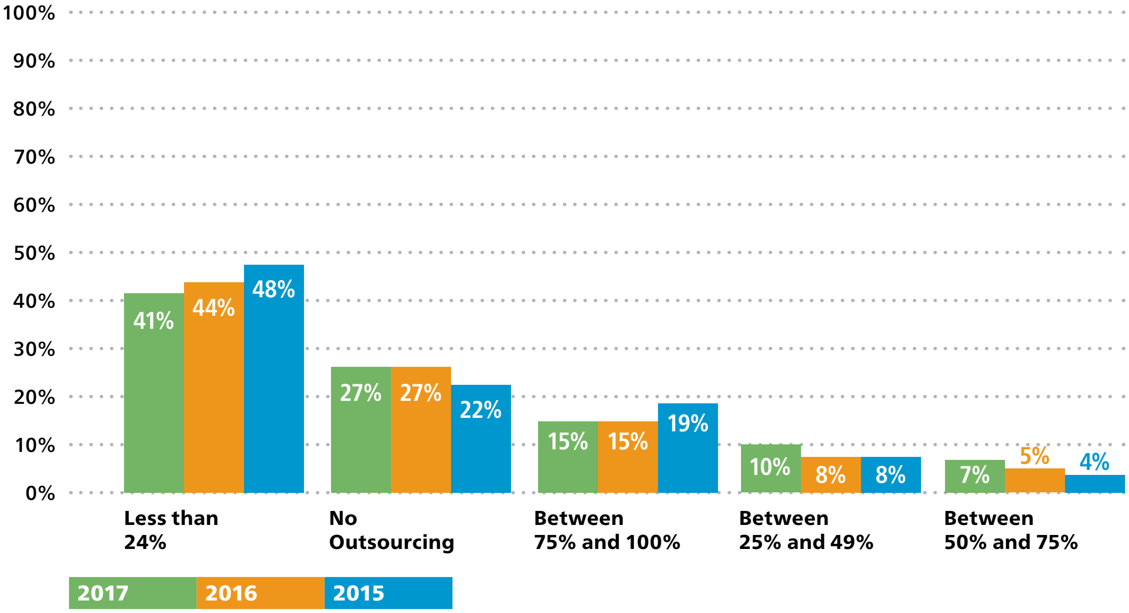


*Figure 4*

According to **Figure 4**, the majority of respondents, on average, outsource less than 24 percent of their IT operations.

**What part of your security operation is outsourced?**

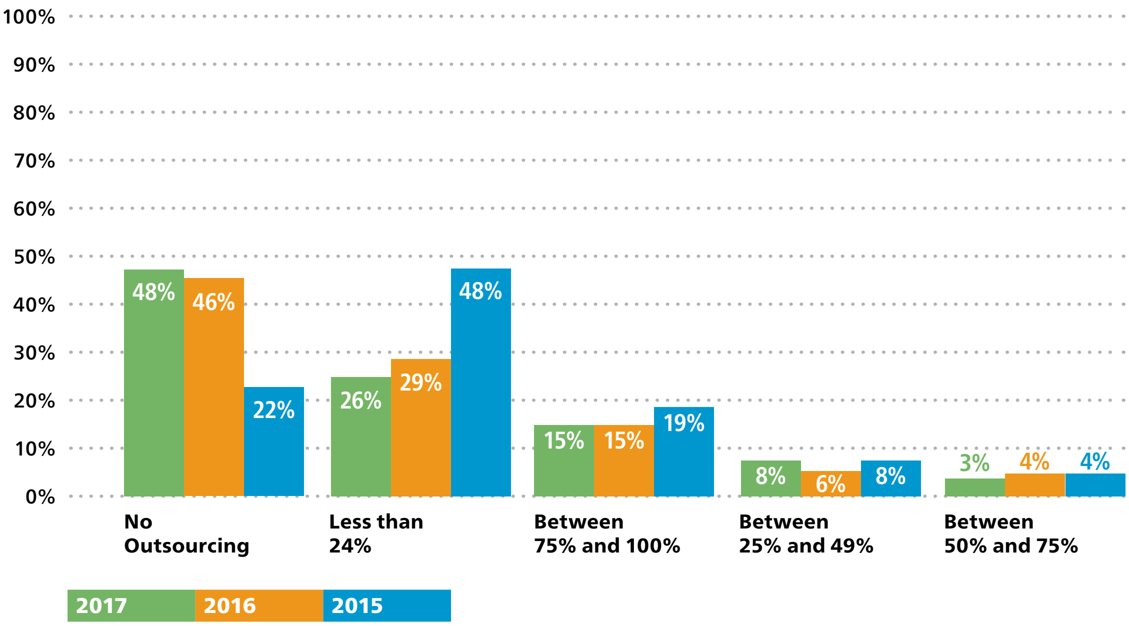


**Figure 5**

According to **Figure 5**, the majority of respondents are not outsourcing their security operations (on average 39 percent).

Participants have continually identified the same top five security concerns over the past three years. Their concerns below are presented in rank order from highest to lowest as identified in 2017.

1) Increasing sophistication of threats
2) Lack of sufficient funding
3) Emerging technologies
4) Lack of documented processes
5) Inadequate availability of cybersecurity professionals

## NCSR Maturity Scale

The NCSR utilizes a maturity scale that assesses how an organization is addressing the different activities within the NIST CSF. The maturity scale allows participants to indicate how formalized these cybersecurity activities are within their organization. Following risk management principles, the response framework allows organizations to identify which activities they have chosen not to implement because of their own risk assessment.

In order to provide a target for the SLTT community, a team of SLTT cybersecurity professionals developed a **recommended minimum maturity level** as a common baseline for the NCSR. The maturity level uses **Implementation in Process** and **Risk Formally Accepted** as the recommended minimum maturity level.

**Figure 6** provides a full breakdown of the NCSR Maturity Level response scale along with the scores associated with each maturity level.

| Score | **Maturity Level**<br>*The recommended minimum maturity level is set at a score of 5 and higher* | |
|---|---|---|
| 7 | **Optimized:** | Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness. |
| 6 | **Tested and Verified:** | Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified. |
| 5 | **Implementation in Process:** | Your organization has formally documented policies, standards, and procedures and are in the process of implementation. |
| 5 | **Risk Formally Accepted:** | Your organization has chosen not to implement based on a risk assessment. |
| 4 | **Partially Documented Standards and/or Procedures:** | Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy. |
| 3 | **Documented Policy:** | Your organization has a formal policy in place. |
| 2 | **Informally Performed:** | Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management. |
| 1 | **Not Performed:** | Activities, processes and technologies are not in place to achieve the referenced objective. |

***Figure 6***

## Analysis by Function

This section provides a high-level analysis at the function level of the 2015, 2016, and 2017 cybersecurity maturity of the state, local, and tribal peer groups, which are displayed in the below figures.

The function scores are calculated by taking the averages within each function's categories of the NIST CSF. For more information regarding an analysis of the categories, please see **Appendix II**.

The definition of each function is provided below, followed by an analysis of the data in three different formats:

- **Year-to-Year Function Averages:** The graphs display the year-to-year scores (averages) within each peer group across the functions, and provide an approximation to the overall maturity.

- **Year-to-Year Percentage Increase/Decrease:** The charts display the percentage increase or decrease captured from year to year within each peer group across the functions.

- **Function Analysis:** This section lists any trends and/or significant findings.

## 2017 Function Averages

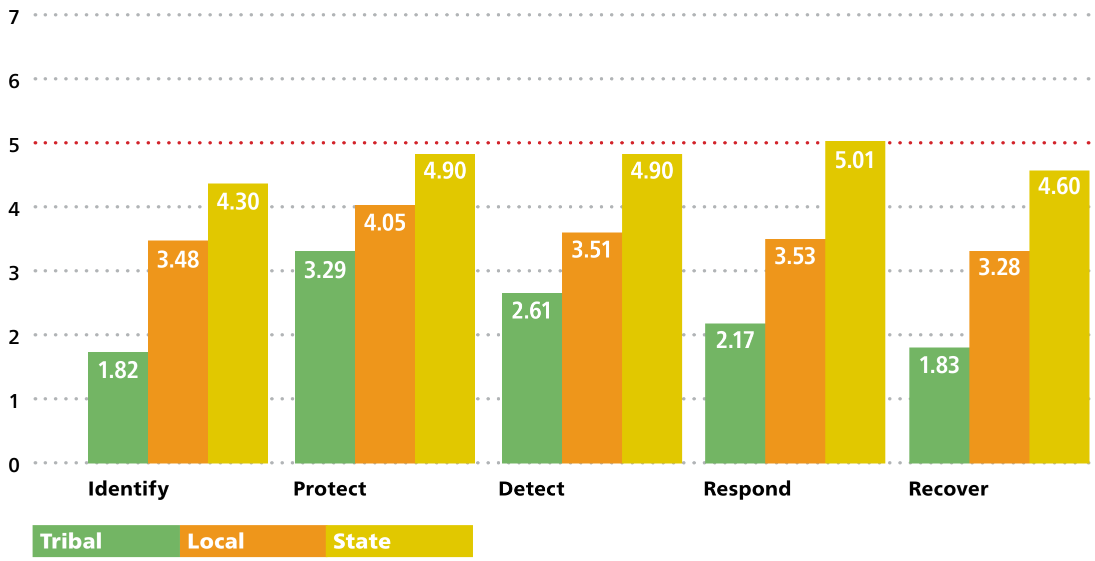


***Figure 7*** *above displays the current 2017 cybersecurity maturity of the state, local, and tribal peer groups. The horizontal red rule on this graph and the other graphs in this report represent the recommended minimum maturity level of* ***Implementation in Process****, which represents the average score of 5.*

## Year-to-Year Percentage Increase/Decrease Across Functions

| Year | Identify | Protect | Detect | Respond | Recover | AVG |
|---|---|---|---|---|---|---|
| **Tribal Peer Profile** | | | | | | |
| **2017** | -21% | 2% | -10% | 0% | -30% | -12% |
| **Local Peer Profile** | | | | | | |
| **2016** | 15% | 11% | 15% | 5% | 8% | 11% |
| **2017** | 10% | 8% | 13% | 11% | 6% | 10% |
| **State Peer Profile** | | | | | | |
| **2016** | 2% | 2% | 4% | 3% | 3% | 3% |
| **2017** | 3% | 4% | 2% | 4% | 3% | 3% |

***Figure 8*** *above represents the Year-to-Year Percentage Increase/Decrease identified within each peer group across the functions.*

## Overall Function Analysis

- The state peer group reached the recommended minimum maturity of **Implementation in Process** with an average score of **5.01** in the Respond Function (Figure 7).
- In both 2016 and 2017, the local peer group average increase across the functions was higher than the state average increase. The local average increase across the functions was **11%** in 2016 and **10%** in 2017 (Figure 8).
- In both 2016 and 2017, the average increase for the state peer group across the functions was **3%** (Figure 8).
- Although a higher percentage average increase was identified in 2016 and 2017 among the local peer group, the local peer group continued to lag behind the state peer group in terms of overall cybersecurity maturity (Figure 7).
- Using the average percentage increase of each function in 2016 and 2017, it is forecasted that the state peer group will meet the recommended minimum maturity across all the functions in 2023 and the local peer group in 2024.
- The tribal peer group is lagging behind both the state and local peer groups in terms of overall cybersecurity maturity (Figure 8).
- In 2017, a **12%** average decrease was identified across the functions in the tribal peer group (Figure 8).
- There was less participation from the tribal peer group in 2017 in comparison with 2016 (Figure 1).

