VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
October 30, 2024 - 10am
VITA, Mary Jackson Boardroom

Agenda

Call to Order and Welcome	Mike Watson Chief Information Security Officer
Review of Agenda	Staff
Approval of August & September Minutes	Staff
Presentation on Assessment Data	Mary Fain
Discussion on Allocation of Year One & Year Two Spending	Discussion, led by Chair
Vote on Authorization of Spending	Staff
Public Comment	
Other Business	Staff
Adjourn	

Committee Email - cybercommittee@vita.virginia.gov

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
August 21, 2024 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

Committee contact address: cybercommittee@vita.virginia.gov

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:03 am. Mr. Watson welcomed the new member: Uma Marques, who is replacing Benjamin Shumaker in the seat for local government. Mr. Watson also mentioned that Adrian Compton has resigned from his seat as tribal representative.

Presiding:

Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present In-Person:

Diane Carnohan, Chief Information Security Officer, Virginia Department of Education

Robbie Coates, Director, Grant Management and Recovery, VDEM

Charles DeKeyser, Major, Virginia Army National Guard.

Charles Huntley, Director of Technology, County of Essex

Derek M. Kestner, Information Security Officer, Supreme Court of Virginia

Uma Marques, Information Technology Director, Roanoke County Government

Ken Pfeil, Chief Data Officer, Commonwealth of Virginia

Brandon Smith, Chief Information Officer, Department of Elections

Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services

Members Participating Remotely:

Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Mr. Dent and Mr. Willams participated remotely because her principal residence is more than 60 miles from the meeting location.

Members Not Present:

Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black.

Staff Present:

Erica Bland, Manager, IT Security Governance and Compliance, Virginia IT Agency

Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency

Patrick Disney, Coordinator Legal & Legislative Services, Virginia IT Agency

Sam Taylor, PR & Marketing Specialist, Virginia IT Agency

Amy Judd, Records Management and Compliance Specialist, Virginia IT Agency

Amma Abbey, Legal Compliance & Policy Specialist, Virginia IT Agency

Atrayo Harper, Graphic Design Specialist, Virginia IT Agency

Review of Agenda:

Mr. Disney provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:

The May 15th meeting minutes were displayed. Upon a motion by Mr. Smith and duly seconded by Mr. Pfeil, the committee unanimously voted to adopt the May 15th meeting minutes.

Approval of Electronic Participation Policy:

The policy was displayed on the screen and summarized by Mr. Heslinga. Upon a motion by Mr. Kestner seconded by Ms. Carnohan, the Council unanimously voted to adopt the updated electronic participation policy.

Financial Update and Update on Assessments Projects

Ms. Fain gave an update on finances. Out of year 1 funds, there is currently $2.1M unallocated so far. $66k on management and administration has been fully allocated. $550k has been allocated for the locality SOC RFP (which is proceeding but early in the RFP process) and programmatic expenses and working with public colleges and universities also fall in this bucket of funding.

Ms. Fain also gave an update on the assessments project. Its status is currently green, but sign off from some localities is taking longer than expected. Actual assessments are on schedule, as are acceptance reviews by VITA security staff – 54 assessments have been completed since Aug. 16, and 32 have been reviewed by our staff.

Preparing for Project Submissions

Mr. Watson proposed an open question to the committee to inform how funds should be identified for each objective or priority in the available funding years. The committee discussed assessment data needed to make decisions on future findings; the conversation will continue in the September meeting.

Public Comment Period:

There were no public commenters.

Other Business:

Mr. Watson opened the floor for other business. Mr. Disney reminded members to complete their travel forms and that the next meeting is scheduled for September 18th at 10am.

Adjourn

Upon a motion by Mr. Kestner and seconded by Mr. Smith, the meeting was adjourned at 11:32 am.

VIRGINIA IT AGENCY

Virginia Cybersecurity Planning Committee
September 18, 2024 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom, Richmond, VA, 23225

Committee contact address: cybercommittee@vita.virginia.gov

Call to Order:

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:01 am.

Presiding:

Michael Watson, Committee Chair, Chief Information Security Officer, Virginia IT Agency

Members Present In-Person:

Diane Carnohan, Chief Information Security Officer, Virginia Department of Education

Robbie Coates, Director, Grant Management and Recovery, VDEM

Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems

Charles Huntley, Director of Technology, County of Essex

Ken Pfeil, Chief Data Officer, Commonwealth of Virginia

Glendon Schmitz, Chief Information Security Officer, Department of Behavioral Health and Developmental Services

Members Participating Remotely:

Uma Marques, Information Technology Director, Roanoke County Government

Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Wesley Williams, Executive Director of Technology, Roanoke City Public Schools

Ms. Burgin Waller, Ms. Marques, and Mr. Willams participated remotely because her principal residence is more than 60 miles from the meeting location.

Members Not Present:

Michael Dent, Chief Information Security Officer, Fairfax County Department of Information Technology

Charles DeKeyser, Major, Virginia Army National Guard

Derek M. Kestner, Information Security Officer, Supreme Court of Virginia

Brandon Smith, Chief Information Officer, Department of Elections

Lisa Walbert, Deputy Secretary of Public Safety and Homeland Security

Staff Present:

Mary Fain, Program Manager, Virginia IT Agency

Erica Bland, Manager, IT Security Governance and Compliance, Virginia IT Agency

Joshua Heslinga, Director of Legal & Legislative Services, Virginia IT Agency

Patrick Disney, Coordinator Legal & Legislative Services, Virginia IT Agency

Sam Taylor, PR & Marketing Specialist, Virginia IT Agency

Review of Agenda:

Mr. Disney provided an overview of the agenda and corresponding items in the digital meeting packets.

Approval of Minutes:

Because there was not a physical quorum and the meeting had not been noticed as an all-virtual meeting, there was no vote to approve the minutes. That will be done at the next meeting.

Financial Update and Update on Assessments Projects

Ms. Fain gave an update on finances. For program year 1 (federal FY2022), there are $71k in actual M&A expenses, $550k allocated for statewide projects, and $1.8M allocated for local passthrough projects, leaving ~$2M remaining for passthrough grants. Year 2 (federal FY2023) funds all remain available: ~$500k M&A (5%), $1.6 statewide (15%), and $8.7M local passthrough (80%). Program year 2 represents the largest grant award year for the program.

Ms. Fain also gave an update on the assessments project. 99% of localities have been scheduled for assessments. 123 out of 170 have been delivered for review by VITA security, 85 have been completed. A breakdown of locality characteristics for the was also given for the assessments accepted to date: 46% are public school districts, 28% are from local government and 26% are other. 61% are rural, 28% are non-rural and 12% are both.

Ms. Fain also gave an update on timelines. Assessments are wrapping up in early October, then the beginning to build out tools and materials for the next round of projects will start. Approximately December – January, it is expected that applications will be submitted, with award decisions, any related RFPs, and project execution to begin in early 2025.

Preparing for Project Submissions

Mr. Watson proposed for the Committee to discuss how funds should be identified or used for each objective or priority in the available funding years and what information the Committee needs to make those decisions.

Some notes regarding that discussion: Statistics covering the data on the expected impact of recommendations in these assessments were displayed. It was noted that school districts have higher existing cyber baselines and more resources from federal and state funding that have given them a higher level of cyber resilience so far. Criteria needs to be finalized by the October meeting, as far as prioritizing objectives and approving use of funding. Those who have completed assessments will have done most of the application work already, so we likely can open for applications quickly and the end of year may be a good time to do this. Many of the localities will need implementation assistance. Assessors and localities generally agree on where they think they are and what implementation model should be chosen. Assessors and localities generally agree between recommended objectives and interest in working on these objectives. The Committee's decisions likely will focus on those sub-categories that can make the biggest impact and utilize funding for largest majority increase impact areas.

Public Comment Period:

There were no public commenters.

Other Business:

Mr. Watson opened the floor for other business. Mr. Disney reminded members to complete their travel forms and that the next meeting is scheduled for October 30th at 10am. Staff will follow up with Committee members to emphasize the need for attendance and a physical quorum at that meeting.

Adjourn

Upon a motion by Mr. Pfeil and seconded by Ms. Carnohan, the meeting was adjourned at 11:17 am.

VIRGINIA IT AGENCY

VIRGINIA DEPARTMENT OF EMERGENCY MANAGEMENT

State and Local Cybersecurity Grant Program

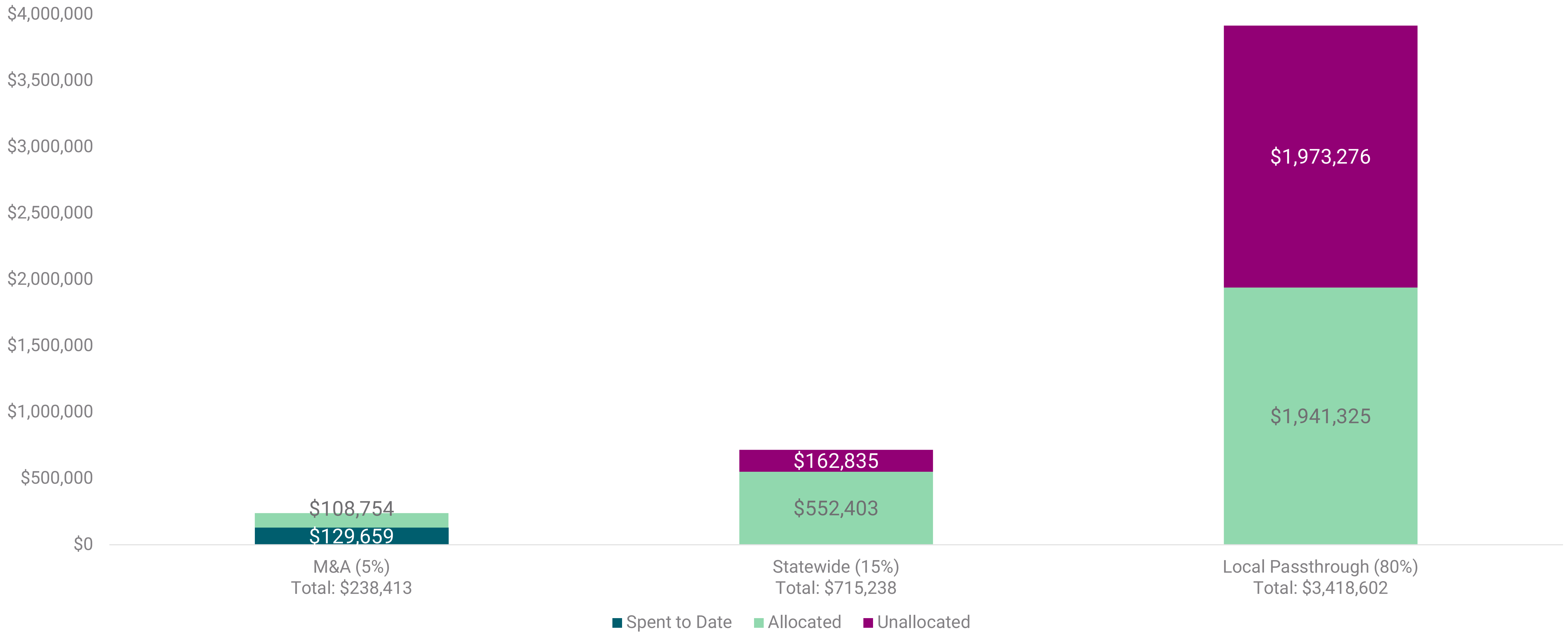
Cybersecurity Plan Capability Assessment Project Update