## Identify Function

The activities under this functional area are key for an organization's understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest-rated functions for many organizations. Immature capabilities in the Identify Function may hinder an organization's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant risks.

## Year-to-Year Identify Function Averages

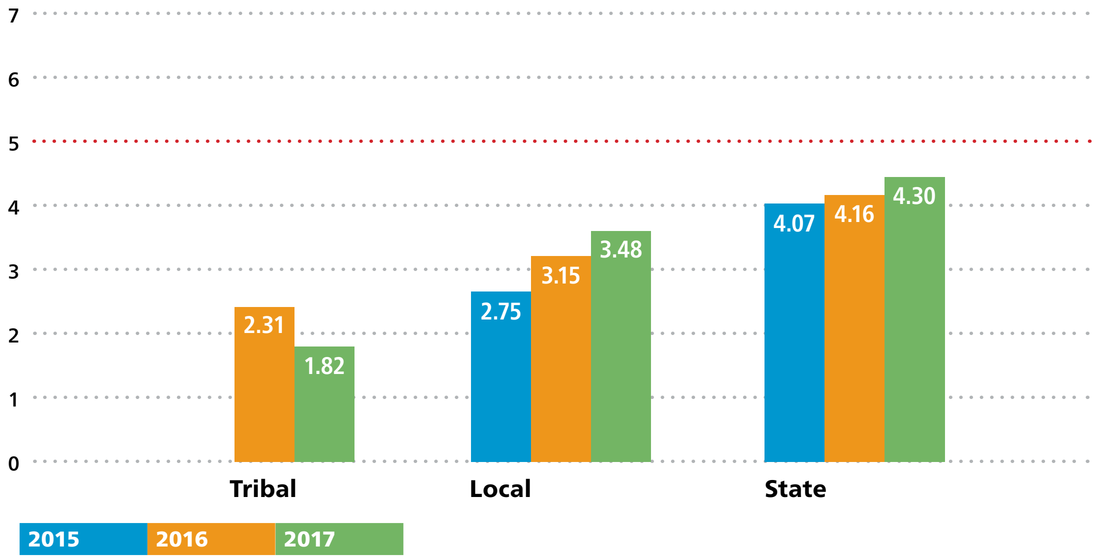


***Figure 9*** *above represents the year-to-year average for the Identify Function across the peer profiles.*

## Year-to-Year Identify Function Percentage Increase/Decrease

| Year | Tribal Peer Group | Local Peer Group | State Peer Group |
|---|---|---|---|
| **2016** | **—** | **15%** | **2%** |
| **2017** | **-21%** | **10%** | **3%** |

***Figure 10*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Identify Function.*

## Identify Function Analysis

- In 2015, 2016, and 2017, the state peer group scored lowest in the Identify Function.
- The tribal peer group saw a shift in the Identify Function. In 2017, this peer group scored lowest in this function, whereas in 2016 they scored lowest in the Respond Function.

## Protect Function

The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communication.

### Year-to-Year Protect Function Averages

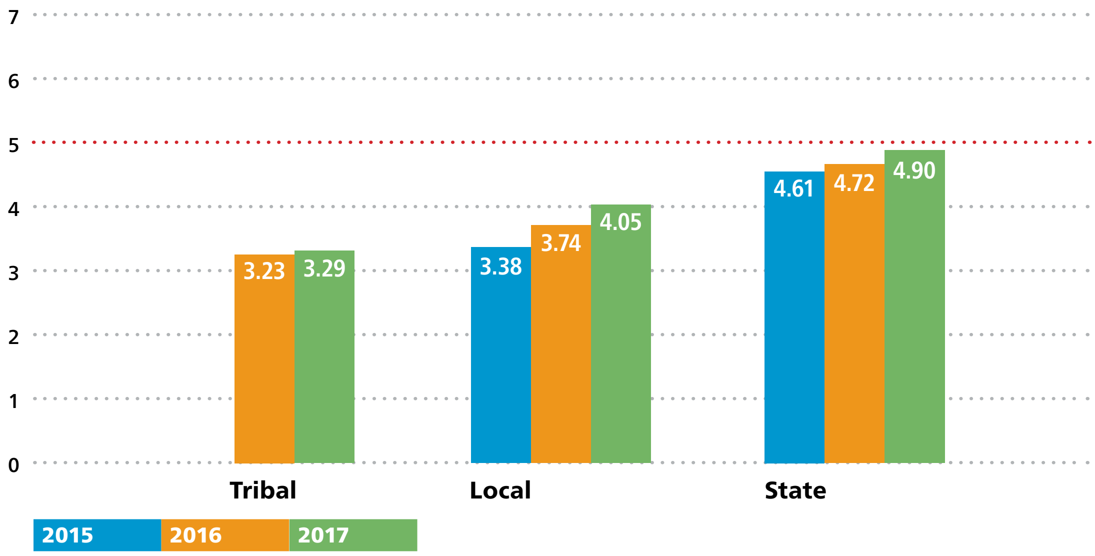


***Figure 11*** *above represents the year-to-year average for the Protect Function across the peer groups.*

### Year-to-Year Protect Function Percentage Increase/Decrease

| Year | Tribal Peer Group | Local Peer Group | State Peer Group |
|---|---|---|---|
| **2016** | — | 11% | 2% |
| **2017** | 2% | 8% | 4% |

***Figure 12*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Protect Function.*

## Protect Function Analysis

- In 2015, 2016, and 2017, the local peer group scored highest in the Protect Function.
- In 2016 and 2017 the tribal peer group scored highest in the Protect Function.

## Detect Function

The quicker an organization is able to detect a cybersecurity incident, the better positioned it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect Function pertain to an organization's ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns. This function continues to represent the largest maturity gap between state and local governments.

## Year-to-Year Detect Function Averages

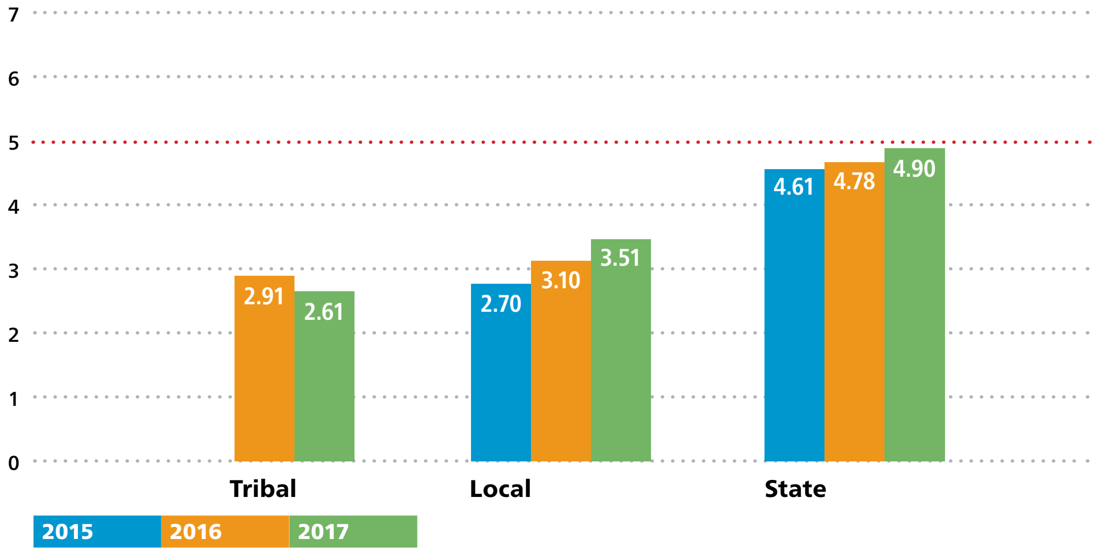


***Figure 13** above represents the year-to-year average for the Detect Function across the peer groups.*

## Year-to-Year Detect Function Percentage Increase/Decrease

| Year | Tribal Peer Group | Local Peer Group | State Peer Group |
|---|---|---|---|
| **2016** | — | 15% | 4% |
| **2017** | -10% | 13% | 2% |

***Figure 14*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Detect Function.*

## Detect Function Analysis

- The local peer group saw a shift in the Detect Function. In 2015, they scored lowest in the Detect function. In 2016, they scored lowest in the Detect and Recover function. Whereas in 2017, they scored lowest in just  the Recover Function.

## Respond Function

An organization's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations identify and remediate the original attack vector. This gap can be addressed through resource sharing within the SLTT community and leveraging organizations such as MS-ISAC and DHS's National Cybersecurity and Communications Integration Center (NCCIC), which have dedicated resources to provide incident response at no cost to the victim.

## Year-to-Year Respond Function Averages

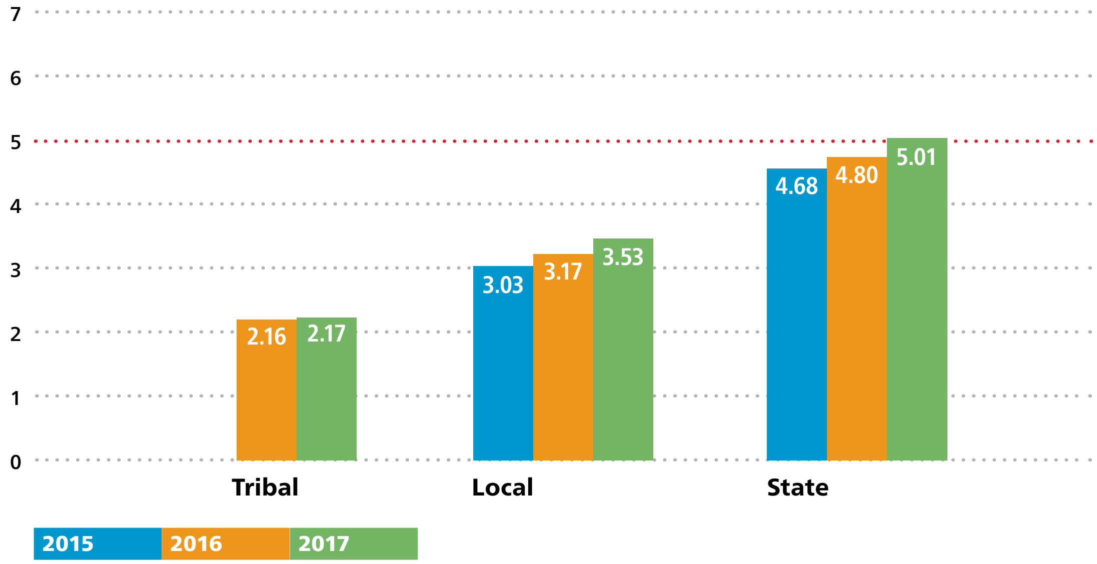


***Figure 15*** *above represents the year-to-year average for the Respond Function across the peer groups.*

## Year-to-Year Respond Function Percentage Increase/Decrease

| Year | Tribal Peer Group | Local Peer Group | State Peer Group |
|---|---|---|---|
| **2016** | — | 5% | 3% |
| **2017** | 0% | 11% | 4% |

***Figure 16*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Respond Function.*

## Respond Function Analysis

- In 2015, 2016, and 2017, the state peer group scored highest in the Respond Function.
- In 2017, the state peer group reached the recommended minimum maturity level of **Implementation in Process** in the Respond Function (average score of **5.01**).

## Recover Function

Activities within the Recover Function pertain to an organization's ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

### Year-to-Year Recover Function Averages

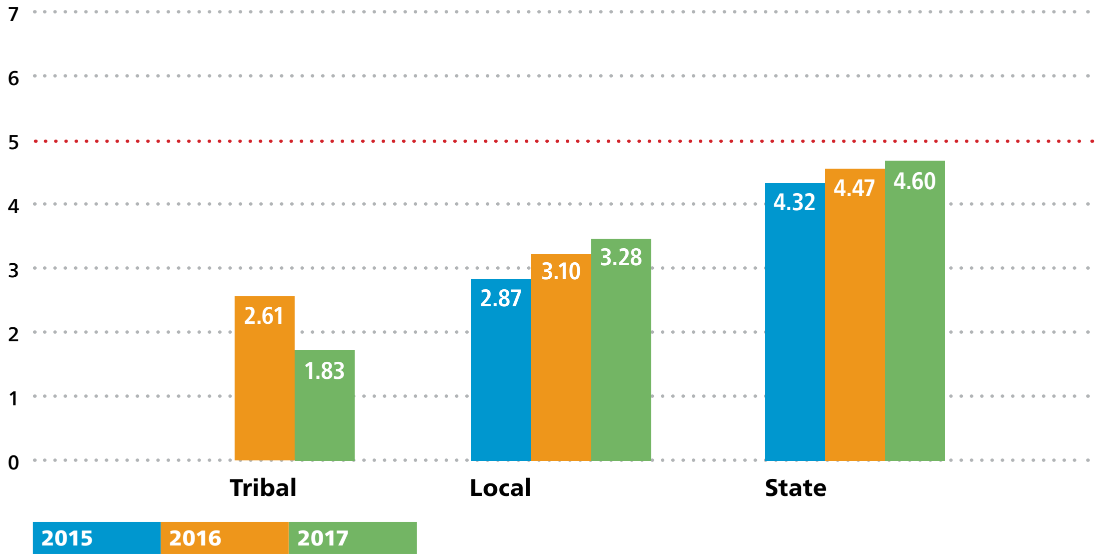


***Figure 17*** *above represents the year-to-year average for the Recover Function across the peer groups.*

## Year-to-Year Recover Function Percentage Increase/Decrease

**% Increase in NIST CSF Recover Function**

| Year | Tribal Peer Group | Local Peer Group | State Peer Group |
|---|---|---|---|
| **2016** | — | 8% | 3% |
| **2017** | -30% | 6% | 3% |

***Figure 18** above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Recover Function.*

## Recover Function Analysis

- In 2016, the local peer group scored lowest in the Detect and Recover Function. Whereas, in 2017, a shift was seen as they scored lowest in just the Recover Function.

## Partners

The U.S. Department of Homeland Security (DHS) has partnered with the Multi-State Information Sharing & Analysis Center (MS-ISAC), the National Association of State Chief Information Officers (NASCIO), and the National Association of Counties (NACo) to develop the Nationwide Cybersecurity Review.

### *U.S. Department of Homeland Security*

DHS is responsible for safeguarding our nation's critical infrastructure from physical and cyber threats that can affect national security, public safety, and economic prosperity. The National Protection and Programs Directorate leads DHS' efforts to secure cyberspace and cyber infrastructure. For additional information, please visit www.dhs.gov/cyber

### *Multi-State Information Sharing & Analysis Center*

Grant-funded by DHS, MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, tribal, and territorial (SLTT) governments. The MS-ISAC 24/7 Security Operations Center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation, and incident response. For more information about the MS-ISAC, please visit https://www.cisecurity.org/ms-isac/

### *National Association of State Chief Information Officers*

NASCIO's mission is to foster government excellence through quality business practices, information management, and technology policy.

Founded in 1969, NASCIO is a nonprofit, 501(c)(3) association representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia. The primary state members are senior officials from state government who have executive-level and statewide responsibility for information technology leadership. State officials who are involved in agency level information technology management may participate as associate members. Representatives from federal, municipal, international government, and nonprofit organizations may also participate as members. Private-sector firms join as corporate members and participate in the Corporate Leadership Council. For more information about NASCIO, please visit https://w ww.nascio.org/

### *National Association of Counties*

The National Association of Counties (NACo) is the only national organization that represents county governments in the United States.

Founded in 1935, NACo provides essential services to the nation's 3,069 counties. NACo advances issues with a unified voice before the federal government, improves the public's understanding of county government, assists counties in finding and sharing innovative solutions through education and research, and provides value-added services to save counties and taxpayers money. For more information about NACo, please visit http://www.naco.org/

## Appendix I: Acronyms

| | |
|---|---|
| **DHS** | U.S. Department of Homeland Security |
| **MS-ISAC** | Multi-State Information Sharing & Analysis Center |
| **NACo** | National Association of Counties |
| **NASCIO** | National Association of State Chief Information Officers |
| **NCCIC** | National Cybersecurity and Communications Integration Center |
| **NCSR** | Nationwide Cybersecurity Review |
| **NIST** | National Institute of Standards and Technology |
| **NIST CSF** | National Institute of Standards and Technology Cybersecurity Framework |
| **SLTT** | State, Local, Tribal, and Territorial |

## Appendix II: Peer Group Detailed Data Analysis for Function Categories

This appendix provides a detailed year-to-year analysis of the categories within the functions of the NIST CSF for the state, local, and tribal peer groups.

The definition of the function and categories within each function are provided and accompanied by an analysis of the data in three different ways:

- **Year-to-Year Category Averages:** The graphs display the year-to-year scores within each peer group across the categories within each function and provide an approximation as to the overall maturity.
- **Year-to-Year Percentage Increase/Decrease:** The charts display the percentage increase/decrease captured from year to year within each peer group across the categories of the functions.
- **Category Percentage Increase/Decrease Highlights:** These sections provide highlights that are displayed in two different formats:
  - **Moderate:** Lists any percentage increases and/or decreases between 5 percent and 9 percent in each of the function categories across the peer groups in 2016 and 2017.
  - **Significant:** Lists any percentage increases and/or decreases of 10 percent or more in each of the function categories across the peer groups in 2016 and 2017.

The categories' scores are calculated by averaging the sub-categories within each category of the NIST CSF.

## Identify Function

The activities found within this functional area are key for an organization's understanding of their current internal culture, infrastructure, and risk tolerance. This functional area tends to be one of the lowest functions rated for many organizations. Immature capabilities in the Identify Function may hinder an organization's ability to effectively apply risk management principles for cybersecurity. By incorporating sound risk management principles into cybersecurity programs, organizations will be able to continuously align their efforts towards protecting their most valuable assets against the most relevant and pertinent risks.

### *Identify Categories*

- **Asset Management:** The data, personnel, devices, system, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

- **Business Environment:** The organization's missions, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

- **Governance:** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

- **Risk Assessment:** The organization understands the cybersecurity risks to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

- **Risk Management Strategy:** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