As of October 25, 2024

Financial Update

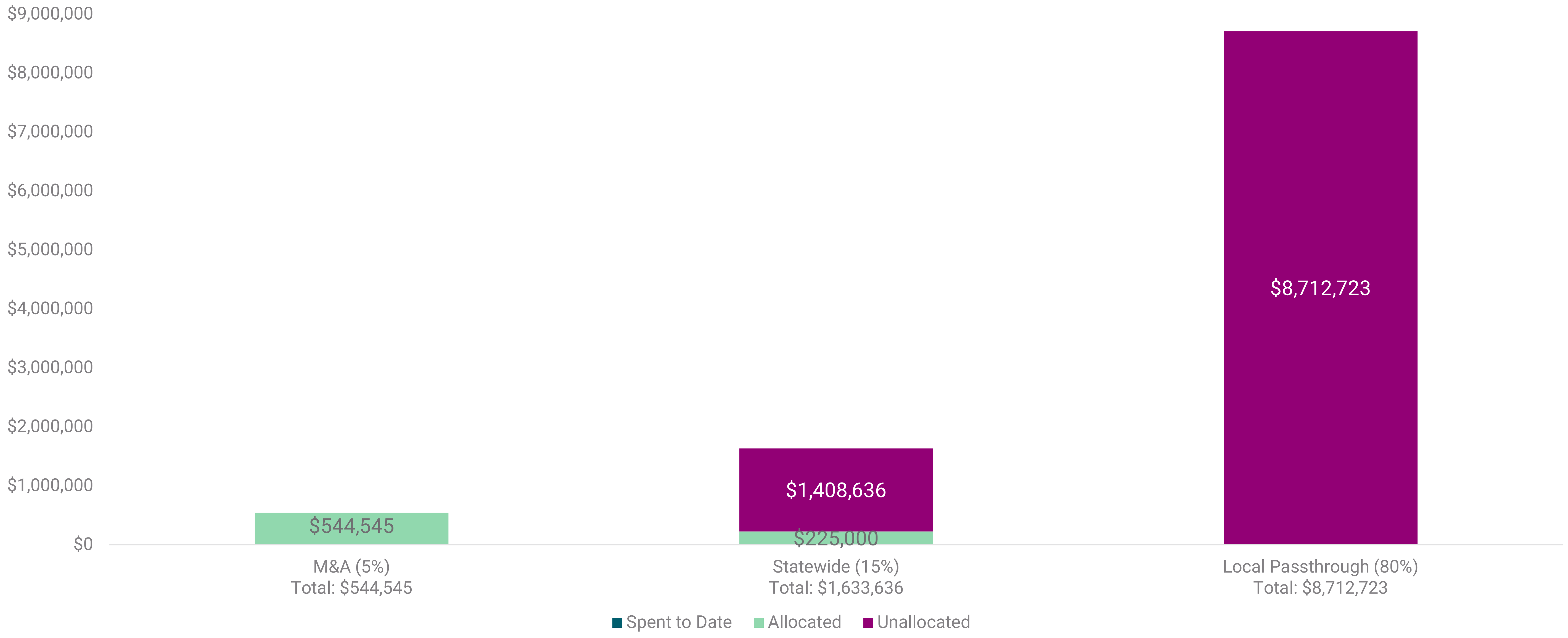
Program Year 1 (2022) Financial Update

Period of Performance End: Nov. 30, 2026



Program Year 2 (2023) Financial Update

Period of Performance End: Nov. 30, 2027

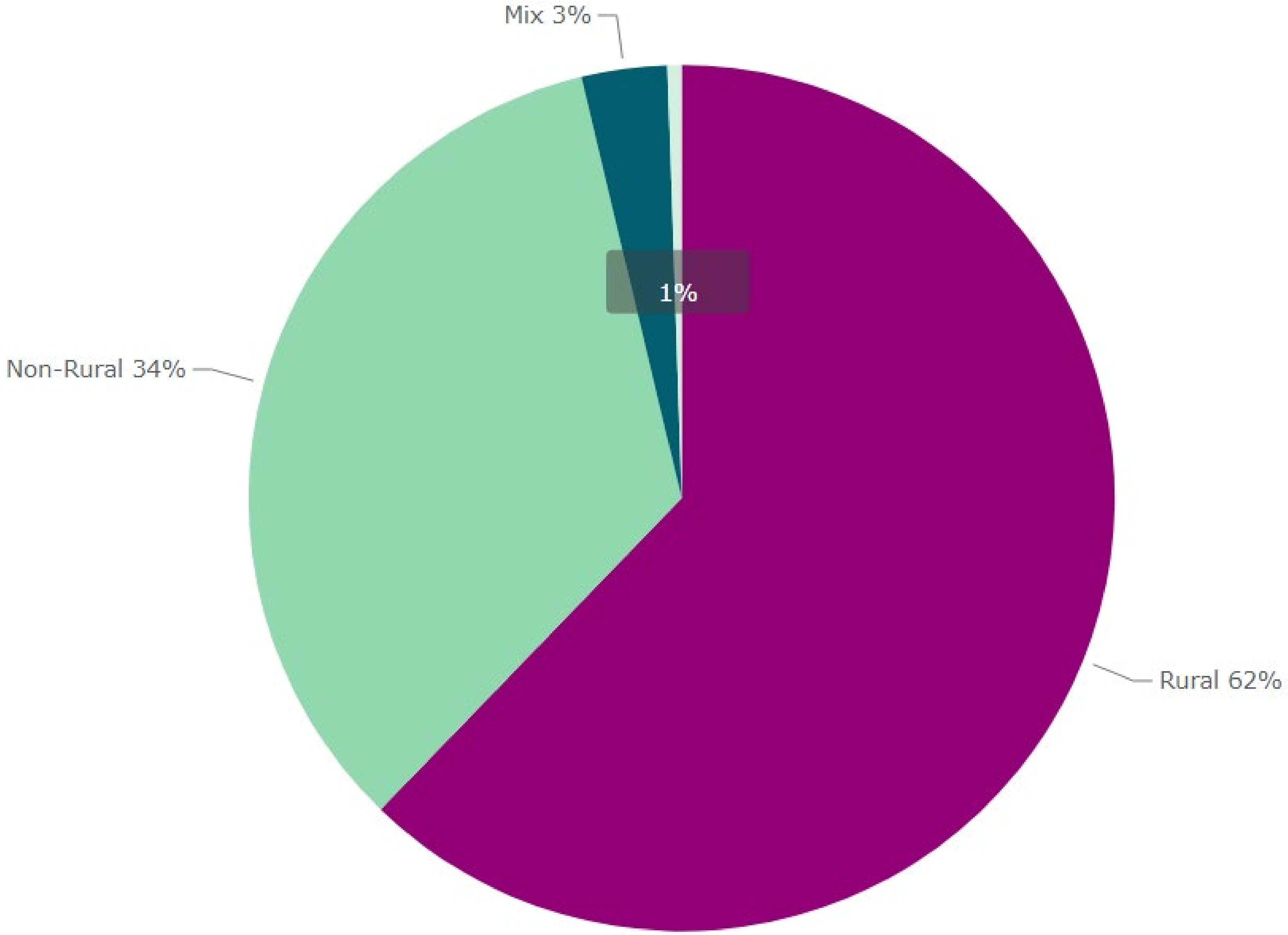


Assessment Data Findings

Summary

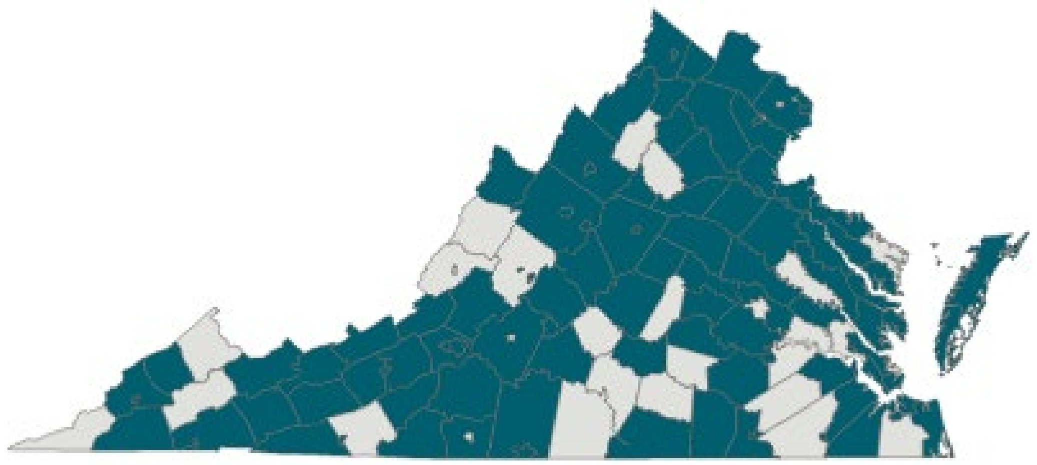
Rural Area Pass-Through Requirement

Exceeded by 37% for this project

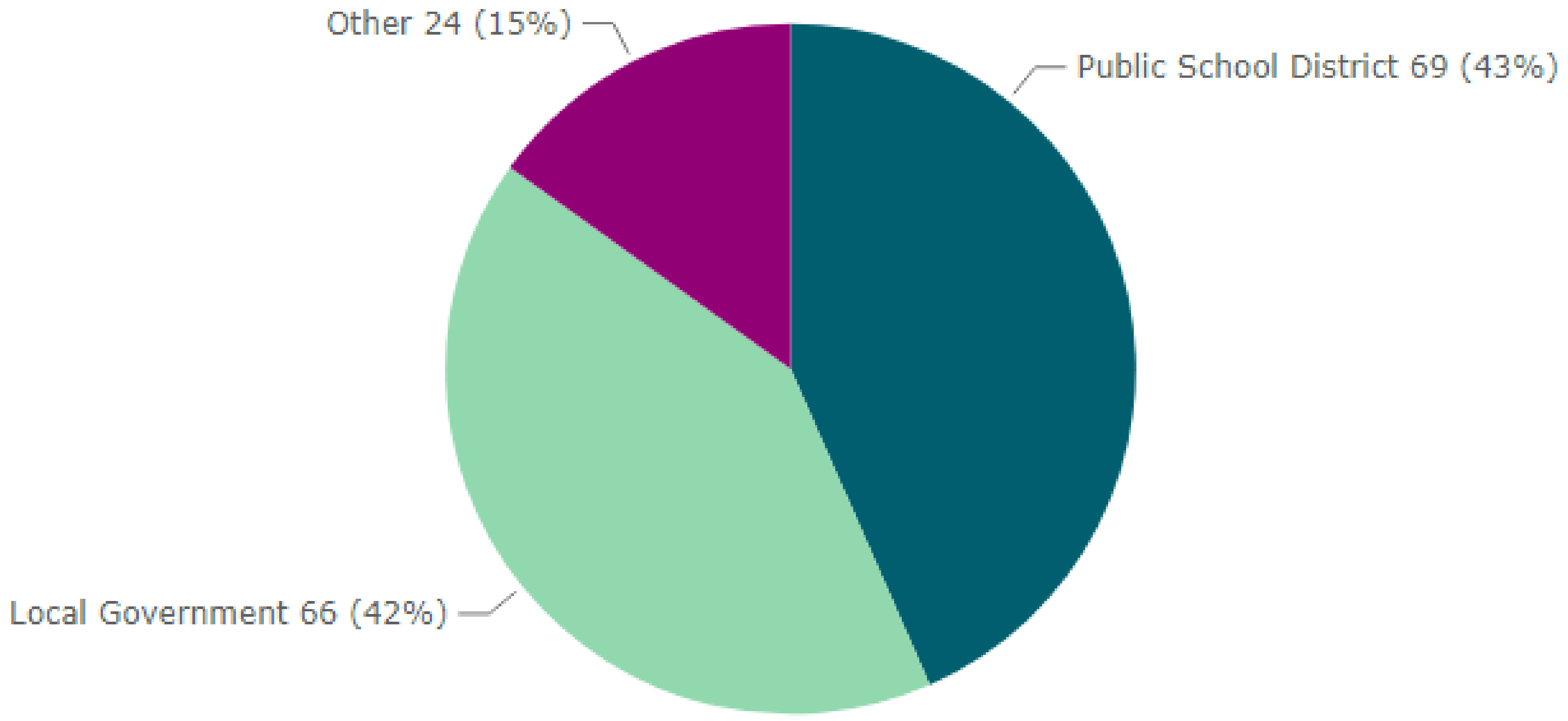


Accepted Assessments – Locality Characteristics

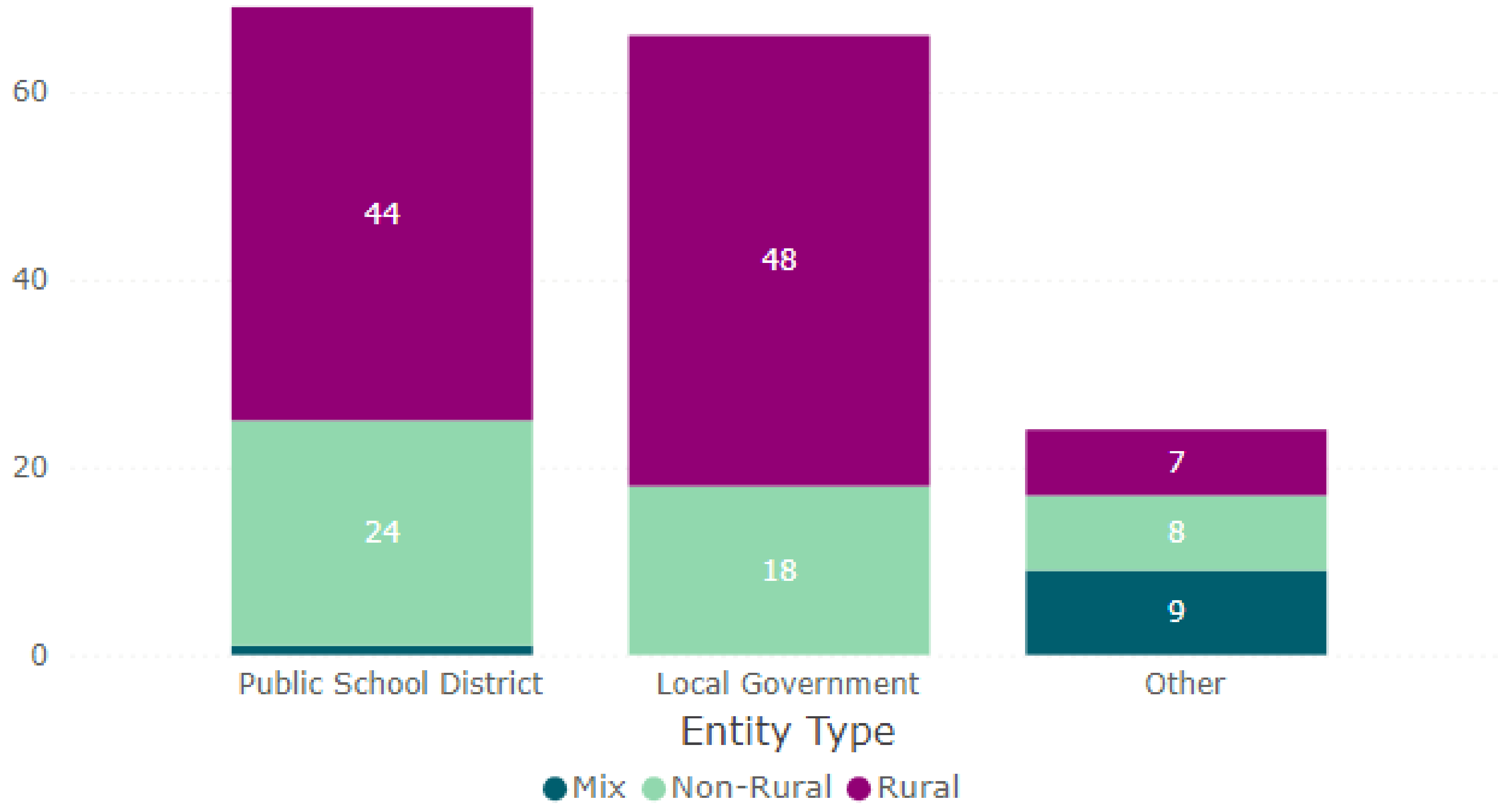
Geographic Reach



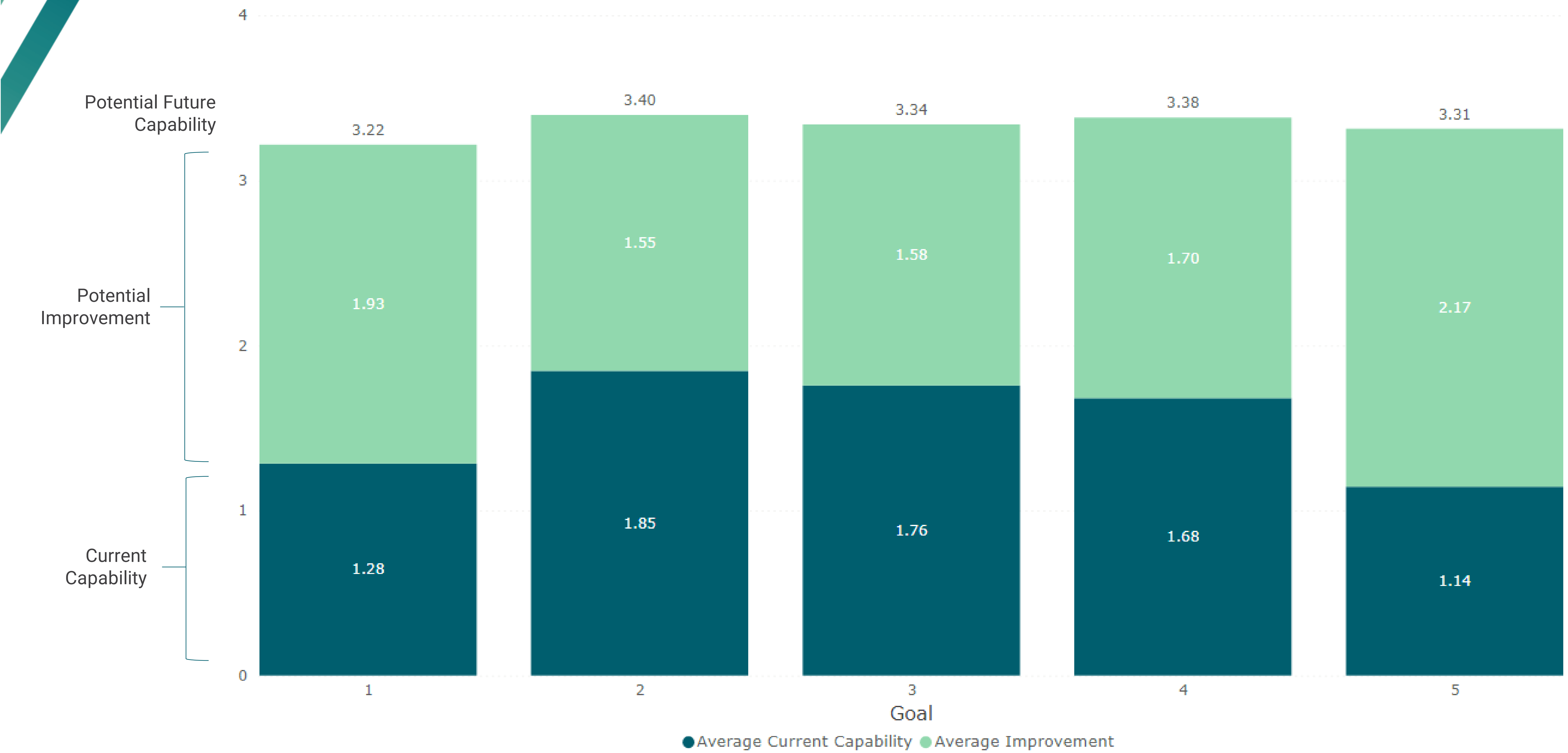
Entity Types



Rural vs. Non-Rural Entities

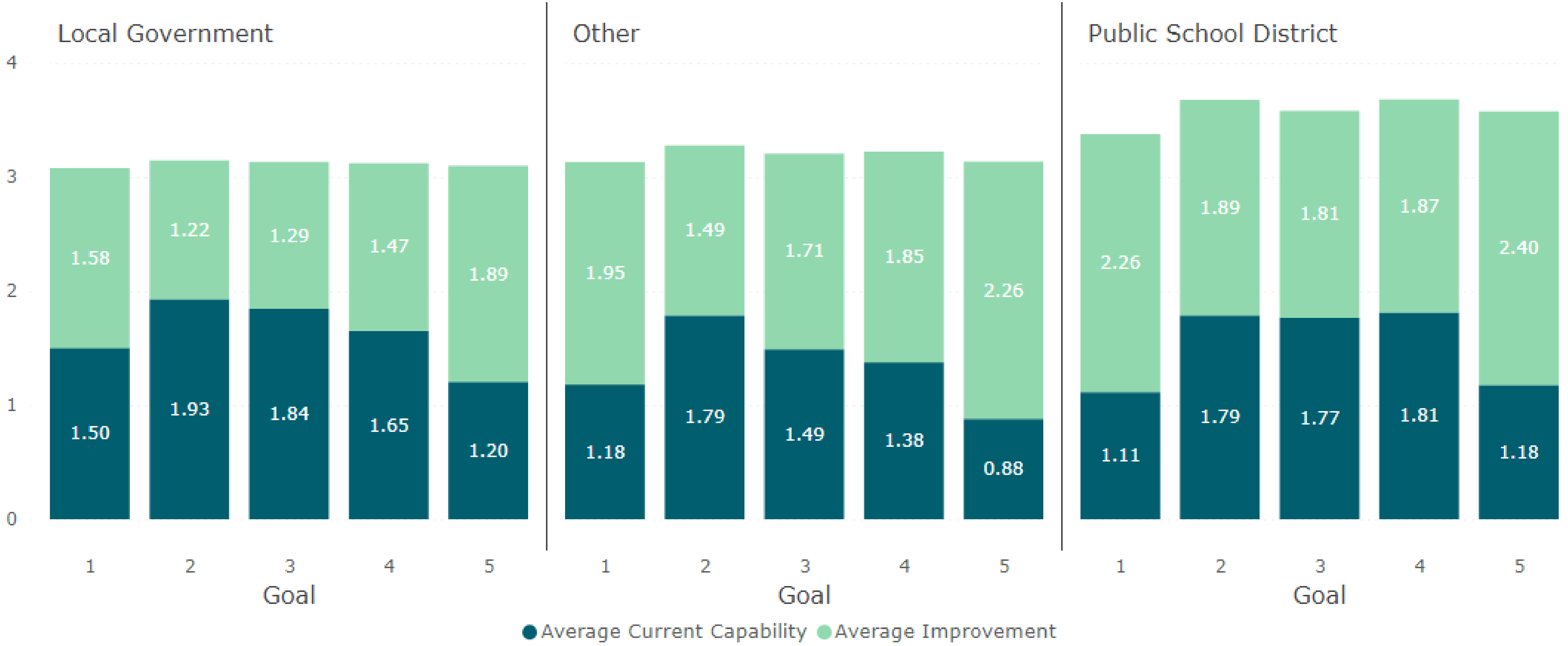


Impact of Capability Improvements



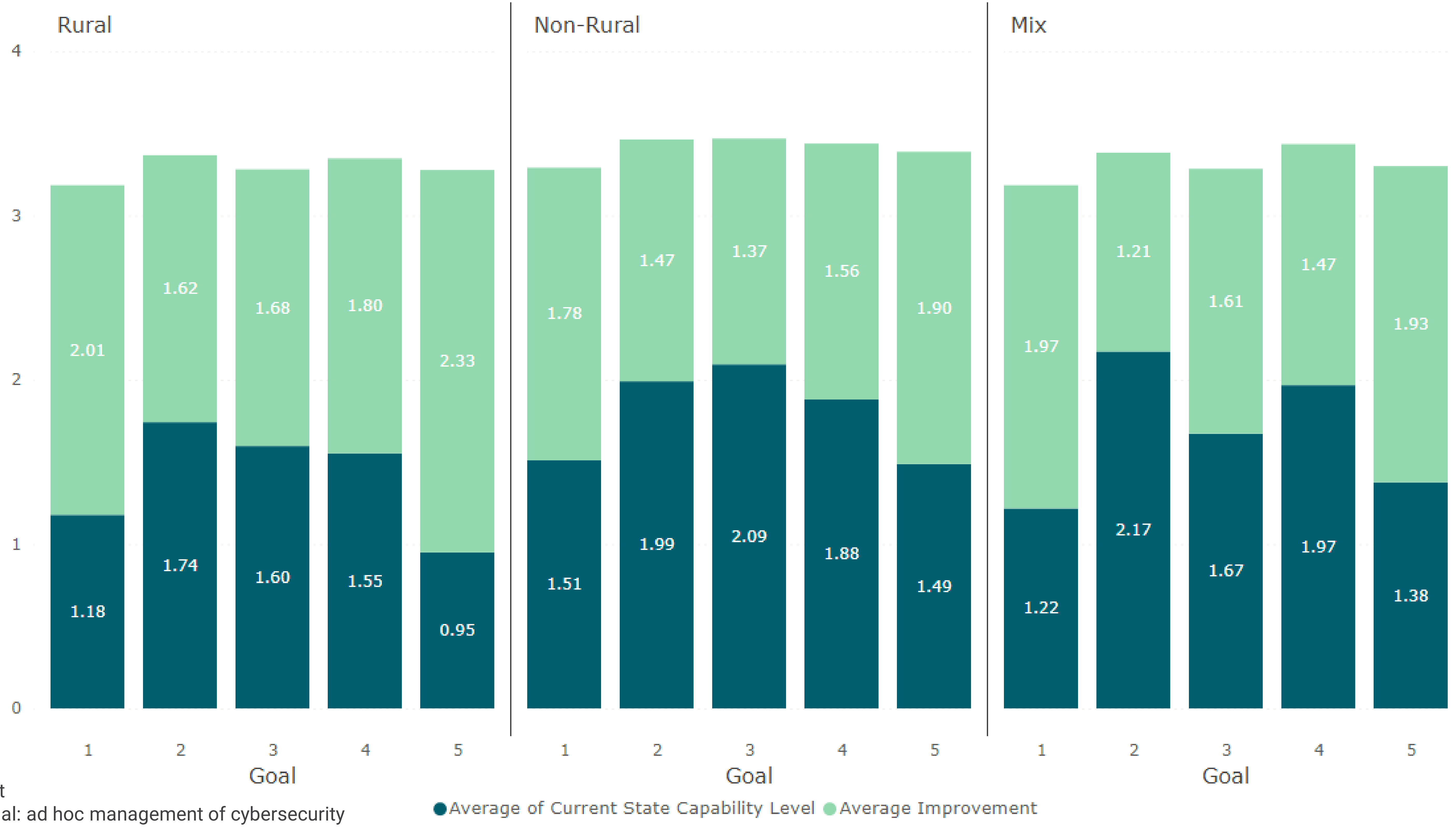
0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

Impact of Capability Improvements By Entity Type



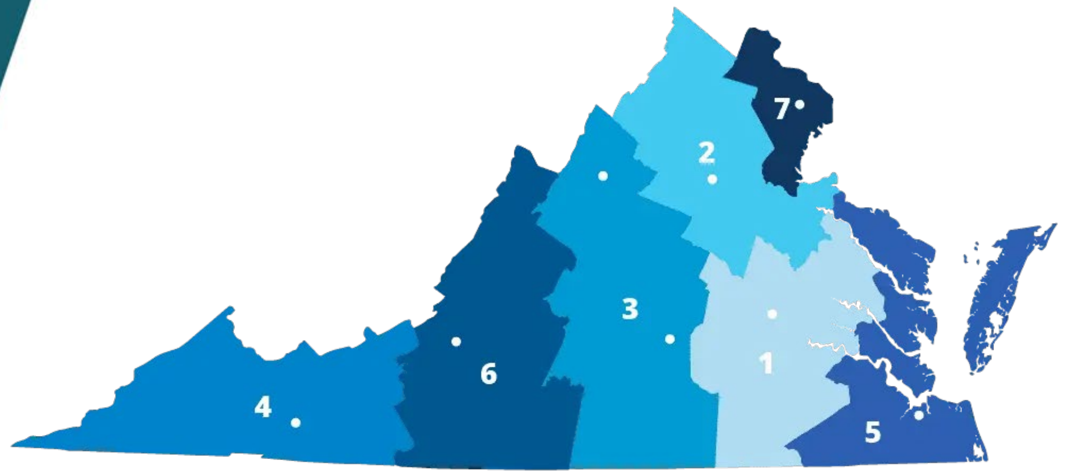
0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