## Year-to-Year Identify Category Averages

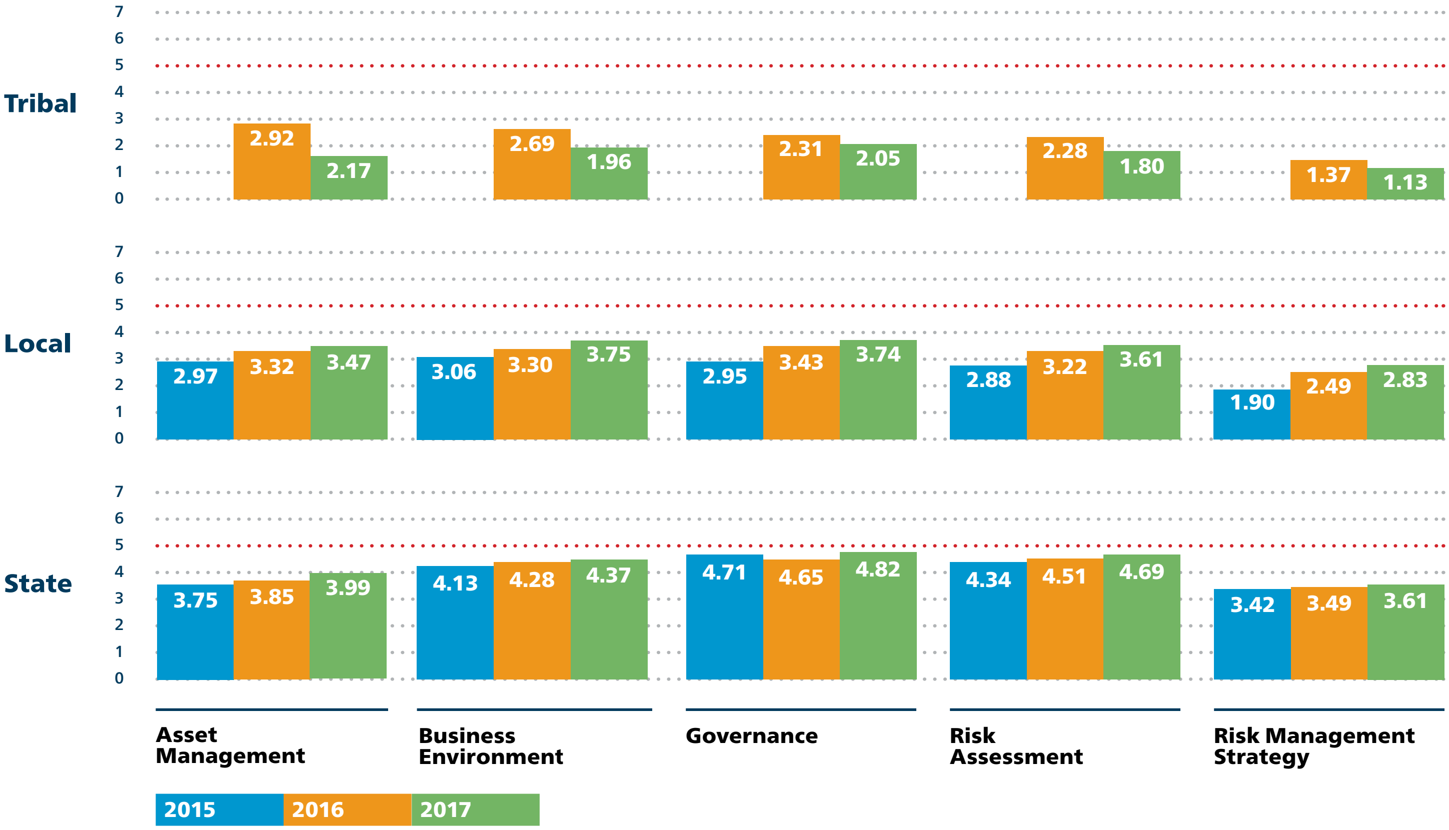


***Figure 19*** *above represents the year-to-year averages for the Identify categories across the peer groups.*

## Year-to-Year Identify Categories Percentage Increase/Decrease

| Year | Asset Management | Business Environment | Governance | Risk Assessment | Risk Management Strategy | Identify |
|---|---|---|---|---|---|---|
| **Tribal Peer Profile** | | | | | | |
| **2017** | **-26%** | **-27%** | **-11%** | **-21%** | **-18%** | **-21%** |
| **Local Peer Profile** | | | | | | |
| **2016** | **12%** | **8%** | **16%** | **12%** | **31%** | **15%** |
| **2017** | **5%** | **14%** | **9%** | **12%** | **14%** | **10%** |
| **State Peer Profile** | | | | | | |
| **2016** | **3%** | **4%** | **-1%** | **4%** | **2%** | **2%** |
| **2017** | **4%** | **2%** | **4%** | **4%** | **4%** | **3%** |

***Figure 20*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Identify categories.*

## Identify Categories Percentage Increase/Decrease Highlights

**Moderate:** The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Identify categories across the peer groups in 2016 and 2017.

| **Increase/Decrease of**<br>**5% to 9%** | |
|---|---|
| **2016 Local** | • 8% increase identified in Business Environment |
| **2017 Local** | • 5% increase identified in Asset Management<br>• 9% increase identified in Governance |

**Significant:** The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Identify categories across the peer groups in 2016 and 2017.

| **Increase/Decrease of**<br>**10% or More** | |
|---|---|
| **2016 Local** | • 12% increase identified in Asset Management<br>• 16% increase identified in Governance<br>• 12% increase identified in Risk Assessment<br>• **31% increase identified in Risk Management Strategy** |
| **2017 Local** | • 14% increase identified in Business Environment<br>• 12% increase identified in Risk Assessment<br>• 14% increase identified in Risk Management Strategy |
| **2017 Tribal** | • **26% decrease identified in Asset Management**<br>• **27% decrease identified in Business Environment**<br>• 11% decrease identified in Governance<br>• 21% decrease identified in Risk Management<br>• 18% decrease identified in Risk Management Strategy |

## Protect Function

The activities under the Protect Function pertain to different methods and activities that reduce the likelihood of cybersecurity events from happening and ensure that the appropriate controls are in place to deliver critical services. These controls are focused on preventing cybersecurity events from occurring through common attack vectors, including attacks targeting users and attacks leveraging inherent weakness in applications and network communications.

### *Protect Categories*

- **Access Control:** Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

- **Awareness and Training:** The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

- **Data Security:** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- **Information Protection Processes & Procedures:** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

- **Maintenance:** Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

- **Protective Technology:** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

## Year-to-Year Protect Category Averages

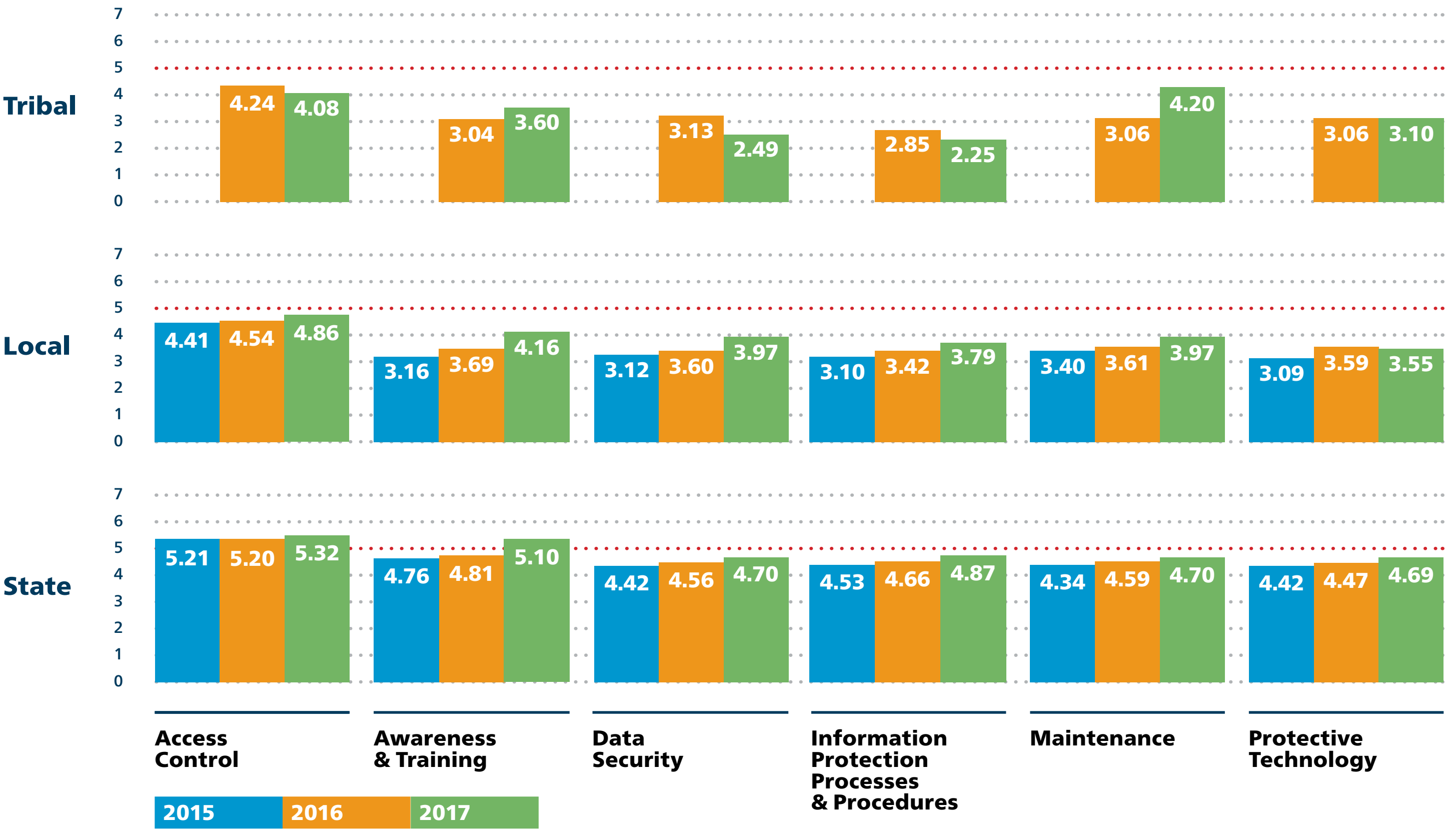


***Figure 21*** *above represents the year-to-year averages for the Protect categories across the peer groups.*

## Year-to-Year Protect Categories Percentage Increase/Decrease

| Year | Access Control | Awareness & Training | Data Security | Information Protection Processes & Procedures | Maintenance | Protective Technology | Protect |
|---|---|---|---|---|---|---|---|
| **Tribal Peer Profile** | | | | | | | |
| 2017 | -4% | 18% | -20% | -21% | 37% | 1% | 2% |
| **Local Peer Profile** | | | | | | | |
| 2016 | 3% | 17% | 15% | 10% | 6% | 16% | 11% |
| 2017 | 7% | 13% | 10% | 11% | 10% | -1% | 8% |
| **State Peer Profile** | | | | | | | |
| 2016 | 0% | 1% | 3% | 3% | 6% | 1% | 2% |
| 2017 | 2% | 6% | 3% | 5% | 2% | 5% | 4% |

***Figure 22*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Protect categories.*

## Protect Categories Percentage Increase/Decrease Highlights

**Moderate:** The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Protect categories across the peer groups in 2016 and 2017.

| Increase/Decrease of<br>5% to 9% | |
|---|---|
| **2016 State** | • 6% increase identified in Maintenance |
| **2016 Local** | • 6% increase identified in Maintenance |
| **2017 State** | • 6% increase identified in Awareness & Training<br>• 5% increase identified in Information Protection Processes & Procedures<br>• 5% increase identified in Protective Technology |
| **2017 Local** | • 7% increase identified in Access Control |

**Significant:** The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Protect categories across the peer groups in 2016 and 2017.

| Increase/Decrease of<br>10% or More | |
|---|---|
| **2016 Local** | • 17% increase identified in Awareness & Training<br>• 15% increase identified in Data Security<br>• 10% increase identified in Information Protection Processes & Procedures<br>• 16% increase identified in Protective Technology |
| **2017 Local** | • 13% increase identified in Awareness & Training<br>• 10% increase identified in Data Security<br>• 11% increase identified in Information Protection Processes & Procedures<br>• 10% increase identified in Maintenance |
| **2017 Tribal** | • 18% increase identified in Awareness & Training<br>• 20% decrease identified in Data Security<br>• 21% decrease identified in Information Protection Processes & Procedures<br>**• 37% increase identified in Maintenance** |

## Detect Function

The quicker an organization is able to detect a cybersecurity incident, the better postured it is to be able to remediate the problem and reduce the consequences of the event. Activities found within the Detect Function pertain to an organization's ability to identify incidents. These controls are becoming more important as the quantity of logs and events occurring within an environment can be overwhelming to handle and can make it difficult to identify the key concerns. This function represented the largest maturity gap between local and state governments.

### *Detect Categories*

- **Anomalies and Events:** Anomalous activity is detected in a timely manner and the potential impact of events is understood.
- **Security Continuous Monitoring:** The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.
- **Detection Processes:** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

**Year-to-Year Detect Category Averages**

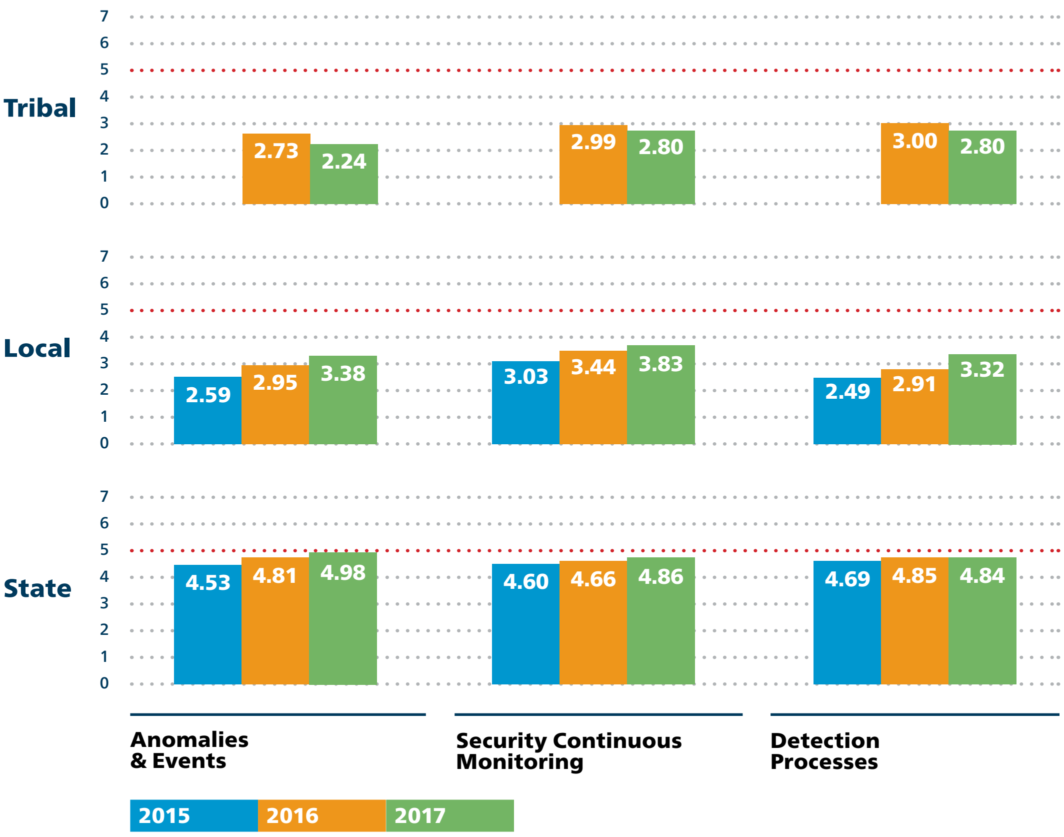


***Figure 23*** *above represents the year-to-year averages for the Detect categories across the peer groups.*

## Year-to-Year Detect Categories Percentage Increase/Decrease

| Year | Anomalies & Events | Security Continuous Monitoring | Detection Processes | Detect |
|---|---|---|---|---|
| **Tribal Peer Profile** | | | | |
| 2017 | -18% | -6% | -7% | -10% |
| **Local Peer Profile** | | | | |
| 2016 | 14% | 14% | 17% | 15% |
| 2017 | 14% | 11% | 14% | 13% |
| **State Peer Profile** | | | | |
| 2016 | 6% | 1% | 3% | 4% |
| 2017 | 4% | 4% | 0% | 2% |

***Figure 24*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Detect categories.*

## Detect Categories Percentage Increase/Decrease Highlights

**Moderate:** The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Detect categories across the peer groups in 2016 and 2017.

### Increase/Decrease of 5% to 9%

| | |
|---|---|
| **2016 State** | • 6% increase identified in Anomalies & Events |
| **2017 Tribal** | • 6% decrease identified in Security Continuous Monitoring<br>• 7% decrease identified in Detection Processes |

**Significant:** The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Detect categories across the peer groups in 2016 and 2017.

### Increase/Decrease of 10% or More

| | |
|---|---|
| **2016 Local** | • 14% increase identified in Anomalies & Events<br>• 14% increase identified in Security Continuous Monitoring<br>• 17% increase identified in Detection Processes |
| **2017 Local** | • 14% increase identified in Anomalies & Events<br>• 11% increase identified in Security Continuous Monitoring<br>• 14% increase identified in Detection Processes |
| **2017 Tribal** | • 18% decrease identified in Anomalies & Events |

## Respond Function

An organization's ability to quickly and appropriately respond to an incident plays a large role in reducing the incident's consequences. As such, the activities within the Respond Function examine how an organization plans, analyzes, communicates, mitigates, and improves its response capabilities. For many organizations, integration and cooperation with other entities is key. Many organizations do not have the internal resources to handle all components of incident response. One example is the ability to conduct forensics after an incident, which helps organizations identify and remediate the original attack vector. This gap can be addressed through resource sharing within the SLTT community and leveraging organizations such as MS-ISAC and DHS's National Cybersecurity and Communications Integration Center (NCCIC), which have dedicated resources to provide incident response at no cost to the victim.

### *Respond Categories*

- **Response Planning:** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.
- **Communications:** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.
- **Analysis:** Analysis is conducted to ensure adequate response and support recovery activities.
- **Mitigation:** Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.
- **Improvements:** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

## Year-to-Year Respond Category Averages

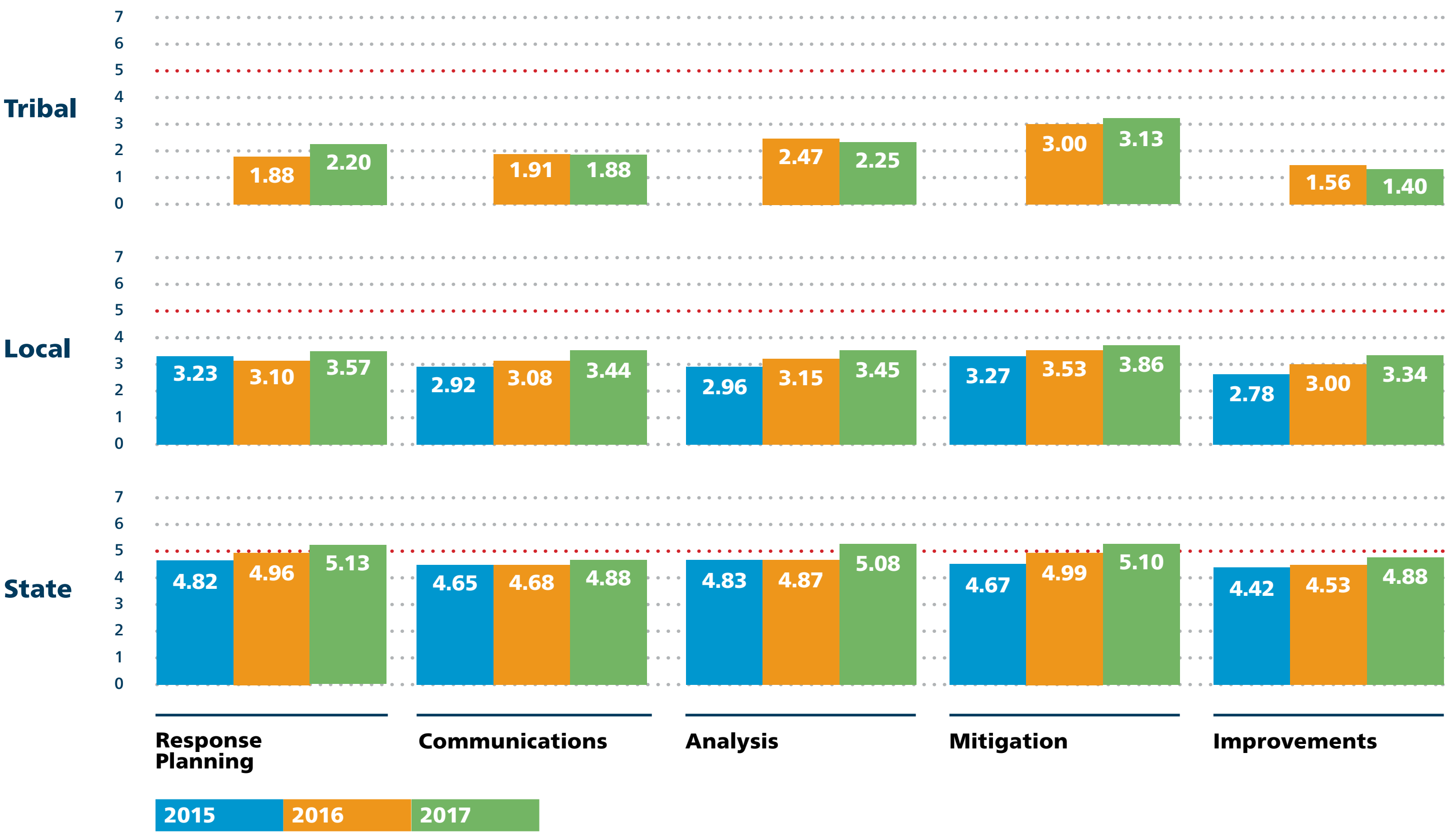


***Figure 25*** *above represents the year-to-year averages for the Respond categories across the peer groups.*

## Year-to-Year Respond Categories Percentage Increase/Decrease

| Year | Response Planning | Communications | Analysis | Mitigation | Improvements | Respond Function |
|---|---|---|---|---|---|---|
| **Tribal Peer Profile** | | | | | | |
| 2017 | 17% | -2% | -9% | 4% | -10% | 0% |
| **Local Peer Profile** | | | | | | |
| 2016 | -4% | 5% | 6% | 8% | 8% | 5% |
| 2017 | 15% | 12% | 10% | 9% | 11% | 11% |
| **State Peer Profile** | | | | | | |
| 2016 | 3% | 1% | 1% | 7% | 2% | 3% |
| 2017 | 3% | 4% | 4% | 2% | 8% | 4% |

***Figure 26*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Respond categories.*

## Respond Categories Percentage Increase/Decrease Highlights

**Moderate:** The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Respond categories across the peer groups in 2016 and 2017.

| Increase/Decrease of<br>5% to 9% | |
|---|---|
| **2016 State** | • 7% increase identified in Mitigation |
| **2016 Local** | • 5% increase identified in Communications<br>• 6% increase identified in Analysis<br>• 8% increase identified in Mitigation<br>• 8% increase identified in Improvements |
| **2017 State** | • 8% increase identified in Improvements |
| **2017 Local** | • 9% increase identified in Mitigation |
| **2017 Tribal** | • 9% decrease identified in Analysis |

**Significant:** The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Respond categories across the peer groups in 2016 and 2017.

| Increase/Decrease of<br>10% or More | |
|---|---|
| **2017 Local** | • 15% increase identified in Response Planning<br>• 12% increase identified in Communications<br>• 10% increase identified in Analysis<br>• 11% increase identified in Improvements |
| **2017 Tribal** | • 17% increase identified in Response Planning<br>• 10% decrease identified in Improvements |

## Recover Function

Activities within the Recover Function pertain to an organization's ability to return to its baseline after an incident has occurred. Such controls are focused not only on activities to recover from the incident, but also on many of the components dedicated to managing response plans throughout their lifecycle.

### *Recover Categories*

- **Recovery Planning:** Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

- **Improvements:** Recovery planning and processes are improved by incorporating lessons learned into future activities.

- **Communications**: Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other Computer Security Incident Response Teams, and vendors.