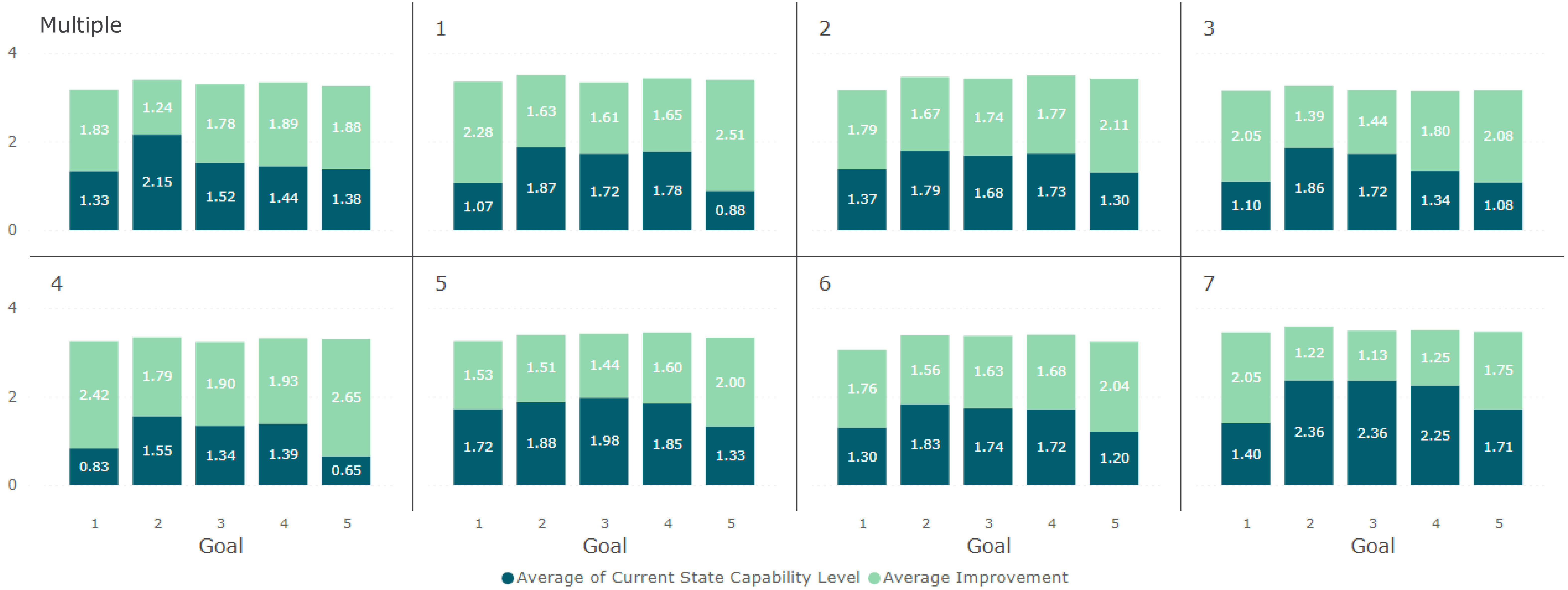
Impact of Capability Improvements By Rural vs. Non-Rural



0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

Impact of Capability Improvements By VDEM Region

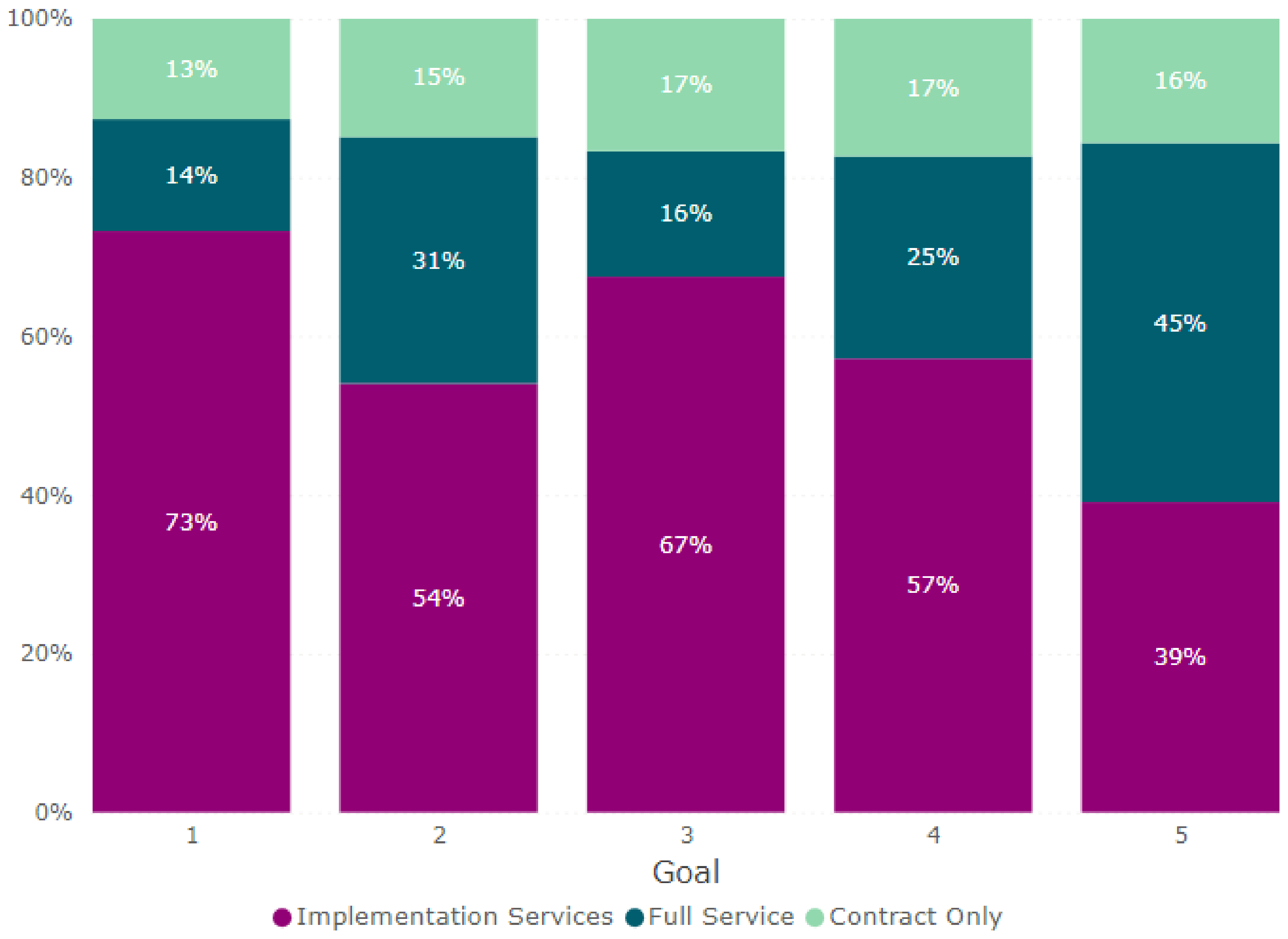




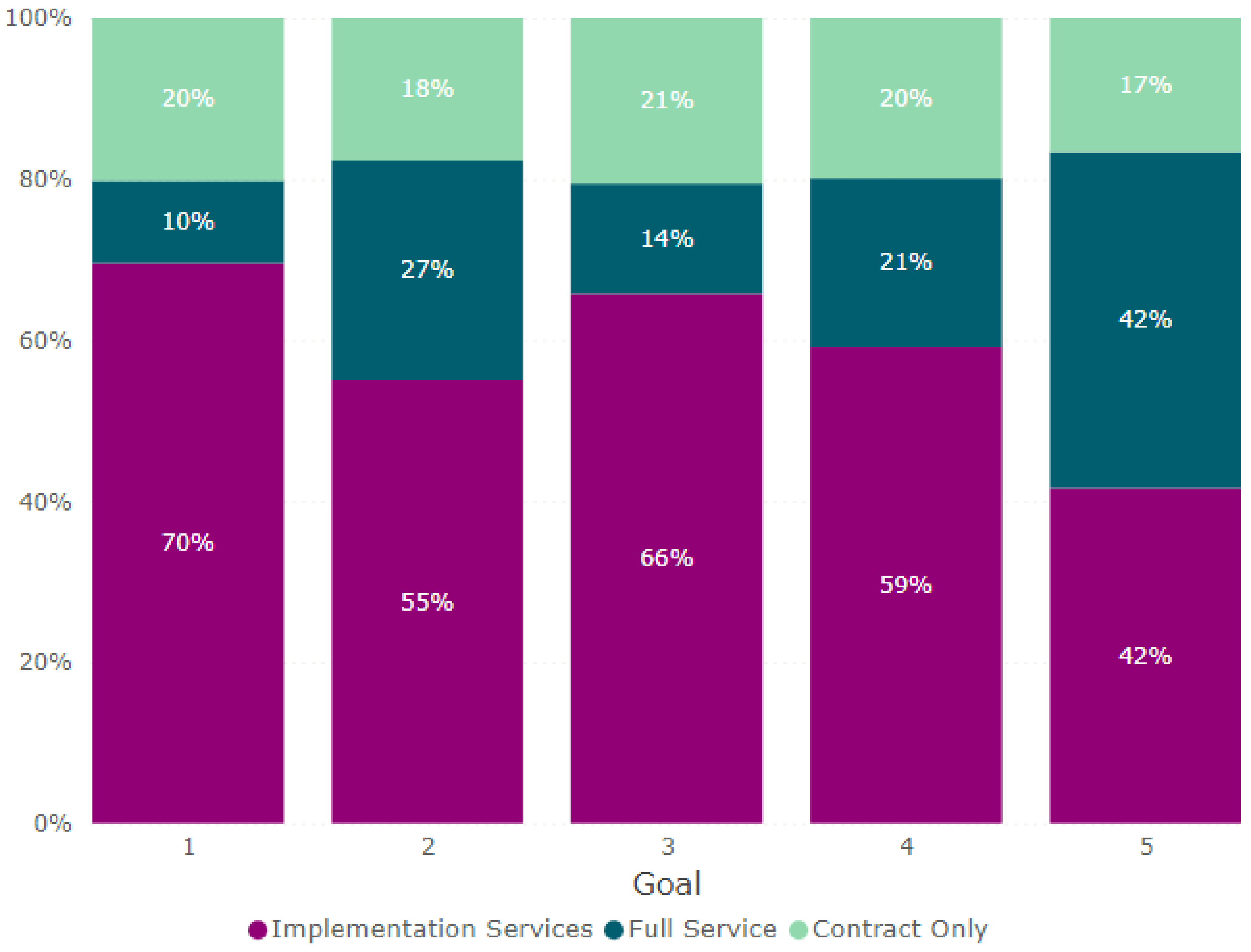
0 – Not present
1 – Foundational: ad hoc management of cybersecurity
2 – Fundamental: policies and procedures in place, limited tools and/or limited usage of tools
3 – Intermediary: enterprise level cybersecurity
4 – Advanced: present across all stakeholders – internal and external to the organization

Implementation Model

Implementation Model - Assessor Recommended



Implementation Model - Organization Preference



- Contract Only – Pre-approved authorized/legal procurement vehicle. The organization is responsible for all aspects of implementation other than establishing the contract.
- Implementation Services – Services needed to stand up the technology or processes of the initiative. Once these services are done the organization becomes responsible for running/managing the implementation.
- Full Service – The organization needs support to build, implement and run the program objective technology or processes. These services require the least amount of support from the organization.

Other Data – General Observations

70%
likelihood of success

- Most goals and associated sub-objectives have at least an ~70% likelihood of success (Success = medium + high)

90%
recommended and interested

- Most goals and associated sub-objectives are at least 90% of assessors recommend and localities are interested

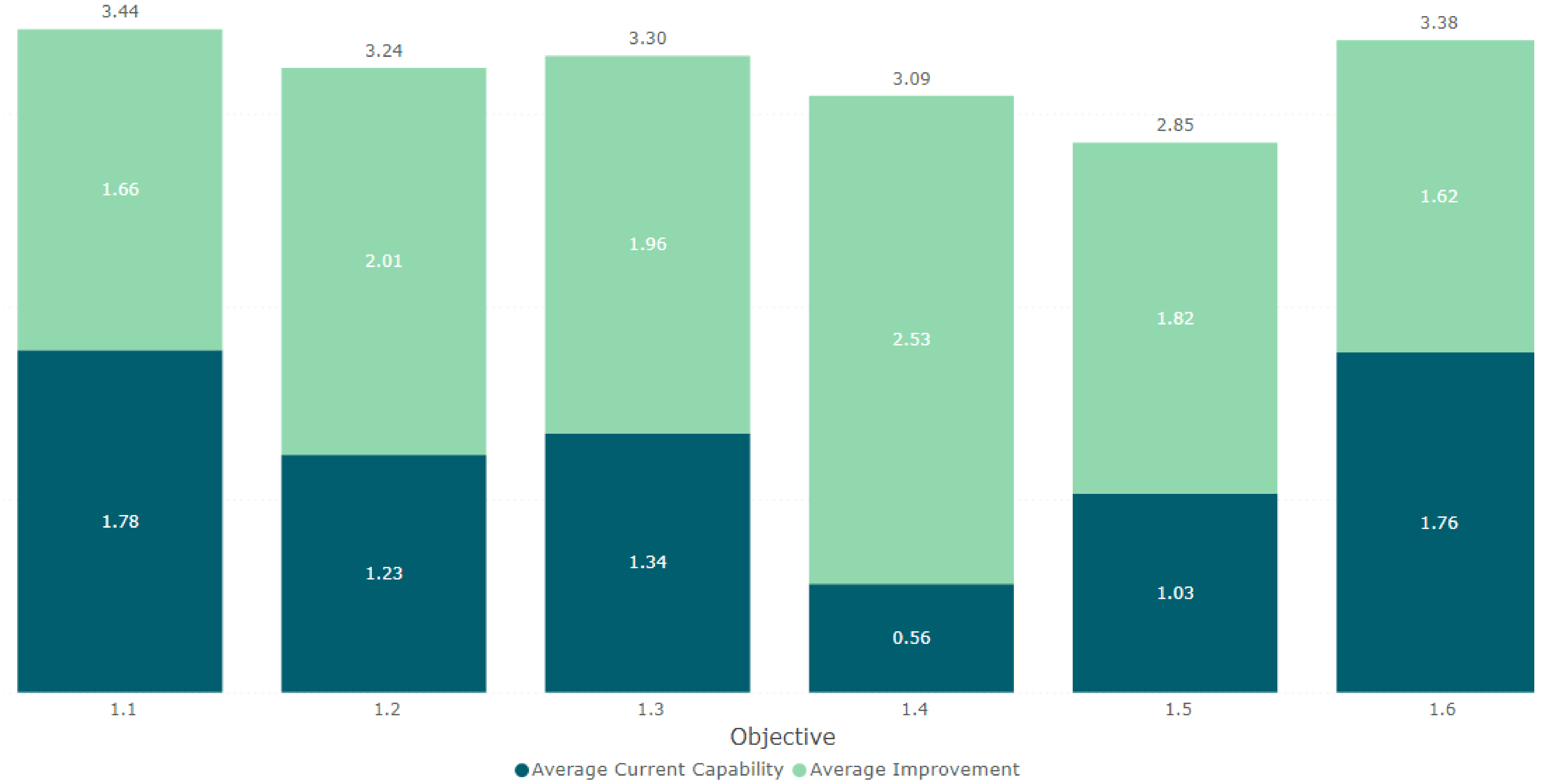
70%
require new funding

- Approximately 70% of entities will require new funding to close goal and associated sub-objective gaps

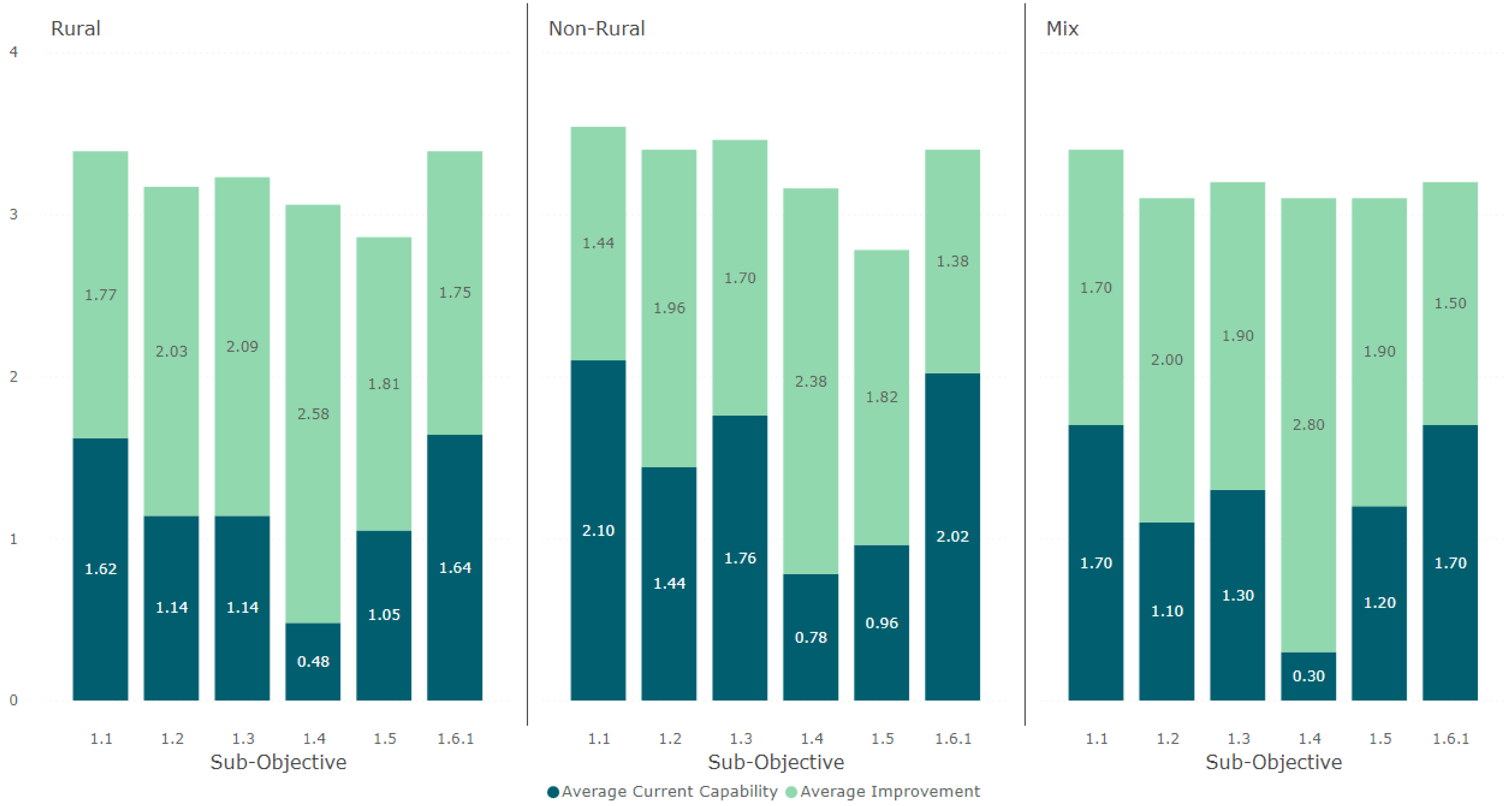
Assessment Data Findings

Goal 1

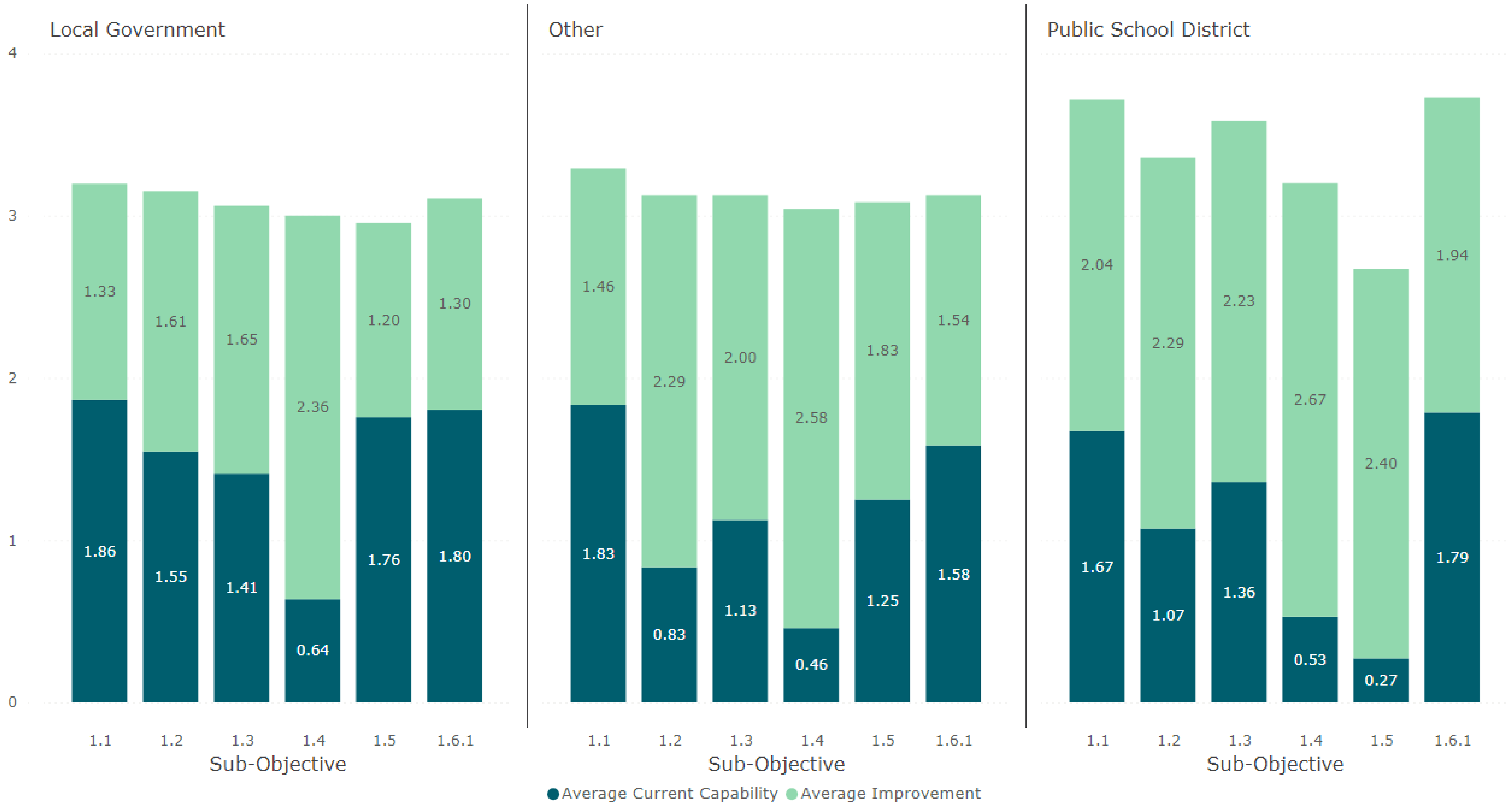
Impact of Capability Improvements



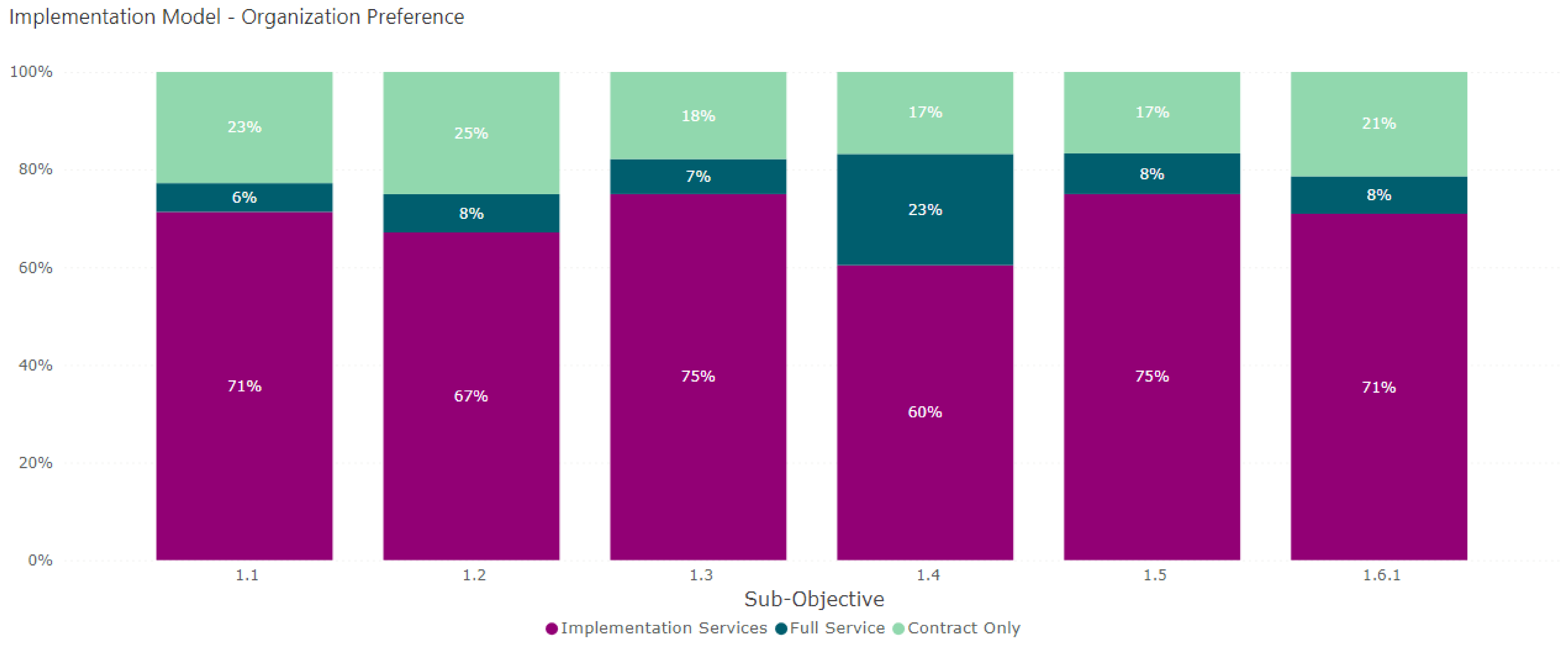
Impact of Capability Improvements
Rural vs. Non-Rural



Impact of Capability Improvements By Entity



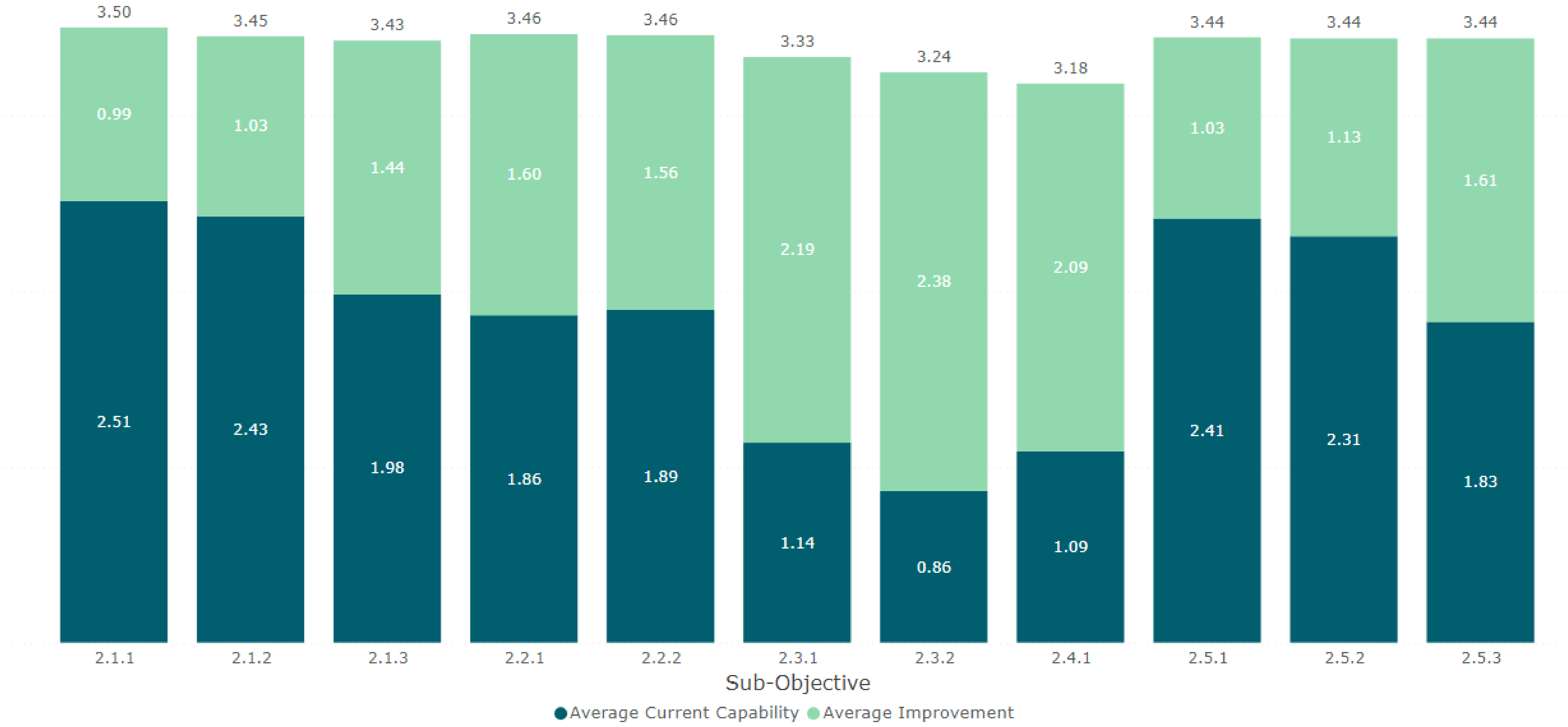
Implementation Model – Organization Preference



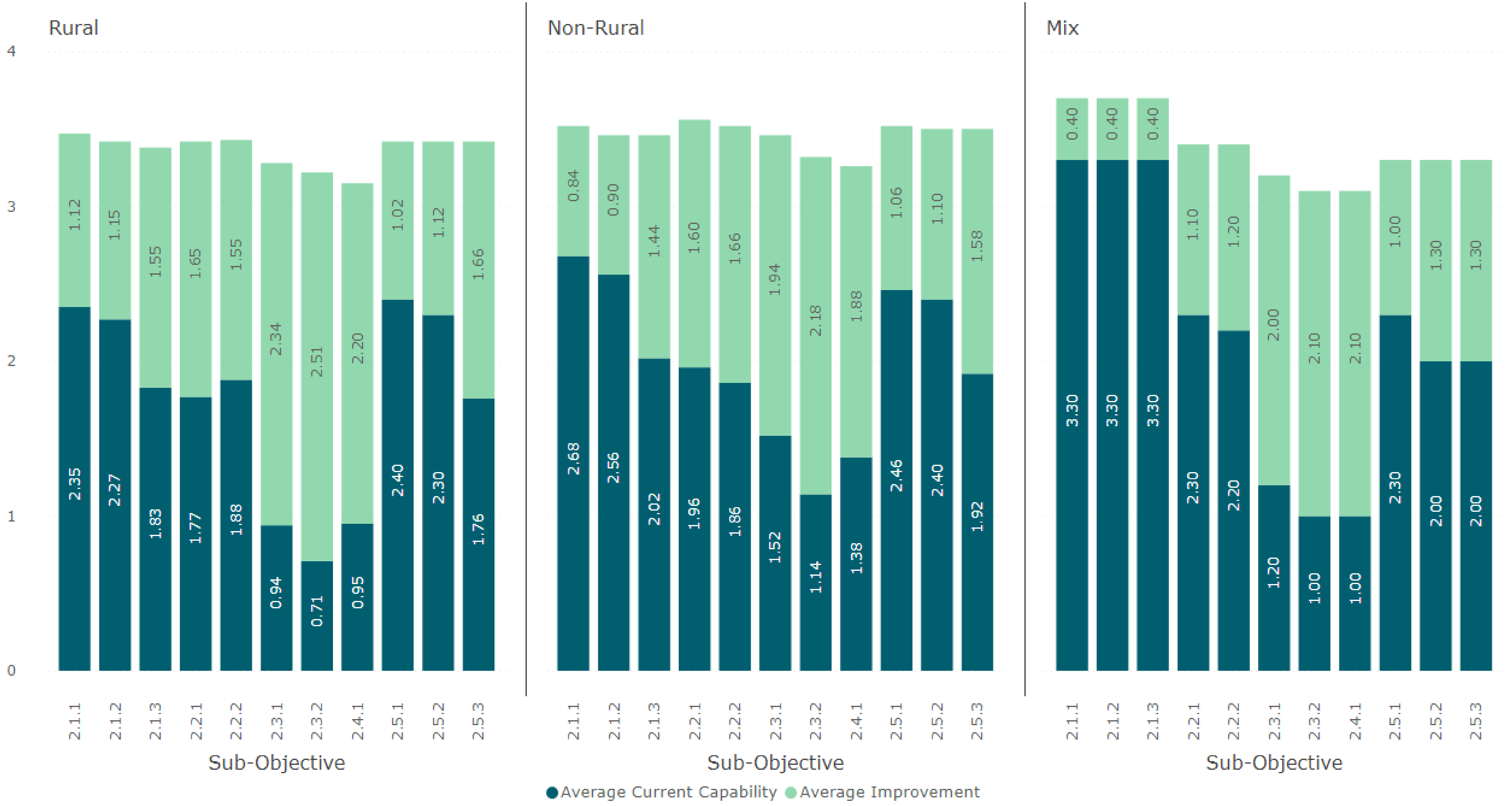
Assessment Data Findings

Goal 2

Impact of Capability Improvements

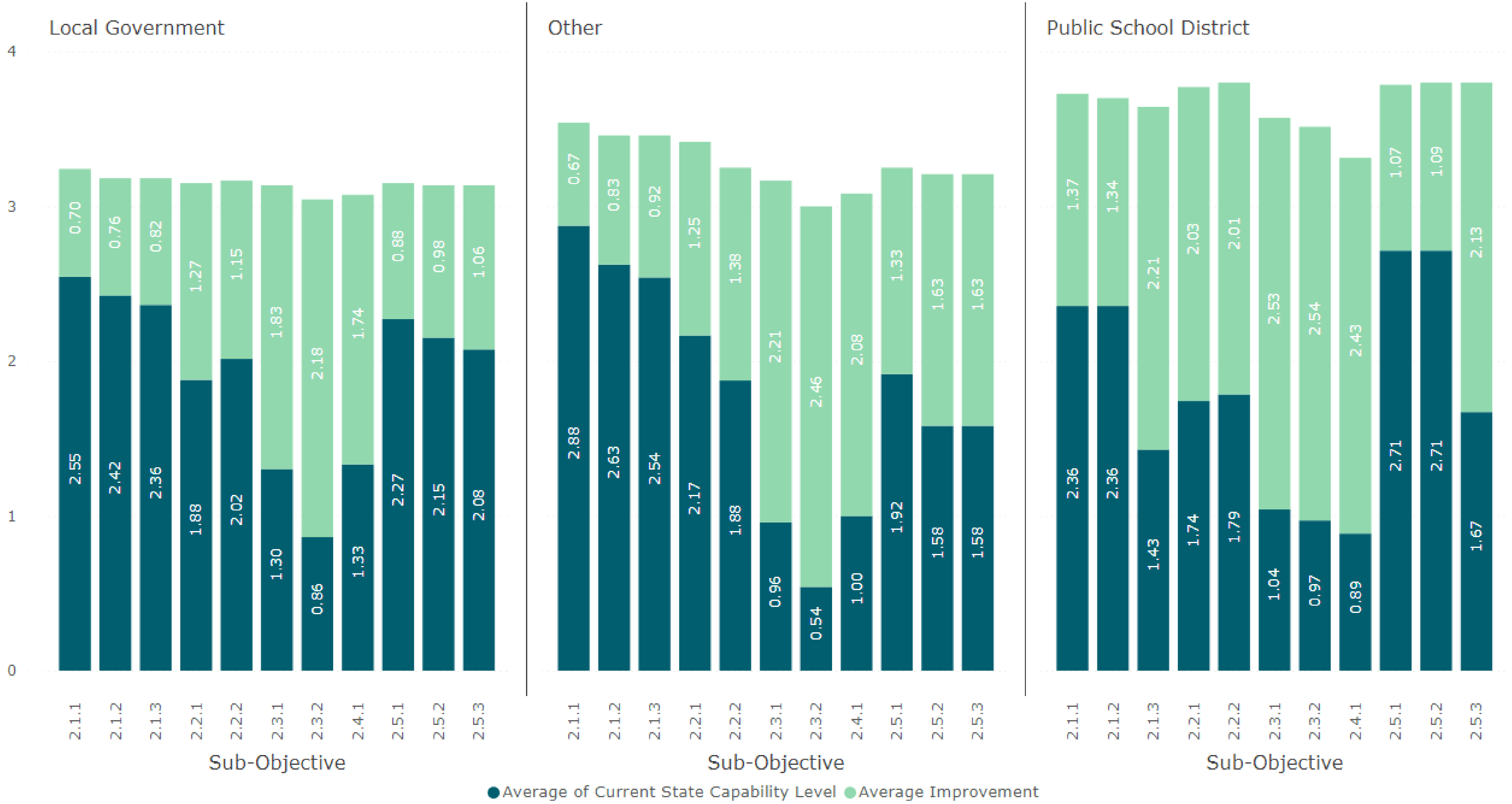


Impact of Capability Improvements Rural vs. Non-Rural

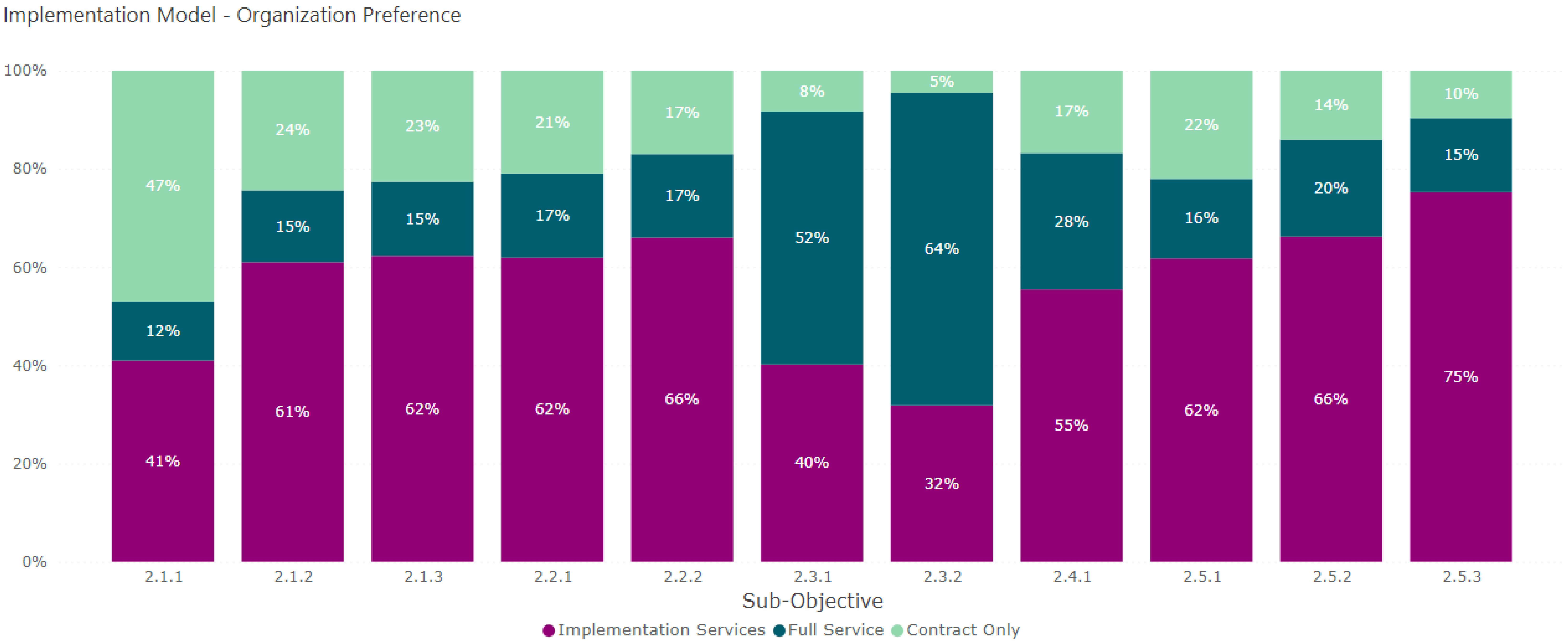


Sub-Objective	Rural Current	Rural Improvement	Non-Rural Current	Non-Rural Improvement	Mix Current	Mix Improvement
2.1.1	2.35	1.12	2.68	0.84	3.30	0.40
2.1.2	2.27	1.15	2.56	0.90	3.30	0.40
2.1.3	1.83	1.55	2.02	1.44	3.30	0.40
2.2.1	1.77	1.65	1.96	1.60	2.30	1.10
2.2.2	1.88	1.55	1.86	1.66	2.20	1.20
2.3.1	0.94	2.34	1.52	1.94	1.20	2.00
2.3.2	0.71	2.51	1.14	2.18	1.00	2.10
2.4.1	0.95	2.20	1.38	1.88	1.00	2.10
2.5.1	2.40	1.02	2.46	1.06	2.30	1.00
2.5.2	2.30	1.12	2.40	1.10	2.00	1.30
2.5.3	1.76	1.66	1.92	1.58	2.00	1.30