### Year-to-Year Recover Category Averages

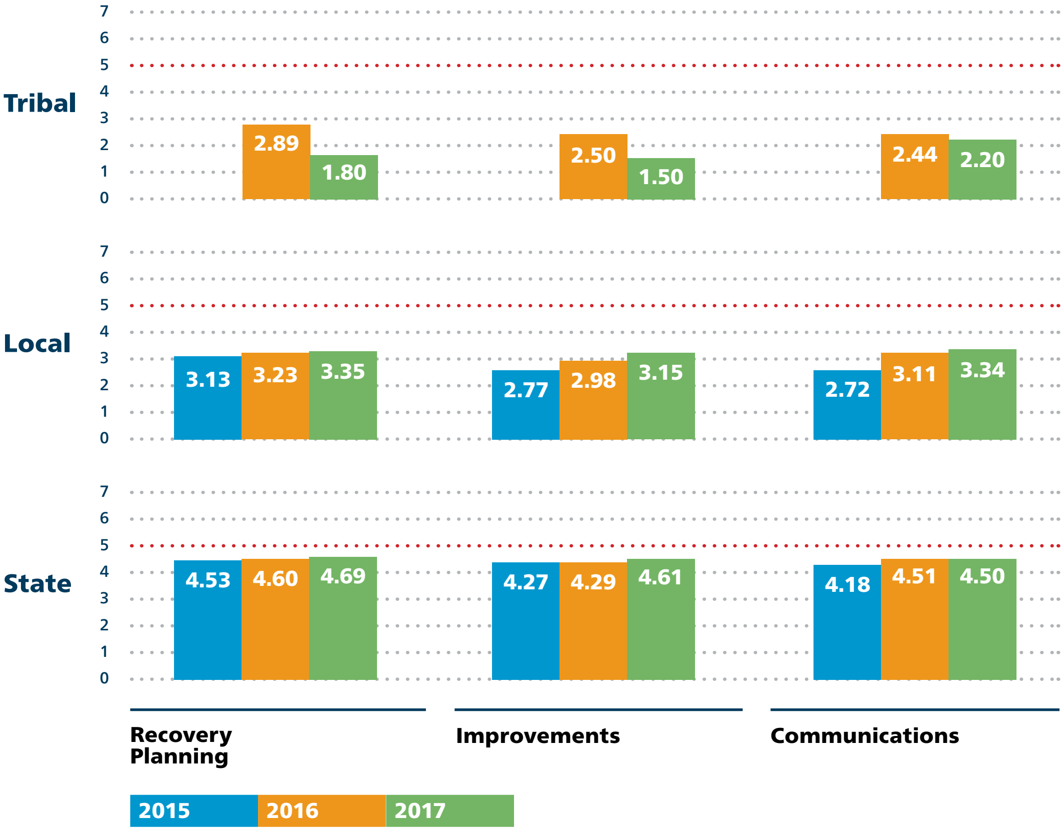


***Figure 27** above represents the year-to-year averages for the Recover categories across the peer groups.*

## Year-to-Year Recover Categories Percentage Increase/Decrease

| Year | Recovery Planning | Improvements | Communications | Recover Function |
|---|---|---|---|---|
| **Tribal Peer Group** | | | | |
| 2017 | -38% | -40% | -10% | -30% |
| **Local Peer Group** | | | | |
| 2016 | 3% | 8% | 14% | 8% |
| 2017 | 4% | 6% | 8% | 6% |
| **State Peer Group** | | | | |
| 2016 | 2% | 0% | 8% | 3% |
| 2017 | 2% | 7% | 0% | 3% |

***Figure 28*** *above displays the percentage increase and/or decrease identified in 2016 and 2017 within each peer group across the Recover categories.*

## Recover Categories Percentage Increase/Decrease Highlights

**Moderate:** The below image lists any percentage increase and/or decrease between 5 percent and 9 percent that was identified in the Recover categories across the peer groups in 2016 and 2017.

**Increase/Decrease of**
**5% to 9%**

| | |
|---|---|
| **2016 State** | • 8% increase identified in Communications |
| **2016 Local** | • 8% increase identified in Improvements |
| **2017 State** | • 7% increase identified in Improvements |
| **2017 Local** | • 6% increase identified in Improvements<br>• 8% increase identified in Communications |

**Significant:** The below image lists any percentage increase and/or decrease of 10 percent or more that was identified in the Recover categories across the peer groups in 2016 and 2017.

**Increase/Decrease of**
**10% or More**

| | |
|---|---|
| **2016 Local** | • 14% increase identified in Communications |
| **2017 Tribal** | **• 38% decrease identified in Recovery Planning**<br>**• 40% decrease identified in Improvements**<br>• 10% decrease identified in Communications |

## Appendix III: Sub-Sector Peer Groups

In 2017, the NCSR was designed to capture **18** additional peer groups based on sub-sectors. The sub-sector peer groups were created for any sub-sector that had a minimum of five organizations complete the 2017 NCSR.

Moving forward, MS-ISAC will be analyzing the year-to-year data within the sub-sectors and providing a year-to-year analysis done at the NIST CSF Function and Category levels.

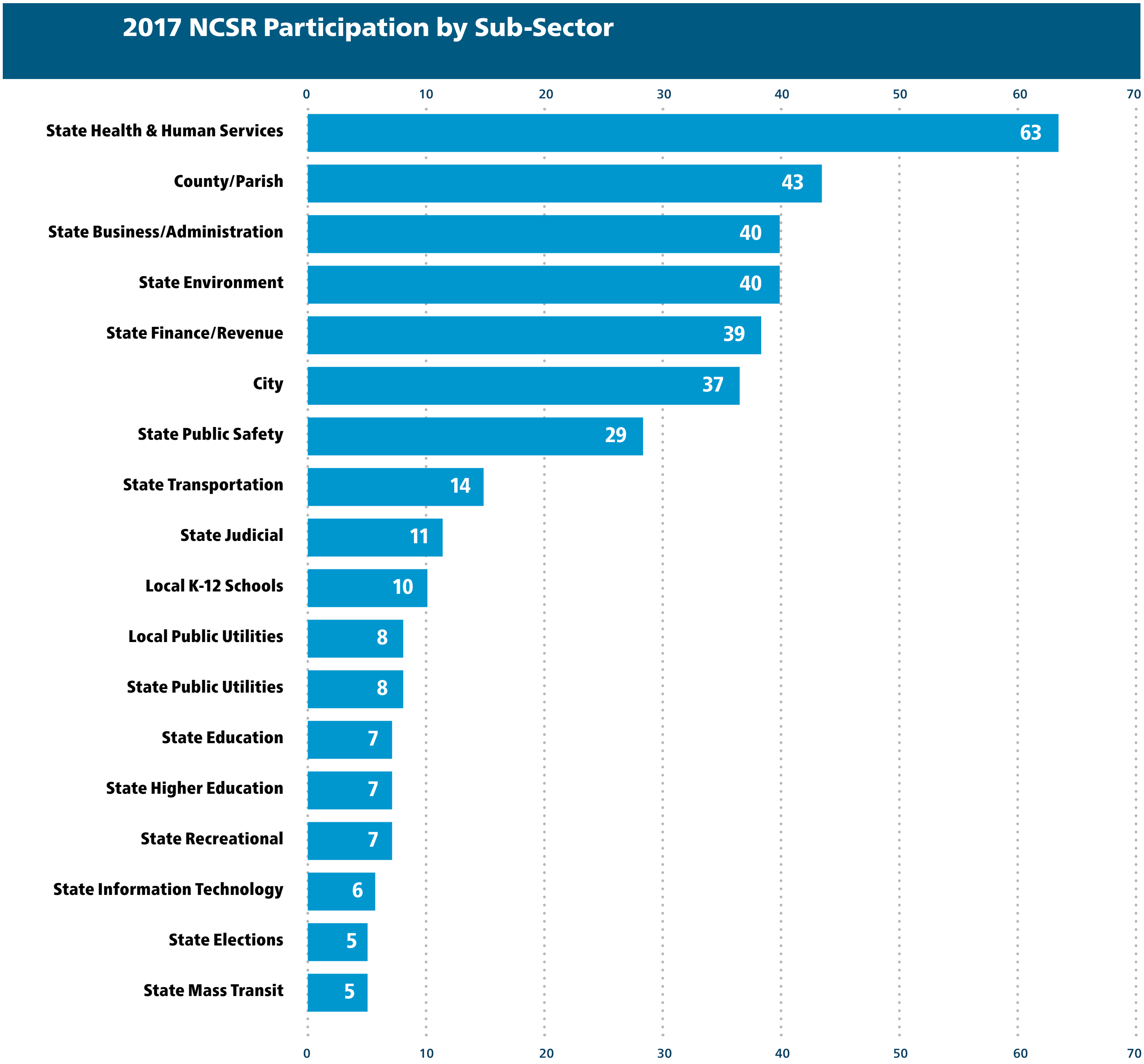


***Figure 29*** *above lists the sub-sector name and the total number of organizations that are applicable to that specific sub-sector.*

## 2017 Sub-Sector Overall Function Averages

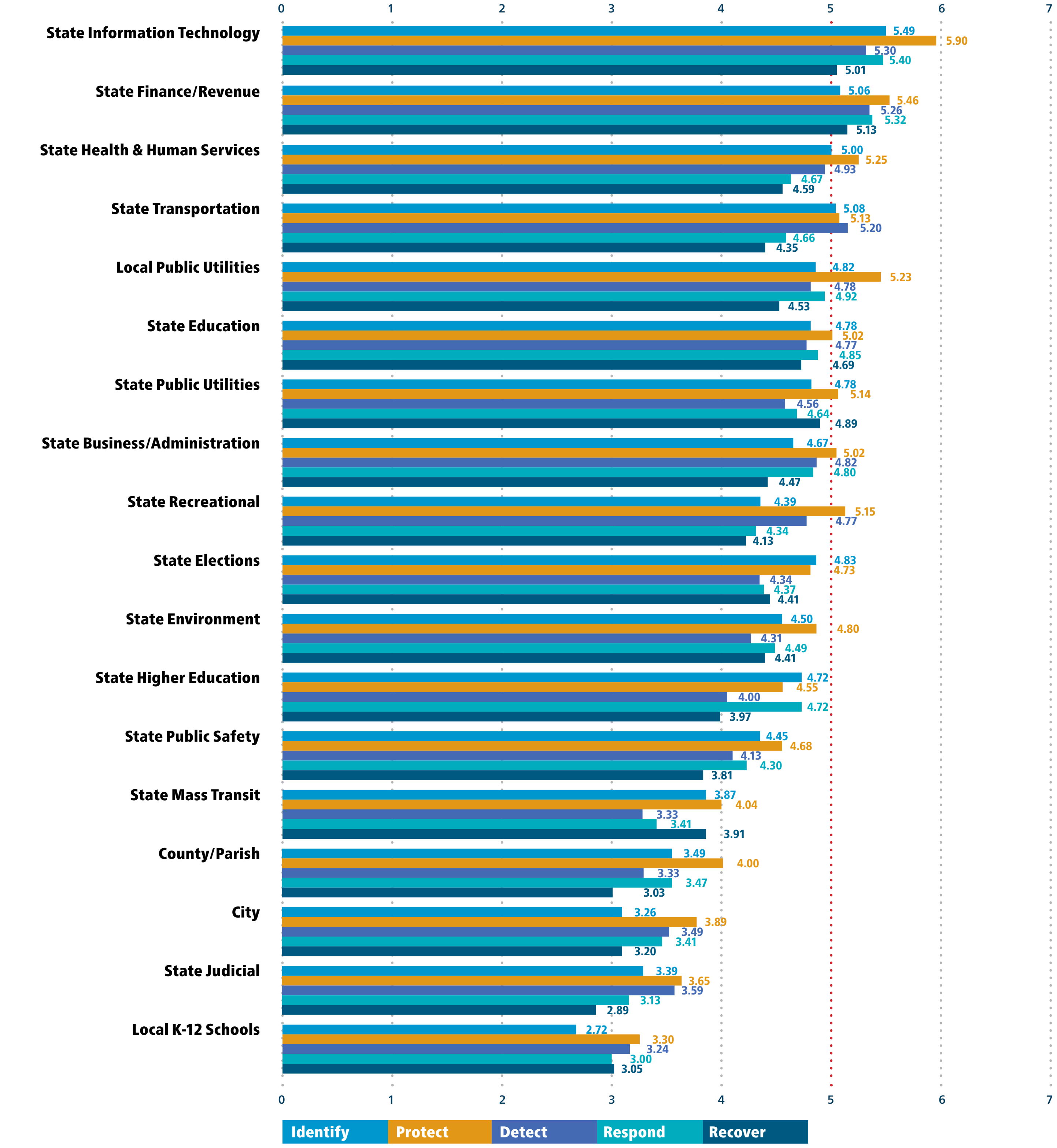


***Figure 30*** *above represents the 2017 averages within each of the sub-sector peer groups across the functions.*

***2017 NCSR Sub-Sector Function Category Averages***

## 2017 Sub-Sector Identify Categories

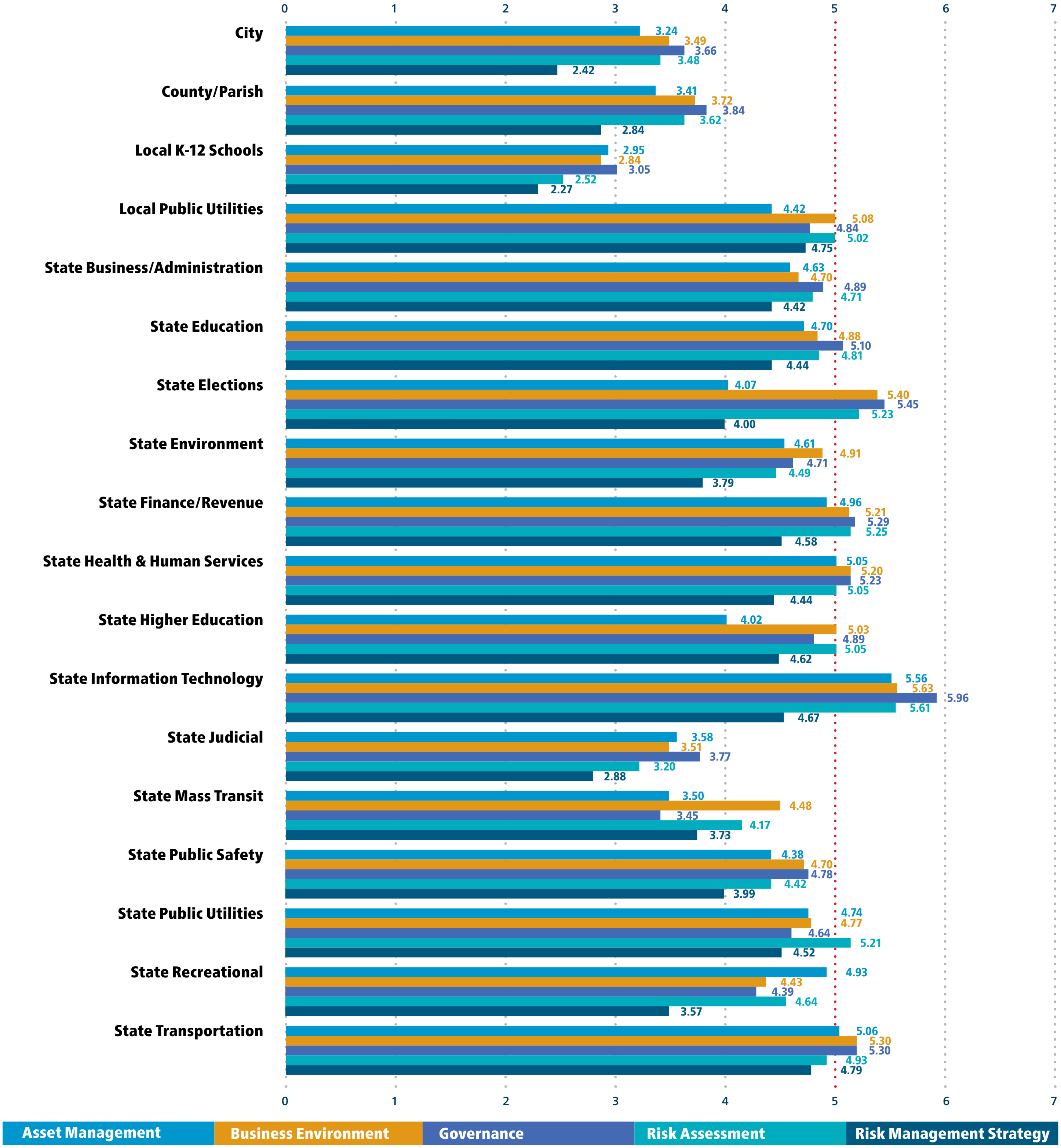


***Figure 31** above represents the overall averages for each of the sub-sectors across the Identify categories.*

## 2017 Sub-Sector Protect Categories

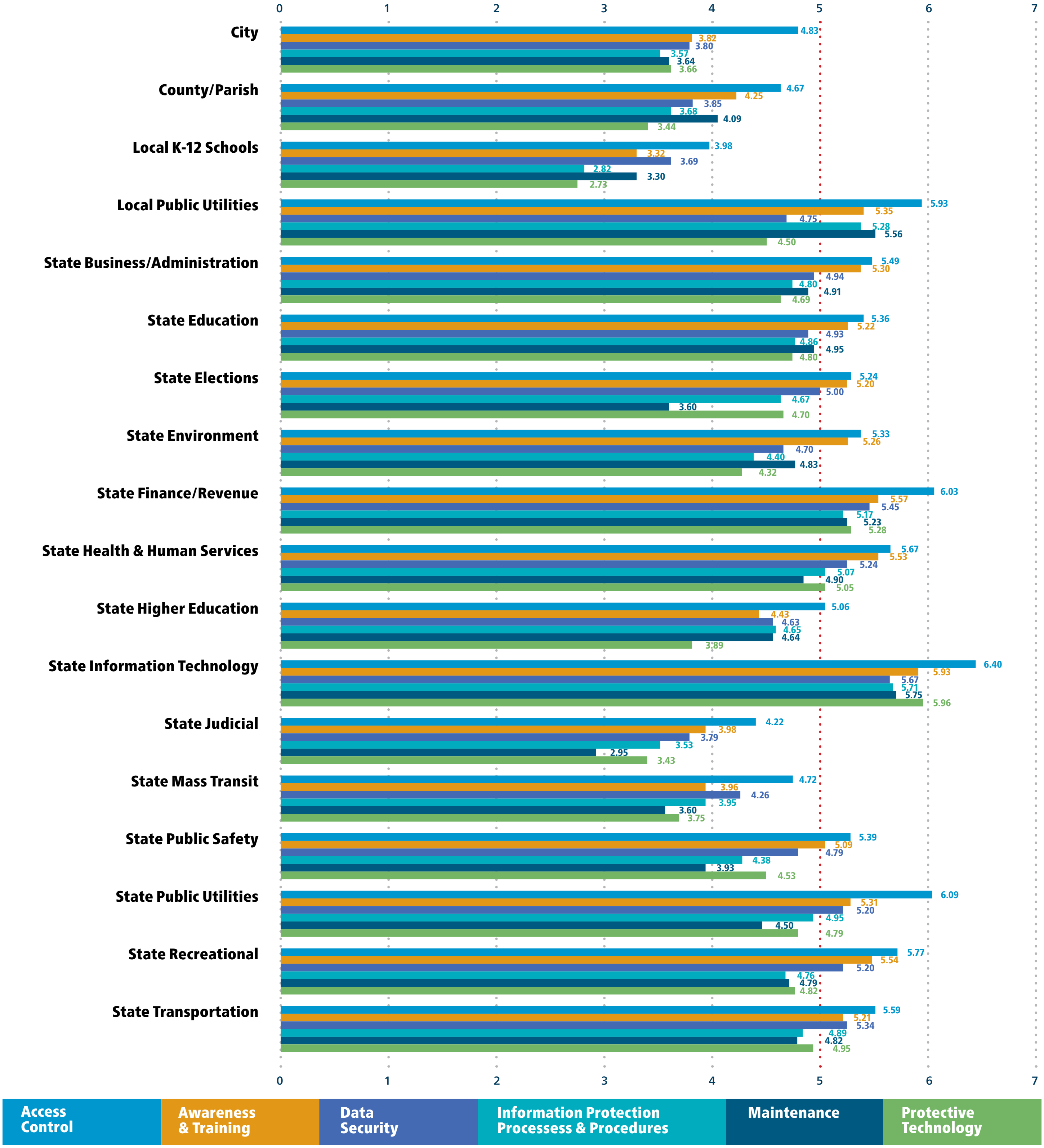


***Figure 32*** *above represents the overall averages for each of the sub-sectors across the Protect categories.*

## 2017 Sub-Sector Detect Categories

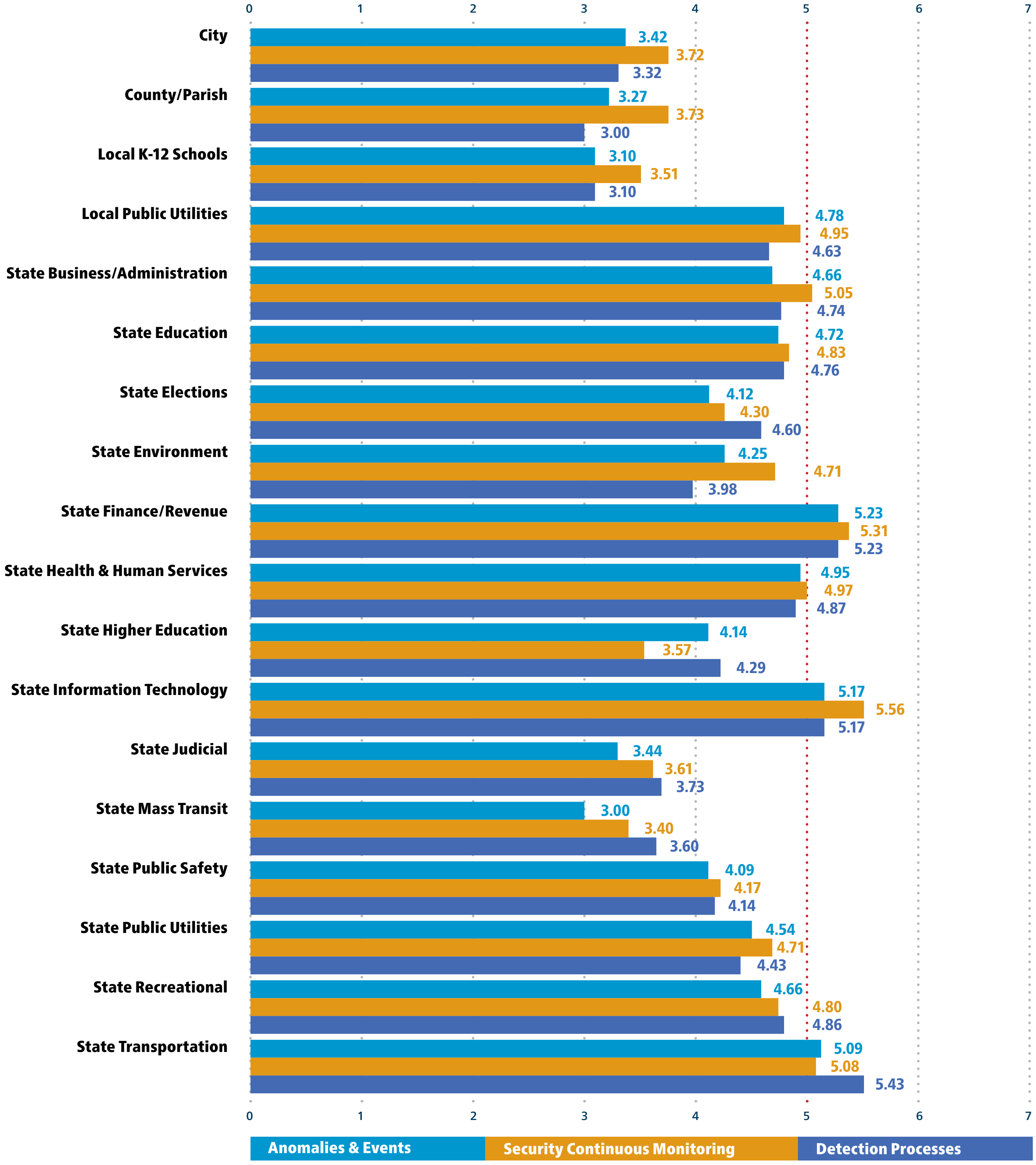