Impact of Capability Improvements By Entity



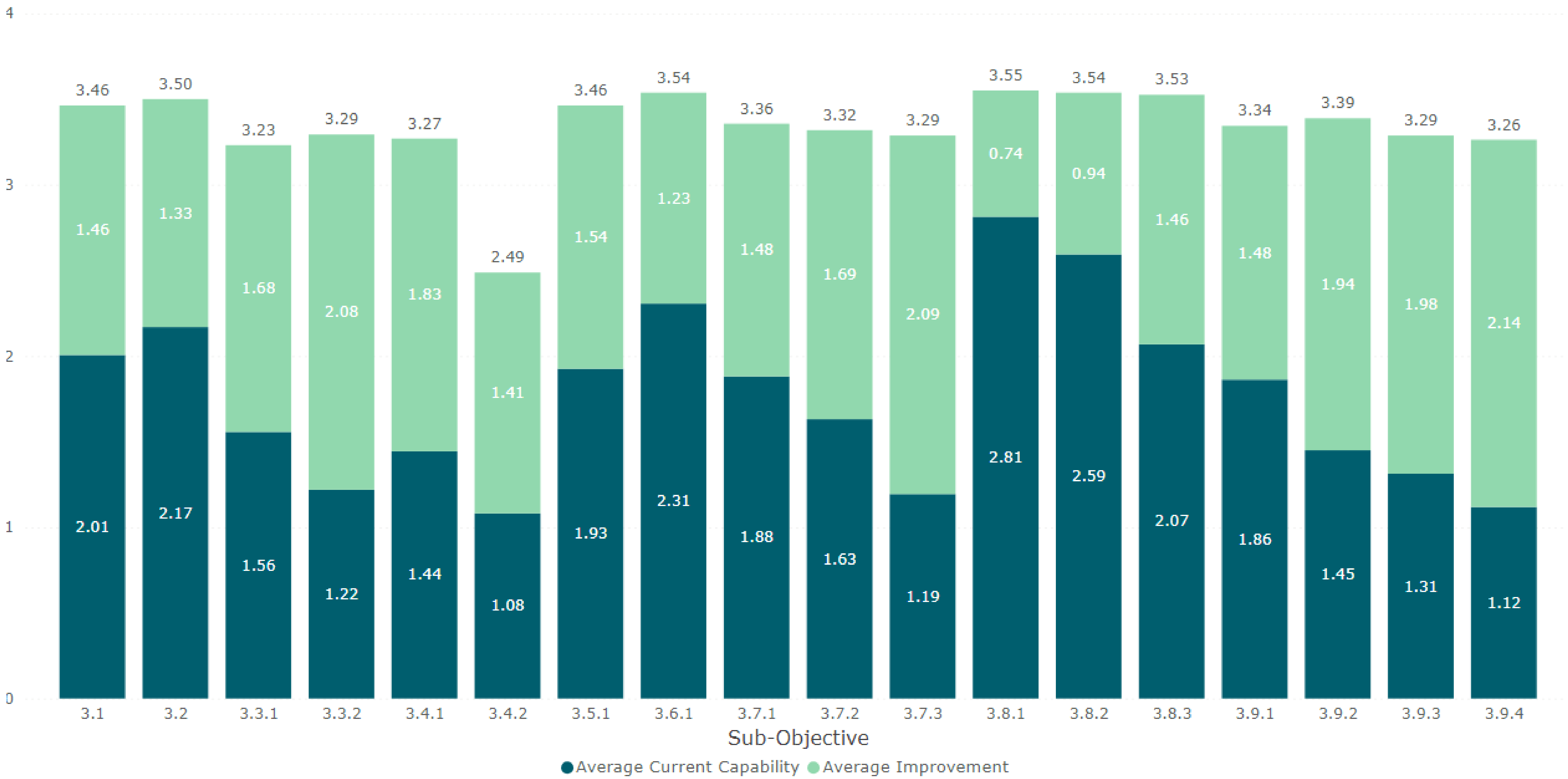
Implementation Model – Organization Preference



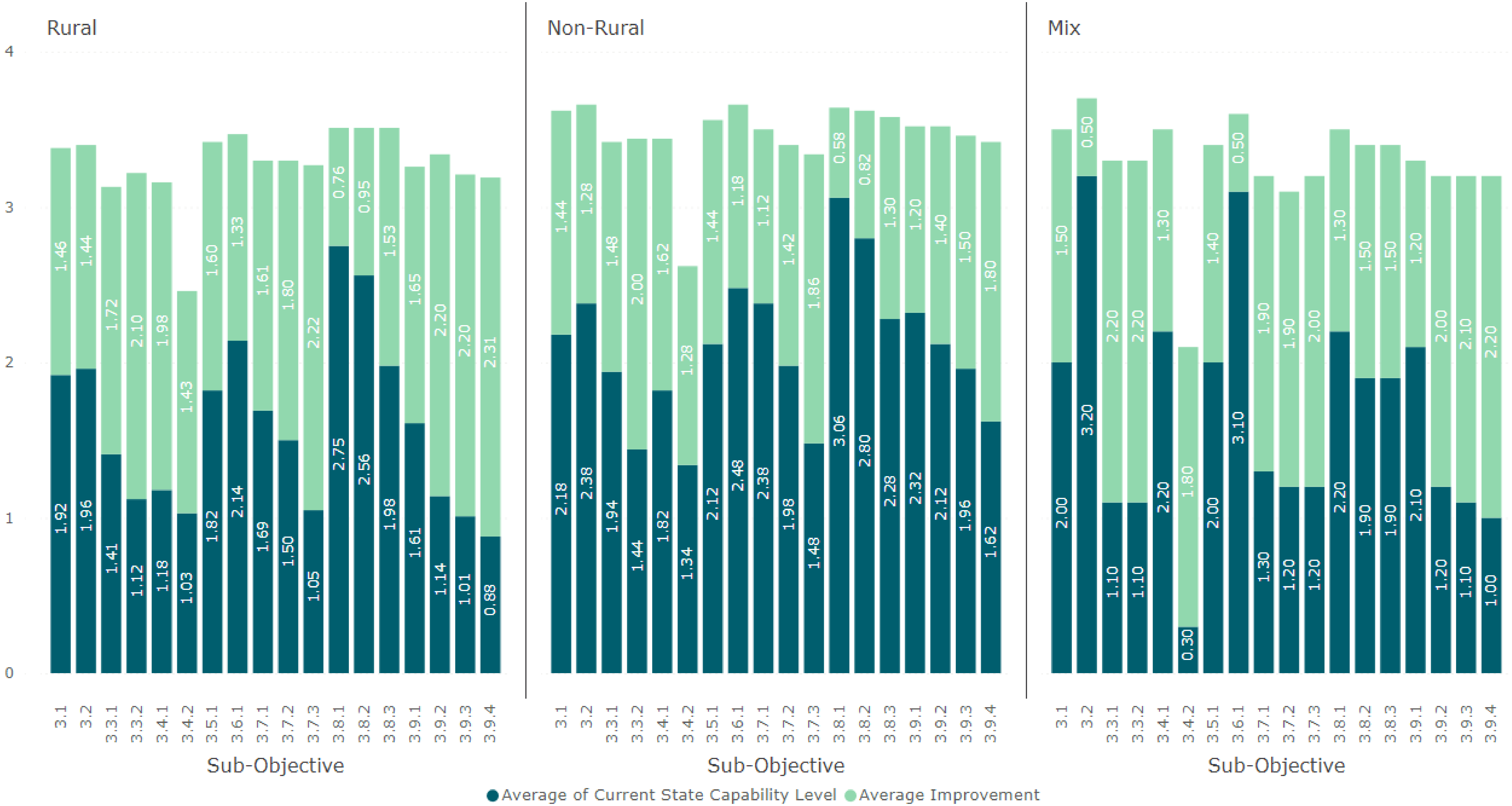
Assessment Data Findings

Goal 3

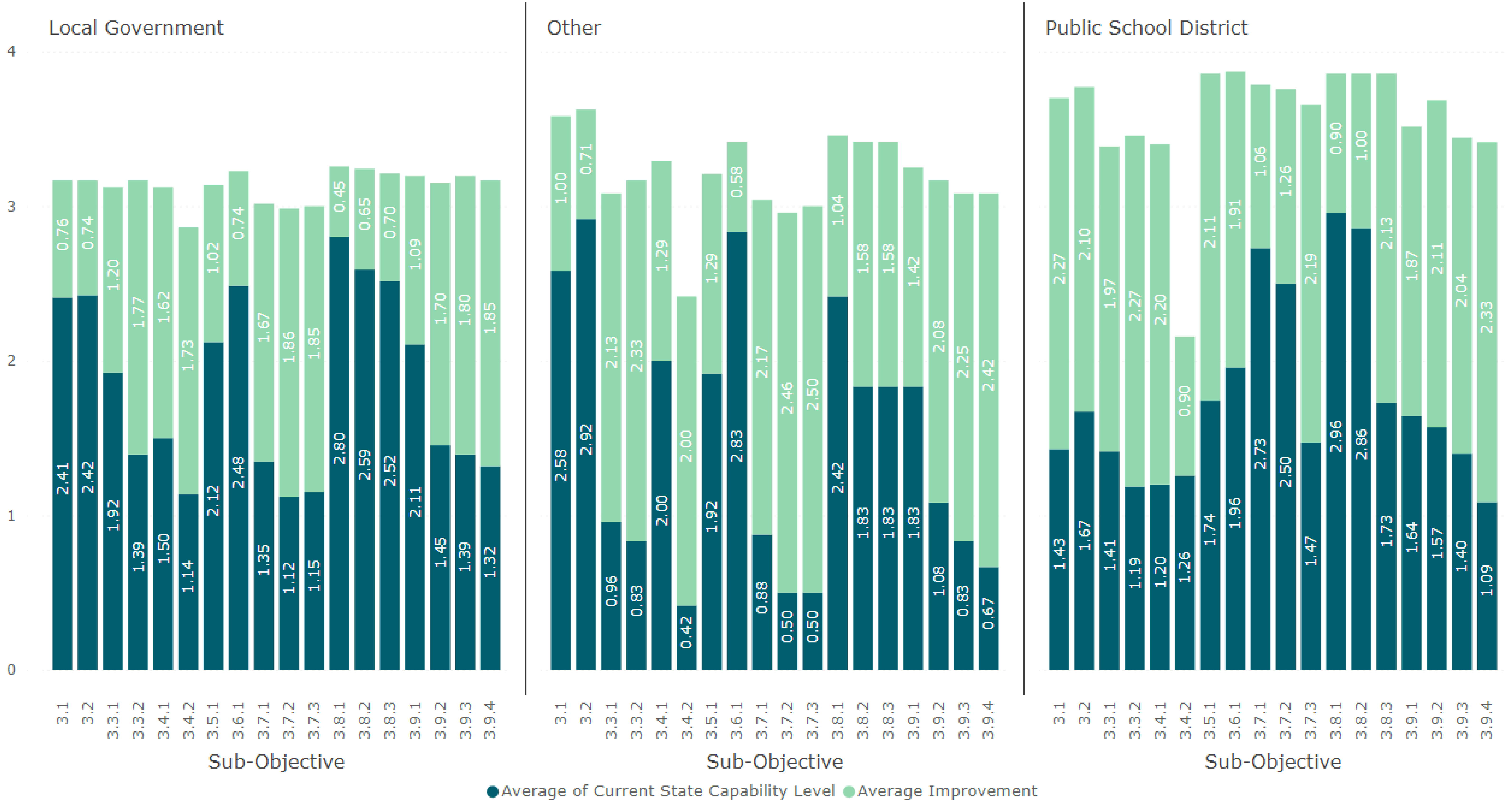
Impact of Capability Improvements



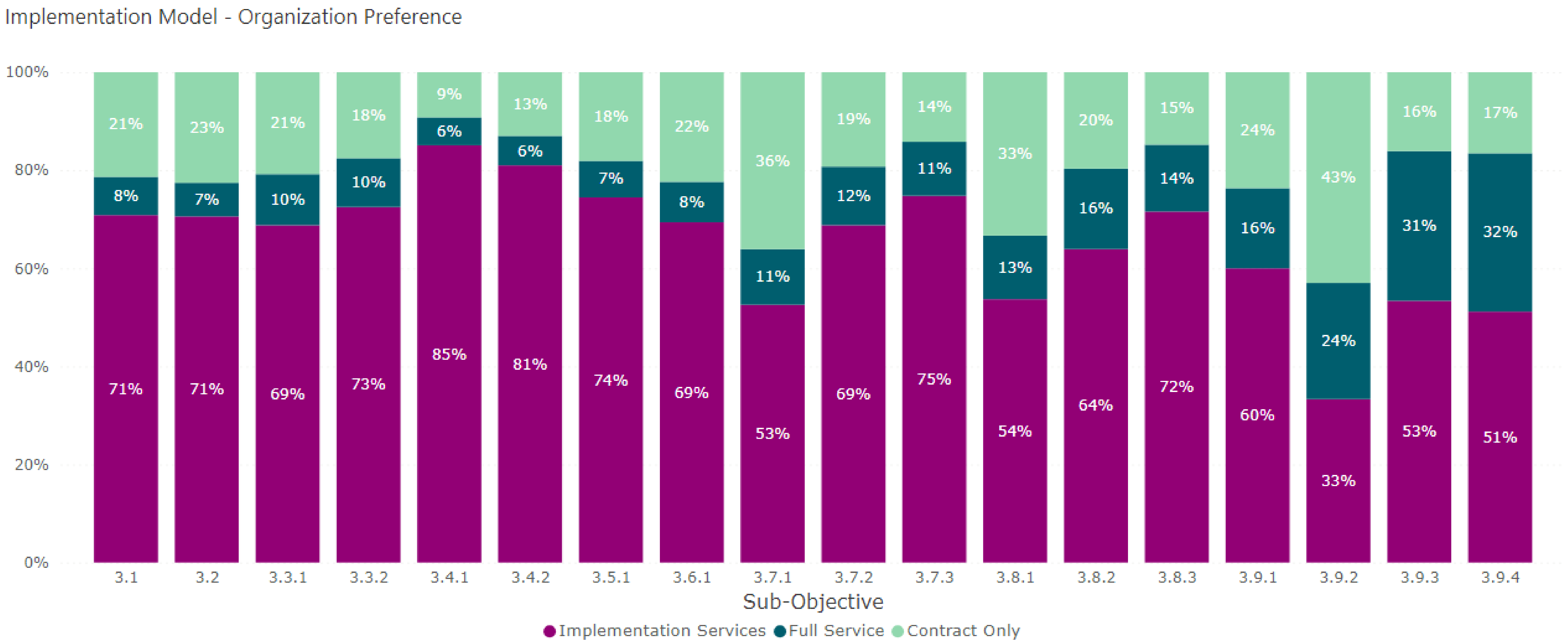
Impact of Capability Improvements
Rural vs. Non-Rural



Impact of Capability Improvements By Entity



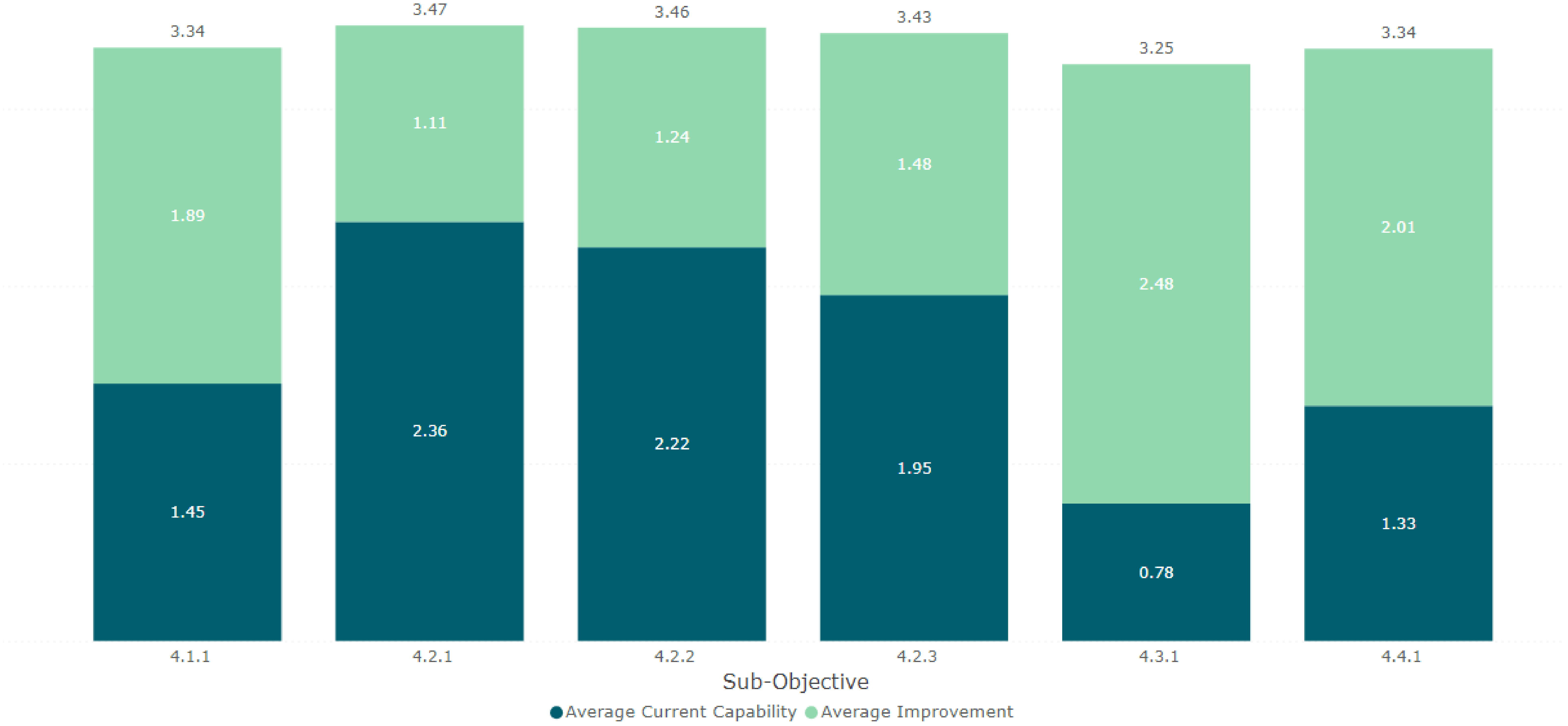
Implementation Model – Organization Preference



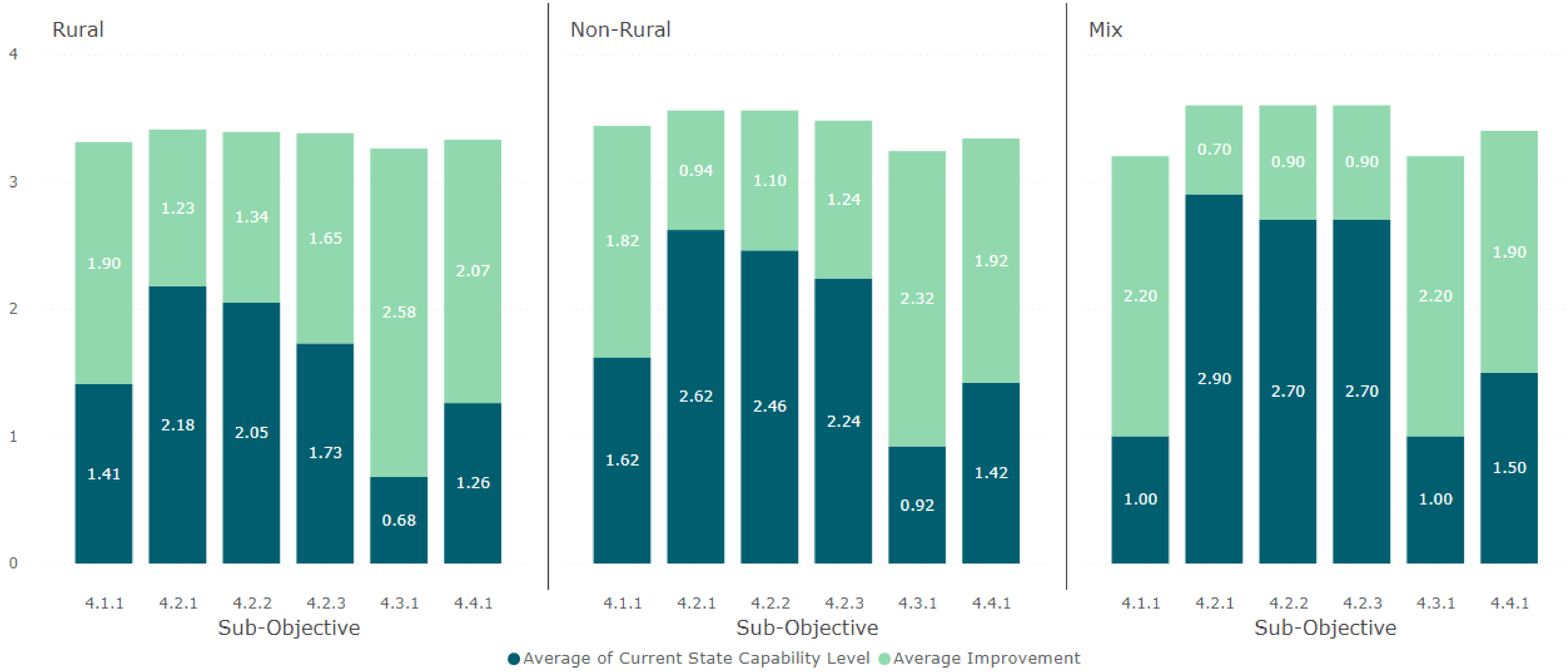
Assessment Data Findings

Goal 4

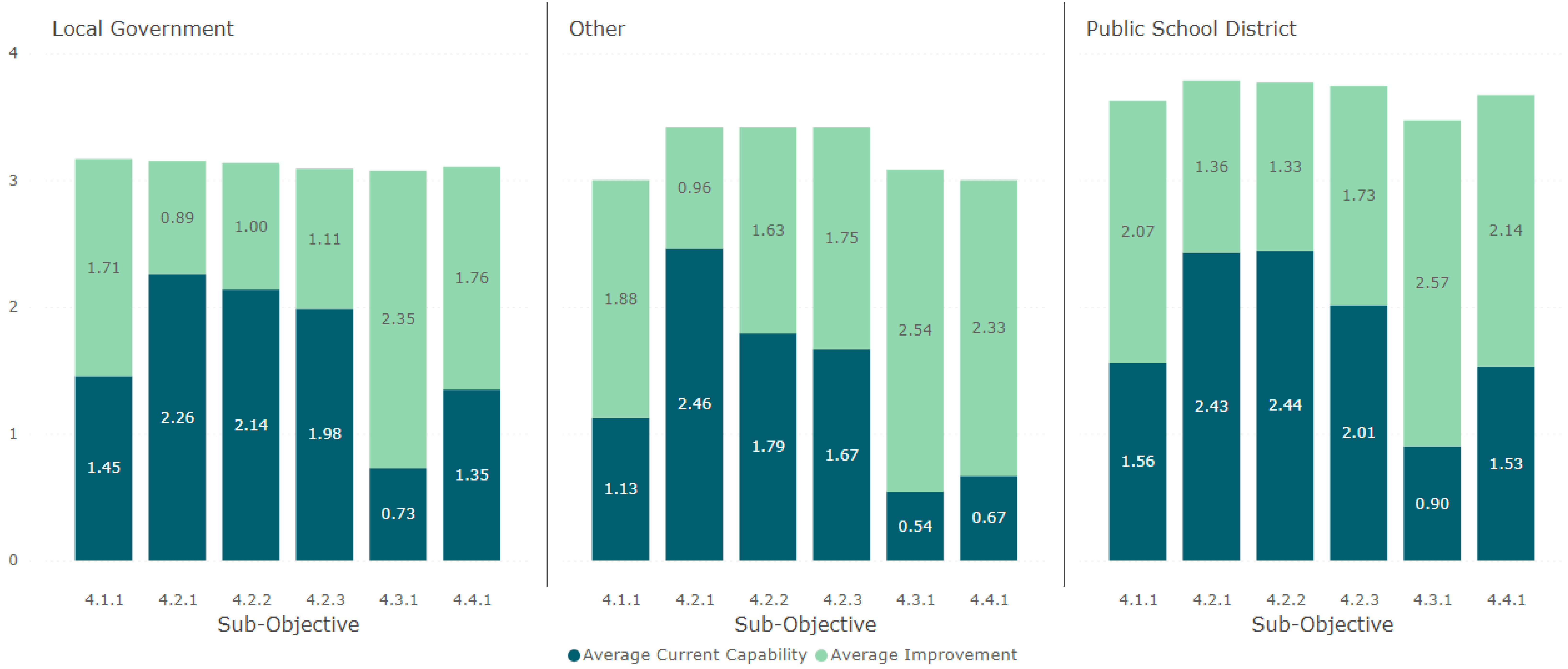
Impact of Capability Improvements



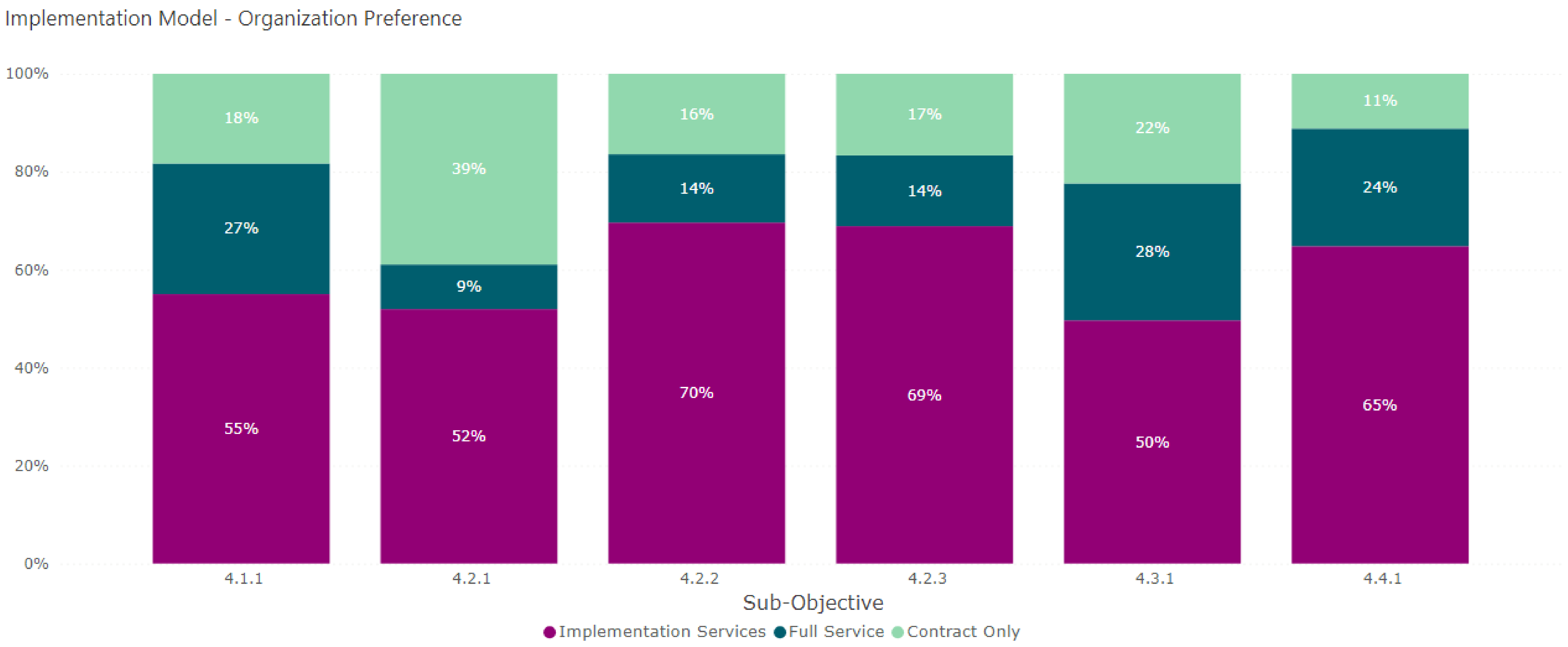
Impact of Capability Improvements
Rural vs. Non-Rural



Impact of Capability Improvements By Entity



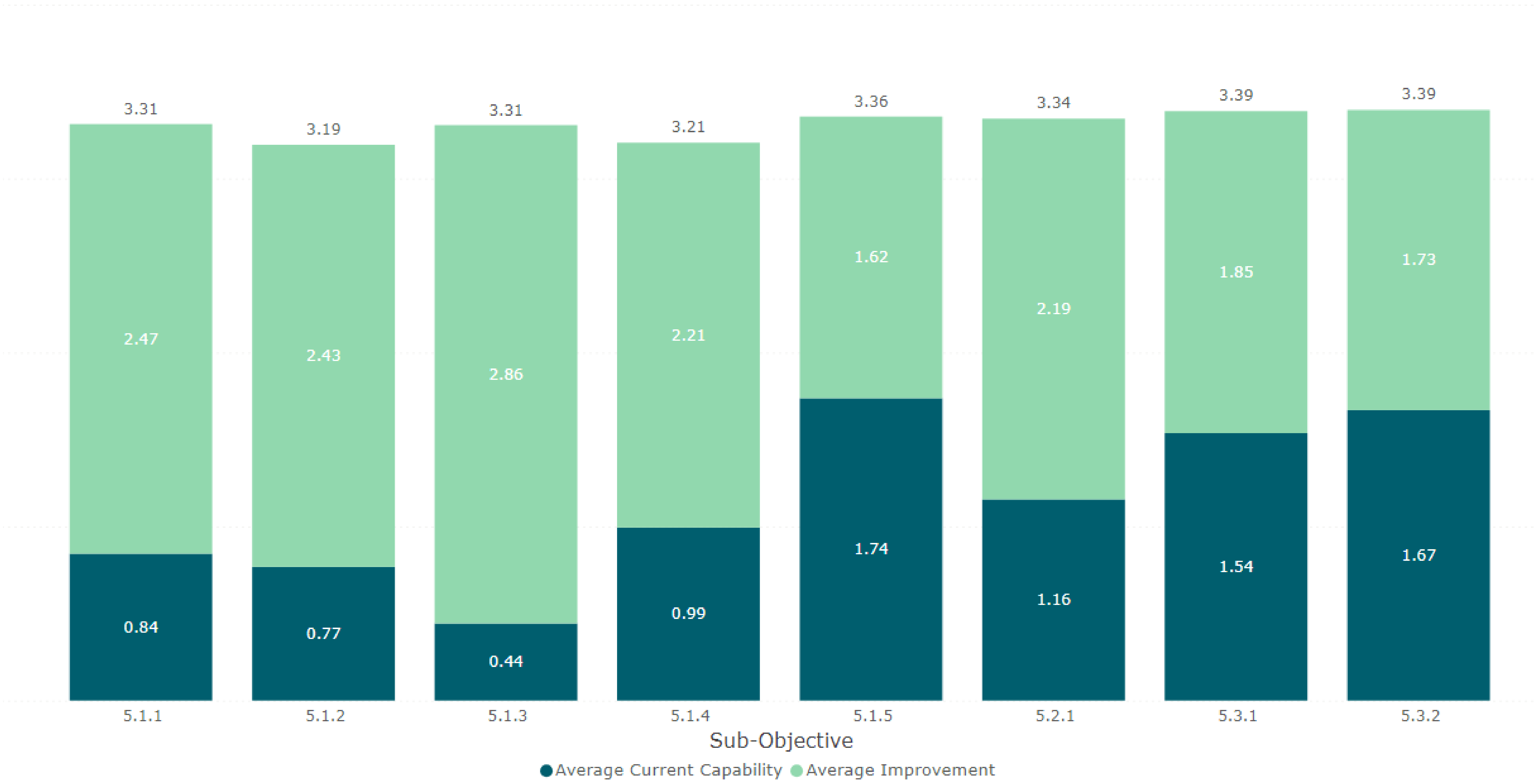
Implementation Model – Organization Preference



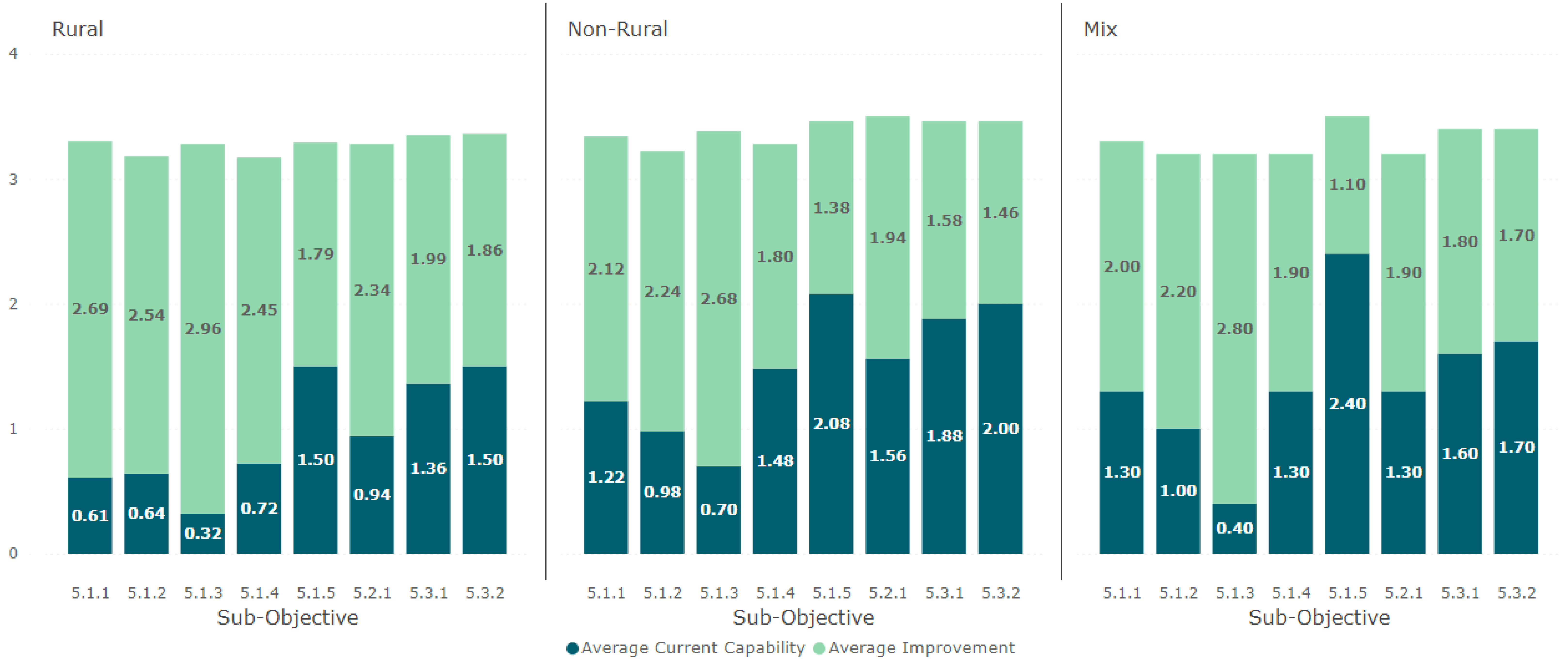
Assessment Data Findings

Goal 5

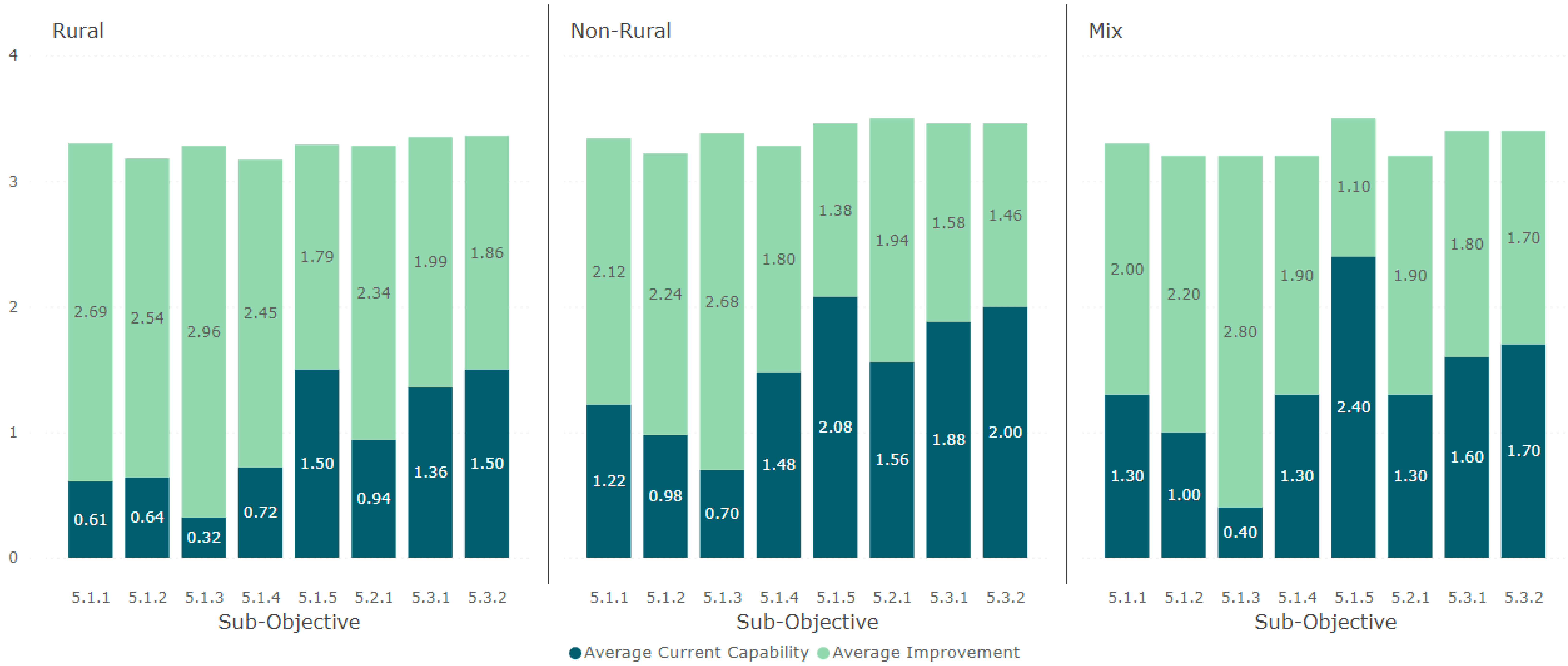
Impact of Capability Improvements



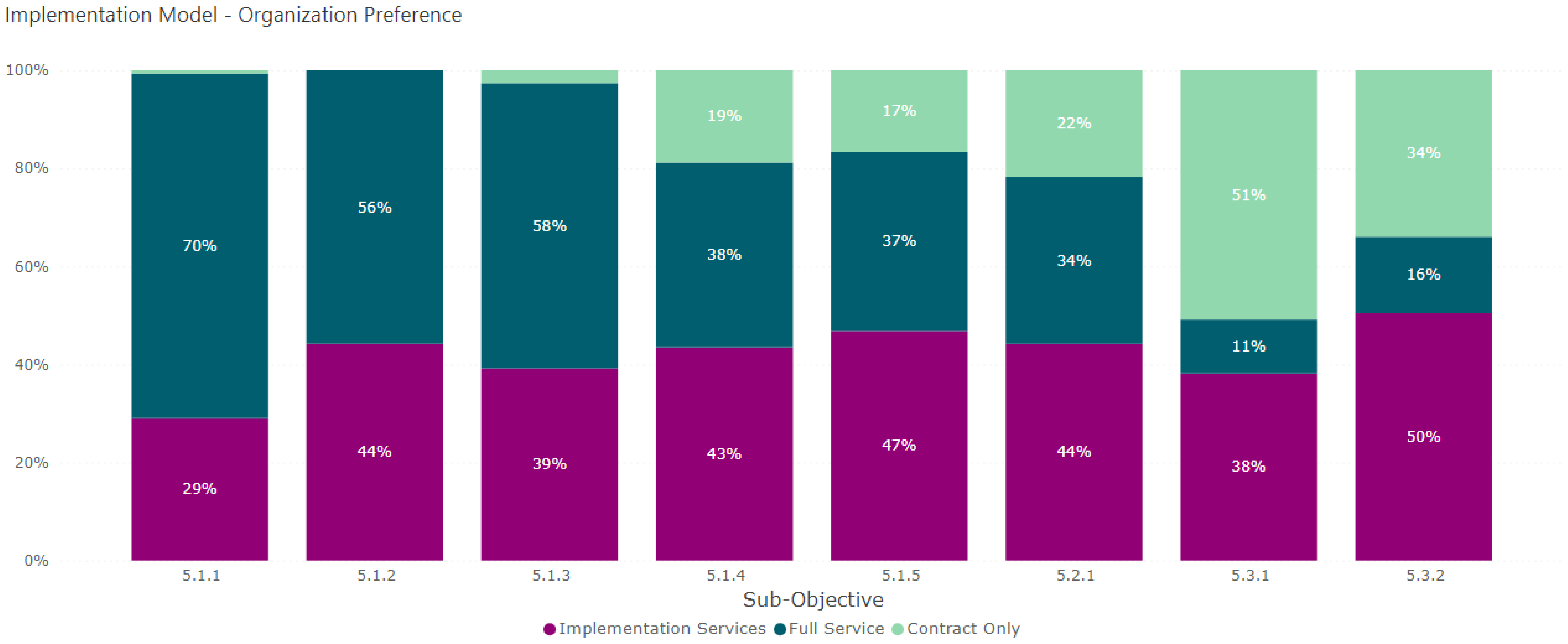
Impact of Capability Improvements
Rural vs. Non-Rural