***Figure 33*** *above represents the overall average for each of the sub-sectors across the Detect categories.*

## 2017 Sub-Sector Respond Categories

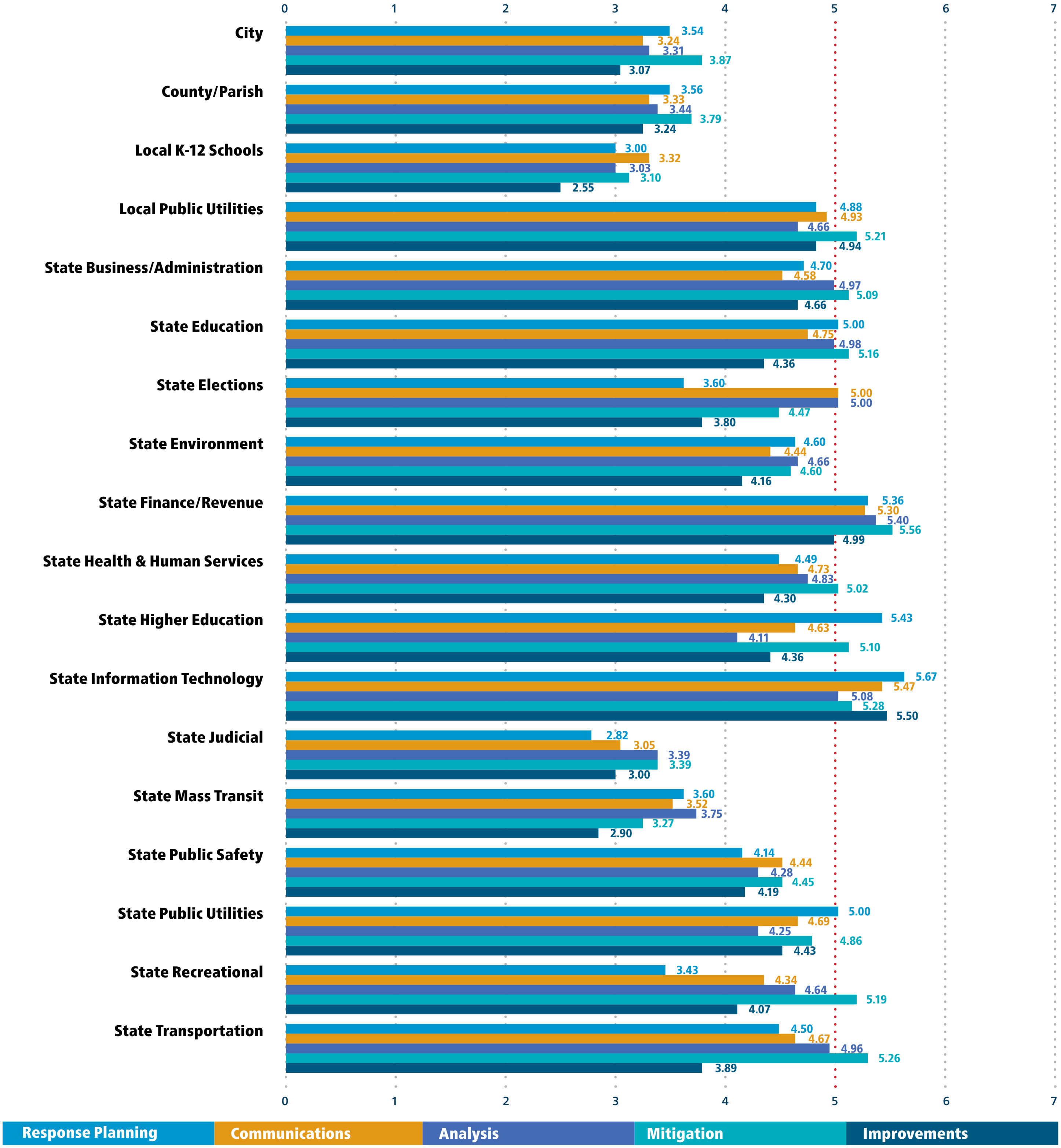


***Figure 34*** *above represents the overall average for each of the sub-sectors across the Respond categories.*

## 2017 Sub-Sector Recover Categories

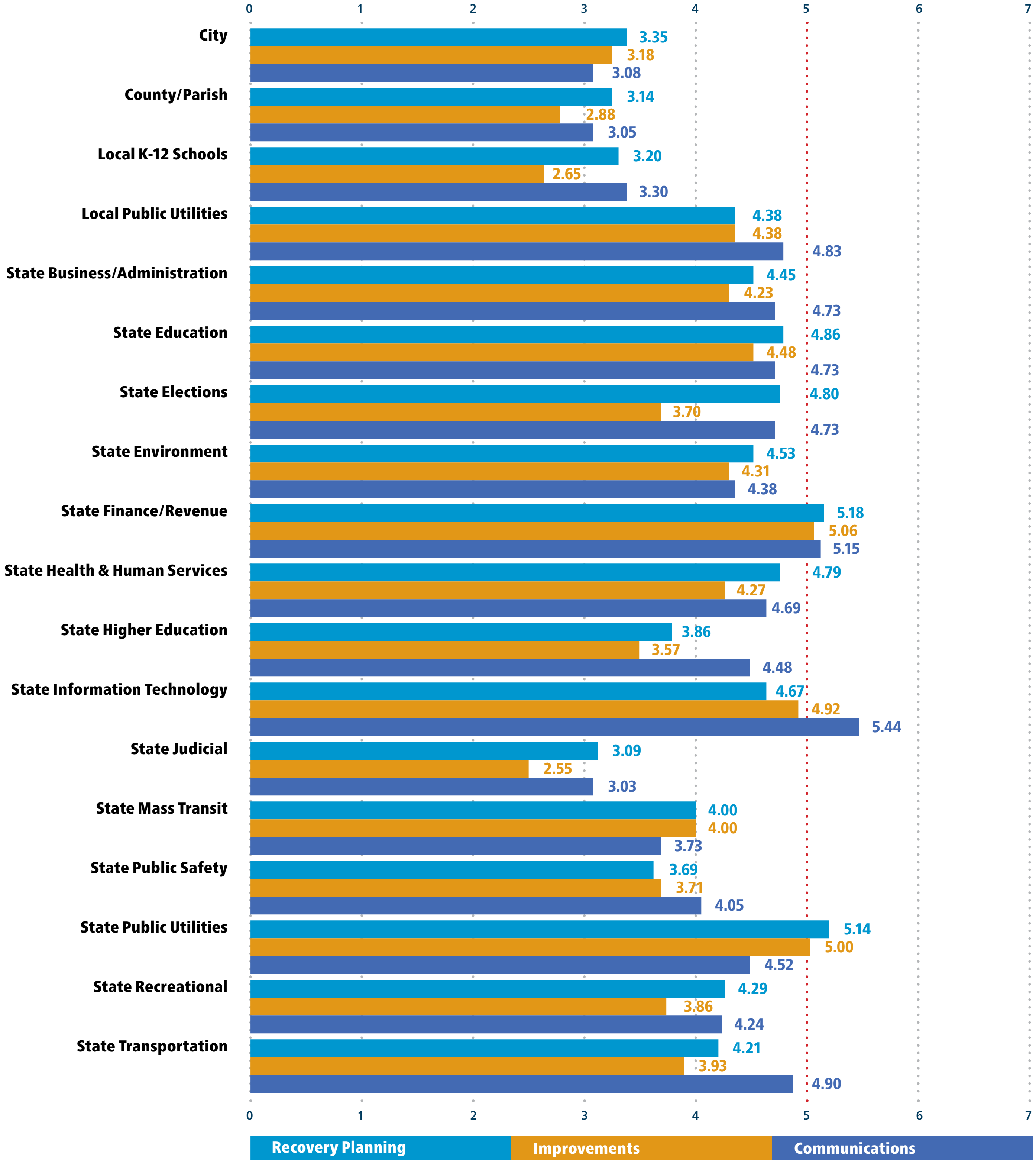


***Figure 35*** *above represents the overall averages for each of the sub-sectors across the Recover categories.*

*Notes:*

*Notes:*

010
0100111001100001011