Impact of Capability Improvements By Entity

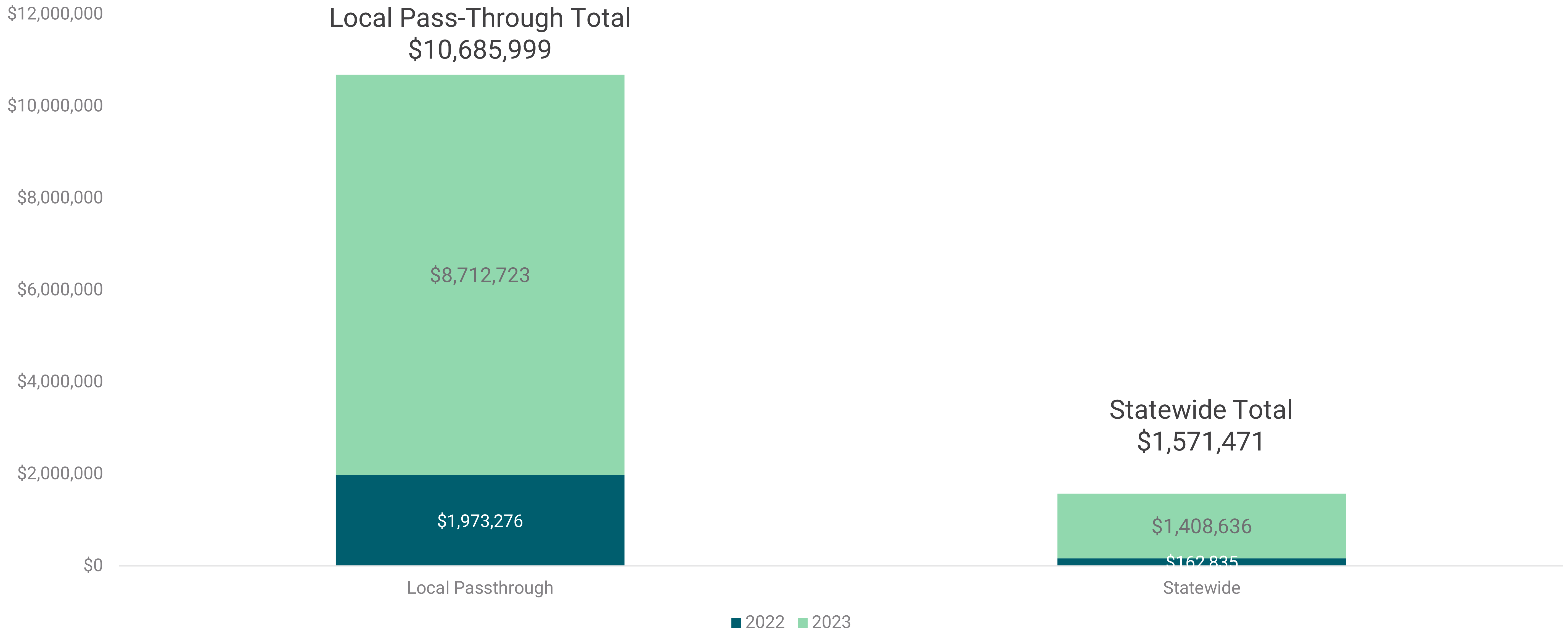


Implementation Model – Organization Preference

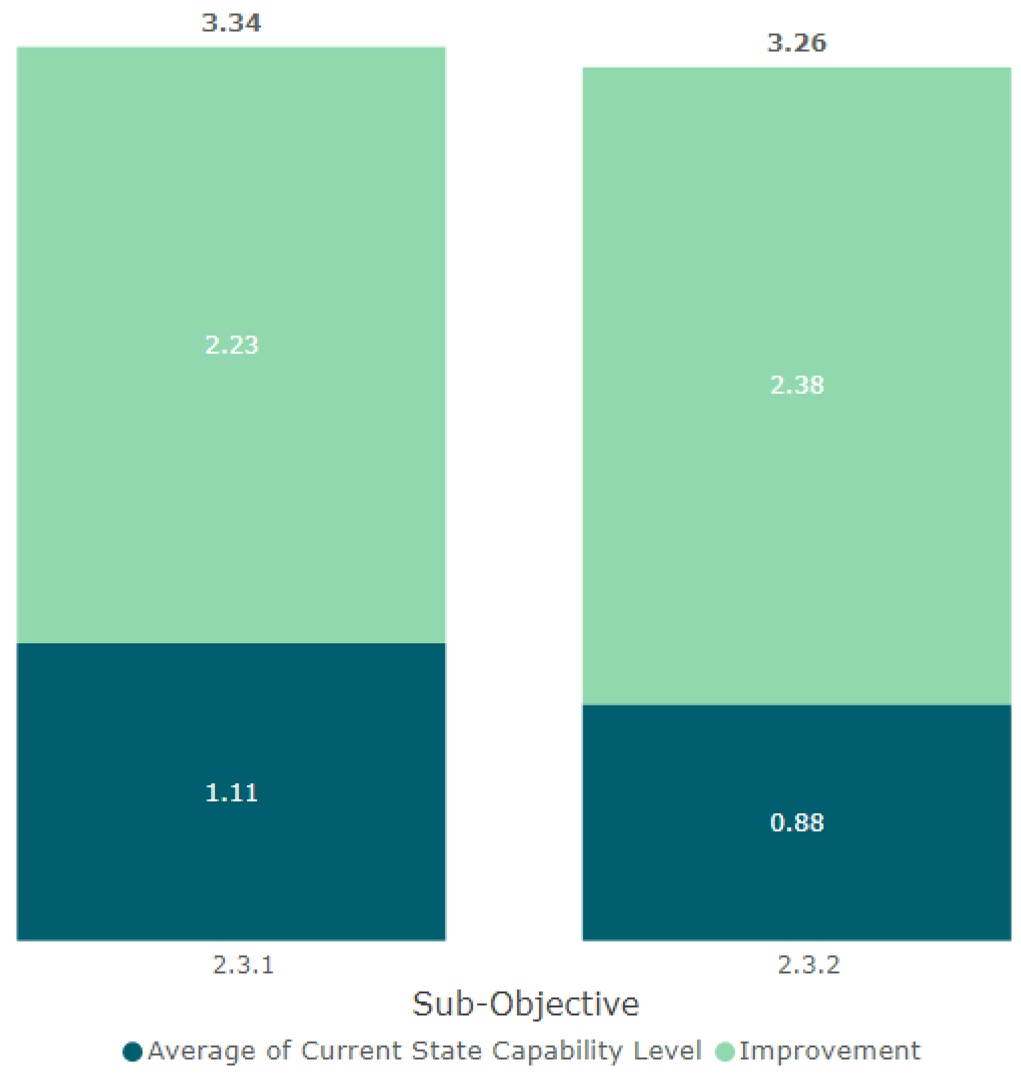


Spending Authorization

Available for Spending



Statewide Spending Allocation Recommendation
Objective 2.3: Centralize security event alerting



Available to allocate:	$1,571,471
Establish statewide SOC for localities	$300,000
Maintain statewide SOC for localities – 4 years	$TBD
Total	$TBD
Remainder to allocate	$TBD

Local Pass-Through Spending Allocation

Option 1: Capability Improvements

- Prioritizes those sub-objectives with greatest amount of improvement
- May prioritize objectives with higher current state
- Excludes Objective 2.3

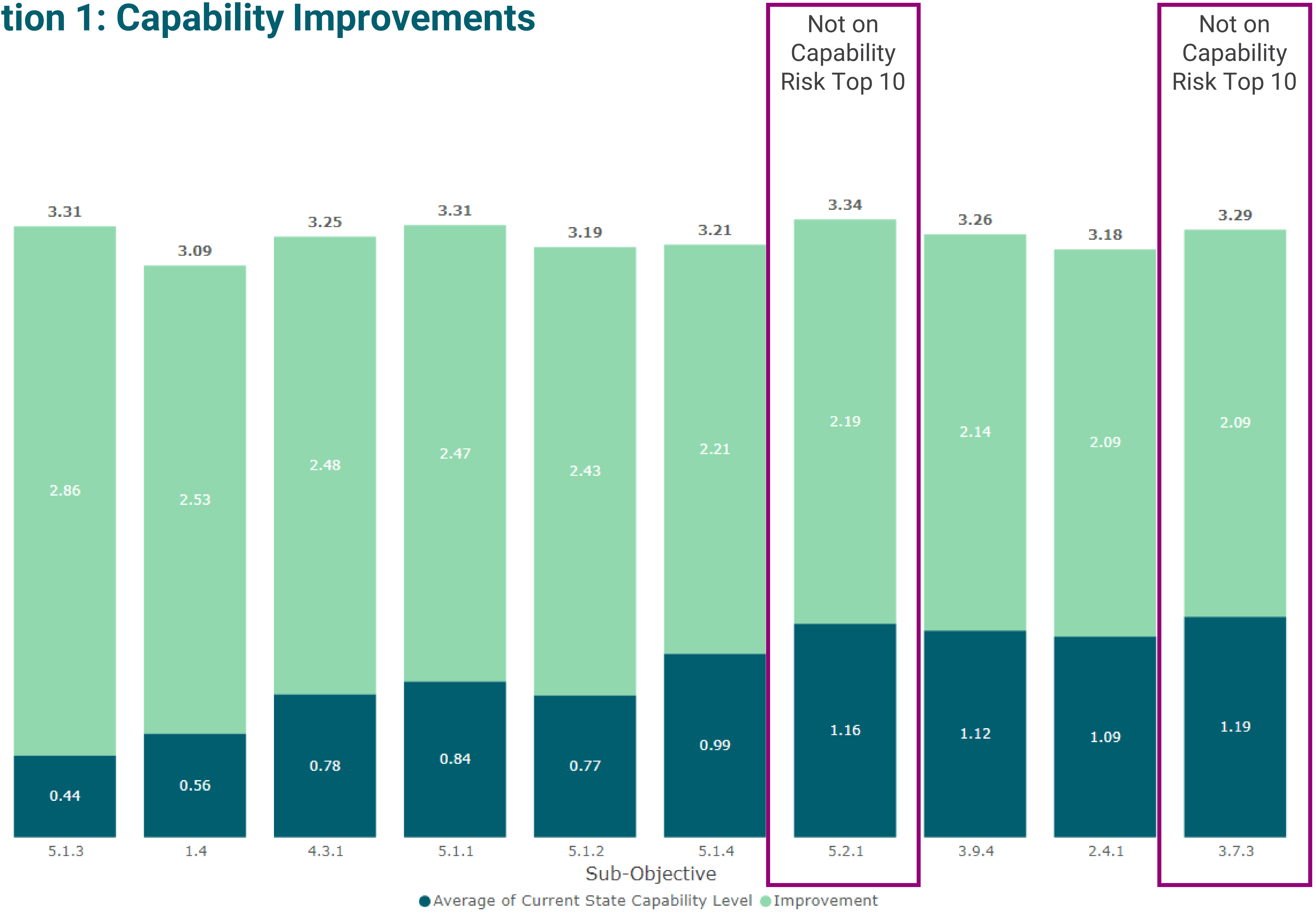
Option 2: Capability Risk

- Prioritizes those sub-objectives with lowest current capability
- May prioritize objectives with lower improvement amounts
- Excludes Objective 2.3

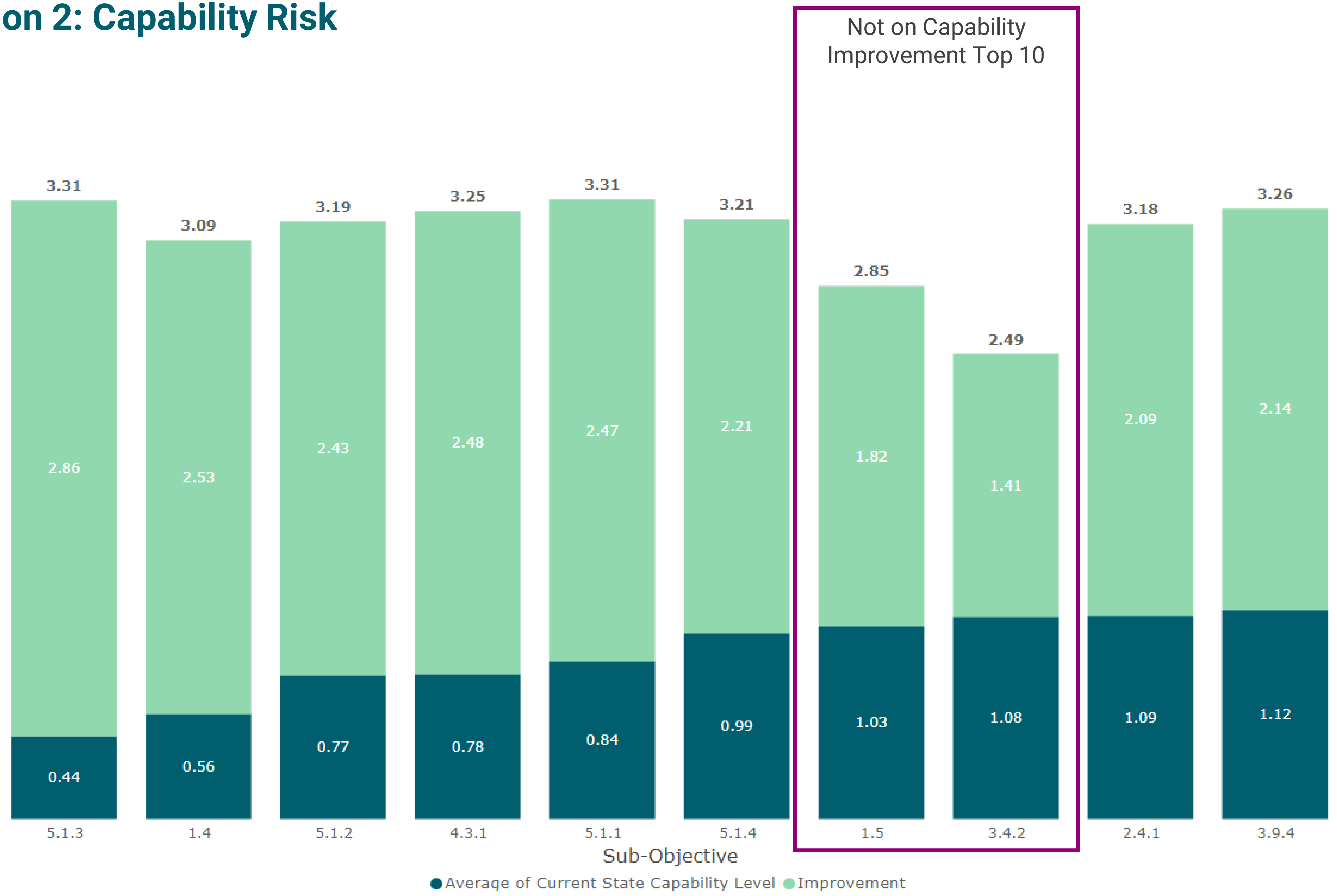
Option 3: Blended (Recommended)

- Prioritizes those sub-objectives that address vulnerability management
- Includes disaster recovery and EDR
- Excludes Objective 2.3

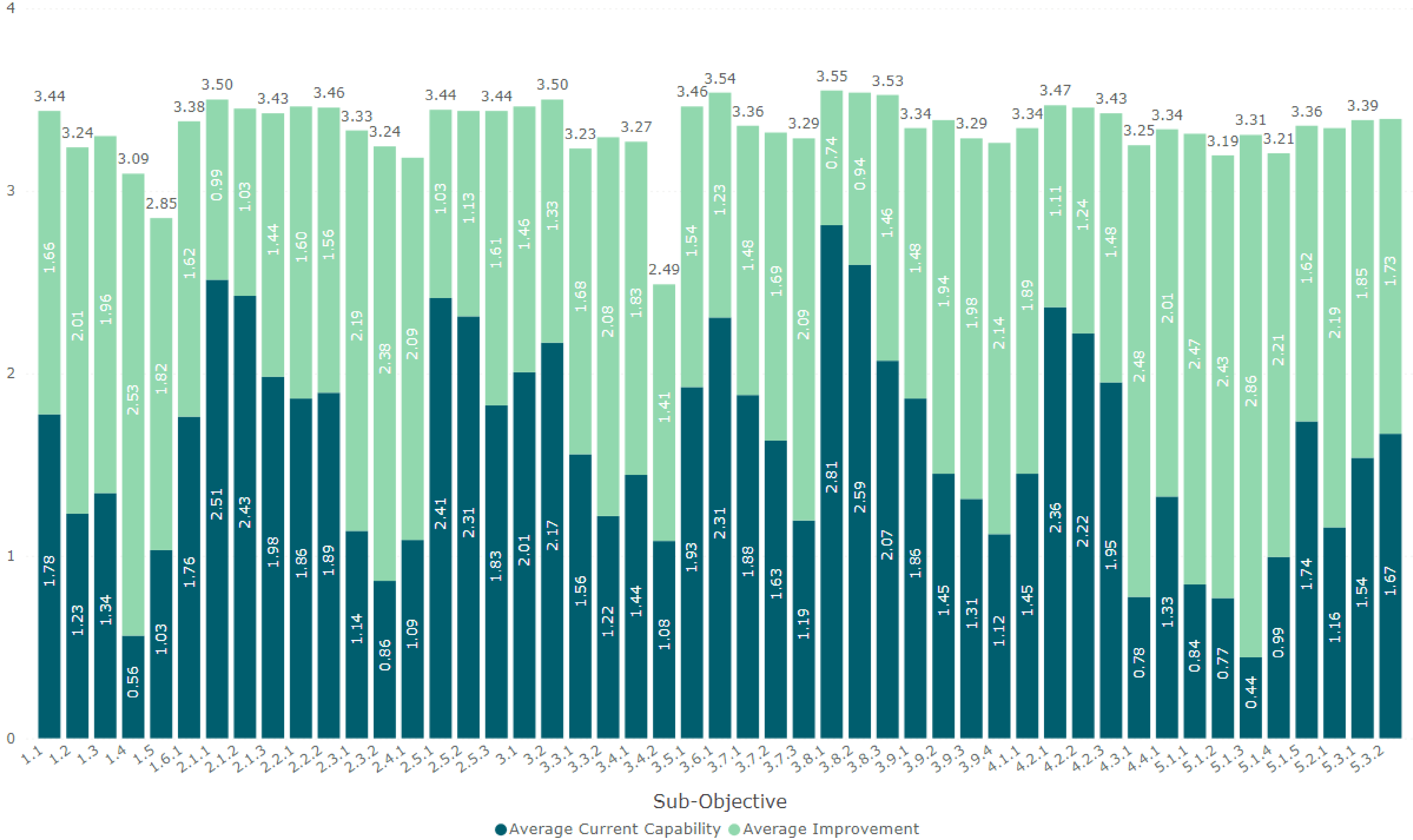
Local Pass-Through Spending Allocation
Option 1: Capability Improvements



Local Pass-Through Allocation Recommendation
Option 2: Capability Risk



Local Pass-Through Allocation Recommendation
Option 3: Blended



Recommended Sub-Objectives

Vulnerability
- 3.9.2
- 3.9.3
- 3.9.4
- 5.2.1

Secure Remote Network Access
- 1.3
- 3.3.2
- 3.4.1
- 3.4.2

Data and Asset Inventory
- 1.1
- 1.4

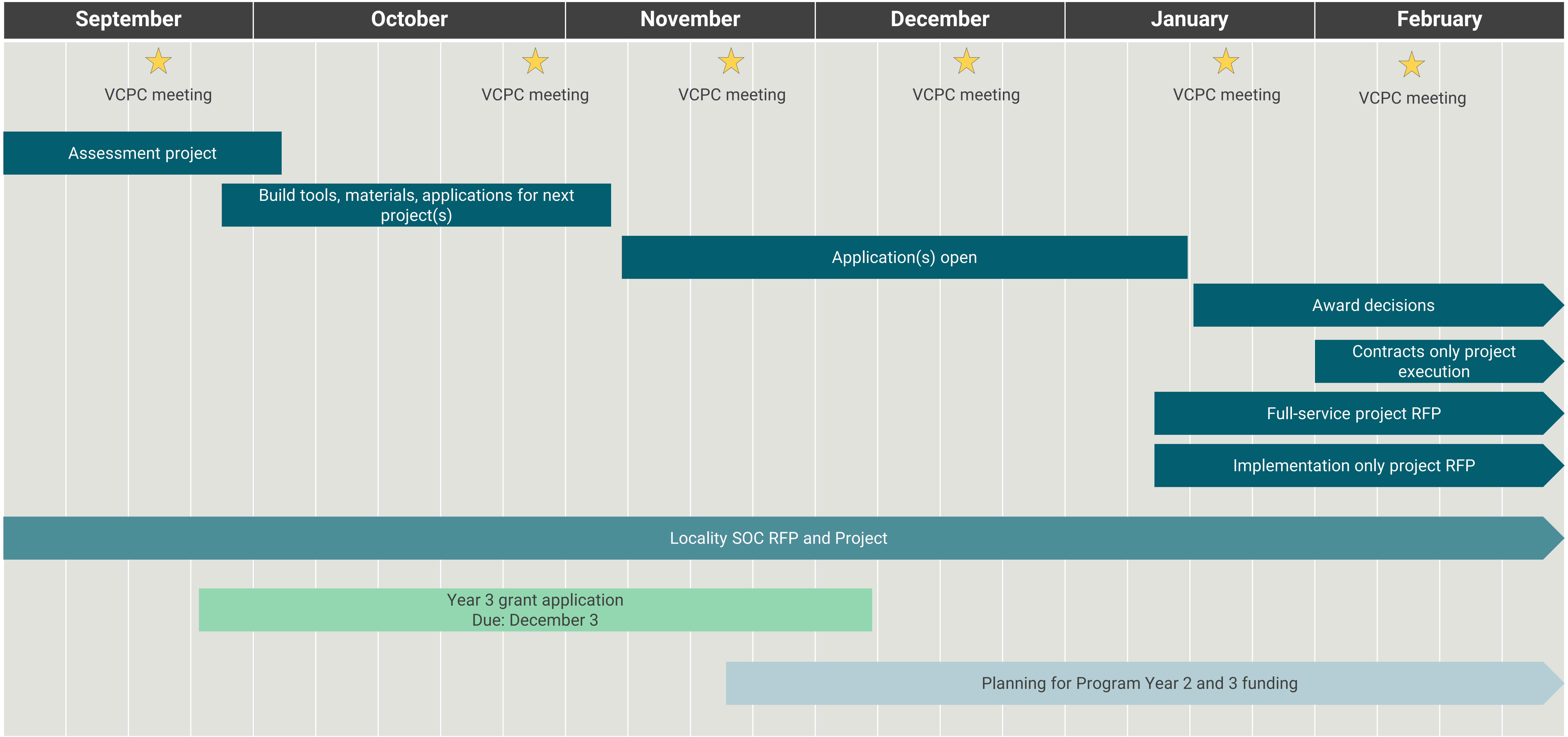
Disaster Recovery
- 4.4.1

EDR
- 2.1 (all sub-objectives)

Firewalls
- 2.2.2
- 2.5 (all sub-objectives)
- 3.1
- 3.2
- 3.5.1

Program Timeline

Program Timeline



September | October | November | December | January | February

★ VCPC meeting (September)

★ VCPC meeting (October)

★ VCPC meeting (November)

★ VCPC meeting (December)

★ VCPC meeting (January)

★ VCPC meeting (February)

Assessment project

Build tools, materials, applications for next project(s)

Application(s) open

Award decisions

Contracts only project execution

Full-service project RFP

Implementation only project RFP

Locality SOC RFP and Project

Year 3 grant application
Due: December 3

Planning for Program Year 2 and 3 funding

Appendix 1
Virginia Cybersecurity Plan Goals, Objectives, and Metrics

Goal 1: Inventory and Control of Technology Assets, Software and Data

Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
1. **Inventory and Control of Technology Assets, Software and Data**	1.1 Establish and maintain a detailed enterprise asset inventory of all technology assets (including hardware and software)	1.1 Implement staff augmentation or third-party services to assess technology inventory	100% of devices and software recorded in inventory – (Total devices and/or software identified) / (Submitter provided initial estimate)	Frequency: Monthly Source: Submitter provided initial estimate NOTE: documentation updating the estimate may be provided at the measurement frequency
	1.2 Ensure only authorized assets connect to enterprise systems and are inventoried	1.2 Implement staff augmentation or third-party services to assess and/or upgrade software without support for security updates.	100% of targeted devices are updated	Frequency: Monthly Source: # of targets / # of upgrades
	1.3 Upgrade or replace all software no longer receiving security maintenance/support	1.3 Implement zero trust network access to provide only authorized systems to connect to the network	100% of authorized devices are using multi factor protected zero trust network access	Frequency: Monthly Source: # of devices connected within the 30 days / # of devices in inventory
	1.4 Establish and maintain a data inventory and perform a data sensitivity analysis for all systems supporting the organization's business	1.4 Implement staff augmentation or third-party services to assess and inventory data according to inventory requirements	100% of targeted and/or identified data sets inventoried. NOTE: If target unknown begin with estimate	Frequency: Monthly Source: Submitter provided initial estimate or target number NOTE: documentation updating the estimate may be provided at the measurement frequency
	1.5 Identify all government websites and migrate non .gov sites to .gov domains	1.5 Implement staff augmentation or third-party services to migrate existing websites to .gov addresses. This migration must include the primary government website (i.e., localityname.gov)	100% of targeted websites	Frequency: Monthly Source: Sites publicly available
	1.6 Establish and maintain inventory of administrator, service, and user accounts	1.6.1 Implement staff augmentation or third-party services to inventory account information 1.6.2 Identify software and/or technology to maintain account inventory	100% of accounts	Frequency: Monthly Source: Accounts reviewed/confirmed within account directory or automated inventory

Goal 2: Threat Monitoring

Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
2. Threat Monitoring	2.1 Deploy host intrusion detection/prevention and endpoint detection and response for all workstations and servers	2.1.1 Purchase and/or license preapproved host-based threat protection software	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. 90% of targets Threat data from threat protection software.
		2.1.2 Implement third party services to deploy preapproved host-based threat protection software	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. Threat data from threat protection software.
		2.1.3 Implement third party services to manage and maintain the preapproved host-based threat protection software deployment	Total number of hosts running the software out of the established target Threat information collected from deployment	Frequency: Monthly Source: Asset Inventory and software deployment totals. Threat data from threat protection software.
	2.2 Deploy network monitoring, filtering and detection at network egress and ingress points	2.2.1 Implement third party services to install netflow monitoring at the egress of where a majority of server traffic is traversing or the location that has the most amount of network traffic and will support an approved configuration	At least 1 device deployed and reporting data. Target coverage 90% of assets	Frequency: Completion of installation and quarterly review of data
		2.2.2 Implement third party services to deploy and/or manage firewall, IDS/IPS technology at an organizations egress with deep packet inspection, malware detection, application awareness, intrusion detection and intrusion prevention	Devices deployed. Reports on threat activity available Target coverage 90%	Frequency: Completion of information and quarterly review of data

Goal 2: Threat Monitoring

Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
2. Threat Monitoring	2.3 Centralize security event alerting	2.3.1 Implement and maintain or have third party services implement and maintain security event collection technology to connect to the preapproved security operations center	Devices deployed. Reports on threat activity available	Frequency: Completion of information and quarterly review of data
		2.3.2 Implementation of a Commonwealth security operations center and/or information sharing and analysis center	Devices deployed. Reports on threat activity available	Frequency: Completion of information and quarterly review of data
	2.4 Audit log collection for all servers and systems hosting data in accordance with log management standards.	2.4.1 Establish data collection points for system audit logs	% of systems reporting logs % of event log sources compliant with standards	Frequency: Monthly Source: Asset inventory and log collection system
	2.5 Web application firewall	2.5.1 Purchase and/or license preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.
		2.5.2 Implement third party services to deploy preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.
		2.5.3 Implement third party services to manage and maintain the preapproved web application firewall or DNS filtering	Devices deployed. Reports on threat activity available	Frequency: Monthly Source: threat protection devices Threat data from threat protection devices.

Goal 3: Threat Protection and Prevention

Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
3. Threat Protection and Prevention	3.1 Implement and manage firewalls on all end point devices (i.e., user workstations, servers)	N/A	N/A	N/A
	3.2 Implement and manage network firewalls for ingress and egress points	N/A	N/A	N/A
	3.3 Encrypt sensitive data in transit and on devices hosting sensitive data	3.3.1 Obtain certificates to support encrypted transmissions	Number of public-facing hosted systems with approved encryption	Frequency: Monthly Sources: Websites with approved encryption
		3.3.2 Implement and/or manage zero trust network access connectivity (ZTNA VPN)	Number of non-public facing systems potentially accessible	Frequency: Quarterly Sources: Number of devices remotely accessible using multifactor login
	3.4 Multifactor authentication implementation for compatible externally exposed systems, network access, and/or administrative access	3.4.1 Implement multifactor authentication to systems.	Accounts implemented with multifactor. Target: 100% Minimum: 90%	Source: Target accounts per system or in the environment Frequency: Monthly
		3.4.2 Implement multifactor authentication for Virginian identities		

Goal 4: Data Recovery and Continuity

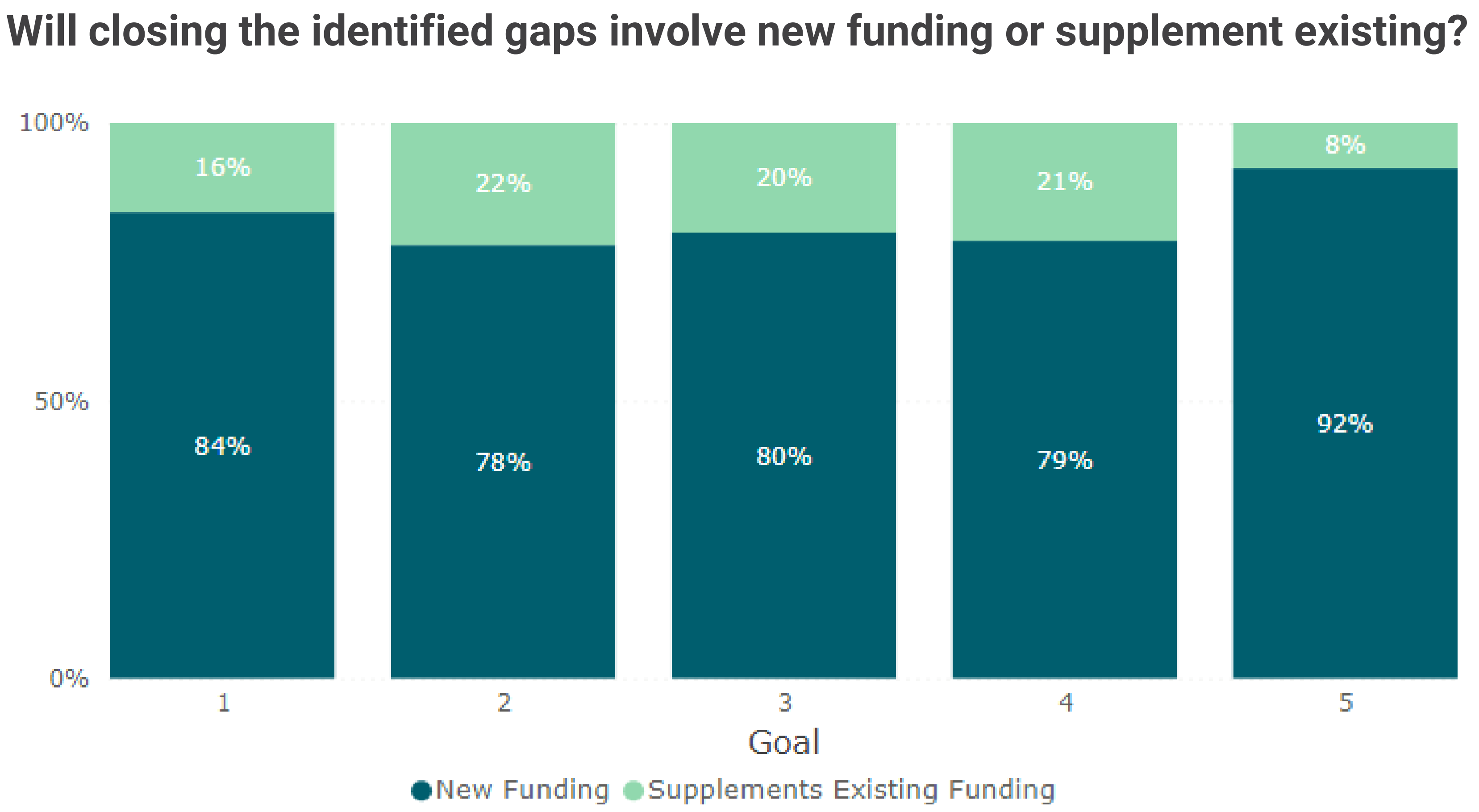
Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
4. Data Recovery and continuity	4.1 Establish and maintain a data recovery process	4.1.1 Develop or have a third party develop a business continuity plan and/or disaster recovery plan that enables the recovery of critical information systems that support business processes for all cloud based and locally stored data.	100% of Critical services will be brought online within 72 hours	Source: Asset inventory Frequency: Once
	4.2 Establish and maintain an isolated/vaulted instance of recovery data	4.2.1 Obtain licenses for a vaulted data recovery solutions	90% of critical data vaulted	Frequency: Source Source: Total GB of data vaulted out of total GB of critical data
		4.2.2 Implement or have a third party implement a vaulted data recovery solution for critical backups		
		4.2.3 Have a third party maintain a vaulted data recovery solution		
	4.3 Implement disaster recovery and data recovery testing	4.3.1 Have a third party test the disaster recovery and/or business continuity plan	Successful recovery within plan established time frame	Frequency: Once Source: Disaster recovery plan information
	4.4 Implement technology to support continuity of services in the case of a natural disaster or cyber attack	4.4.1 Obtain or have a third party provide services to maintain communications in the case of a regional disaster within 500 miles	Successful test of continuity services	Frequency: Semi-Annually Source: Recovery plan and certification of completion

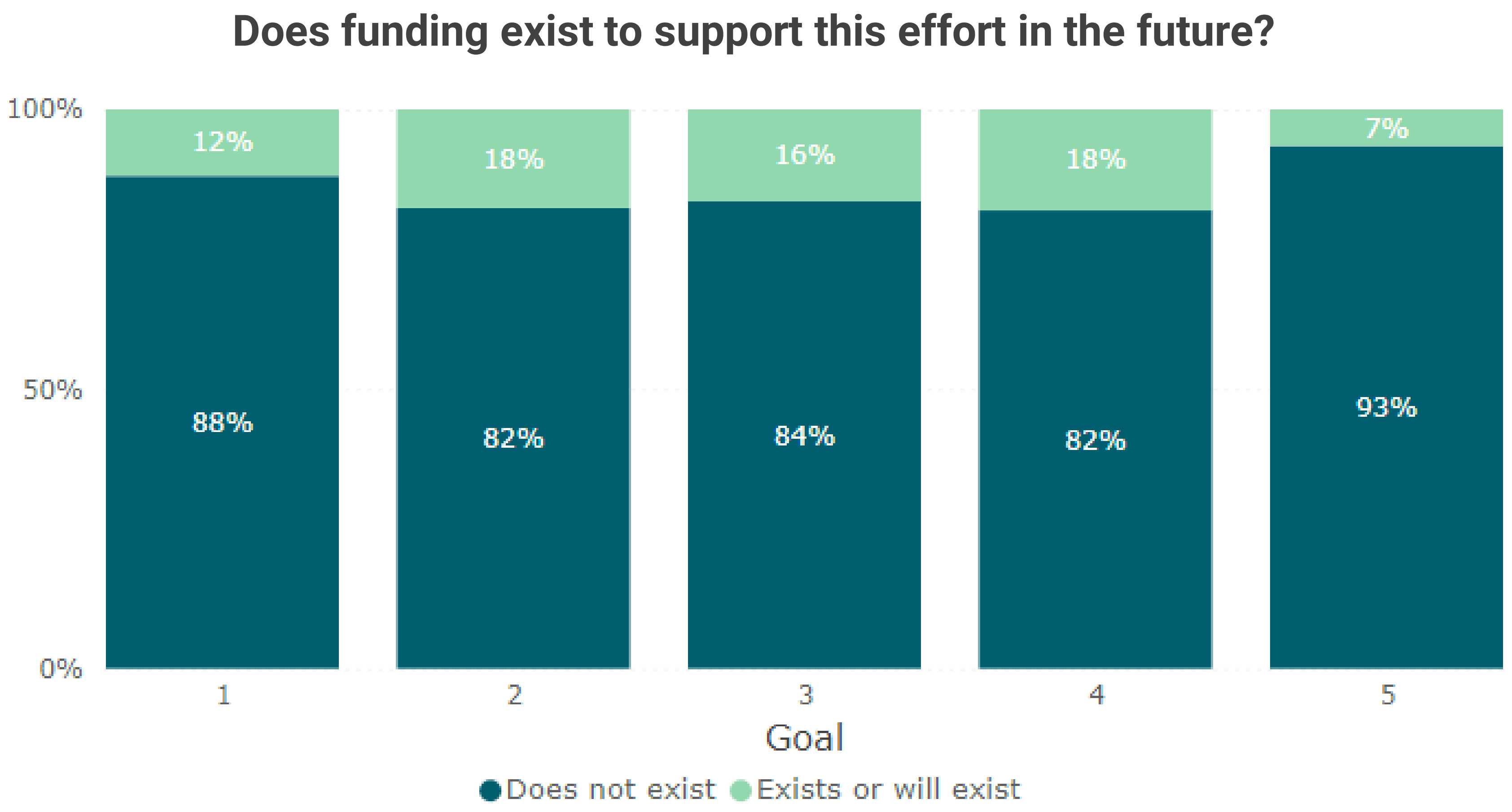
Goal 5: Security Assessment

Program Goal	Program Objectives	Program Sub-Objectives	Associated Metric	Metric Description
5. Security Assessment	5.1 Identify security gaps associated with program objectives which can be supported by the grant program	5.1.1 Have staff augmentation provide an assessment or have a third-party assessment of the technology environment for services supported by the grant program	Assessment completion within 120 days	Frequency: Quarterly
		5.1.2 Obtain services to review and evaluate existing risk assessments/mitigation plans for potential options	Mitigation plans can begin within 30 days	Frequency: Quarterly
		5.1.3 Obtain a service or have a third party provide a skills review for necessary cybersecurity skills in the environment based on the NIST NICE framework		
		5.1.4 Obtain security training used to train or educate personnel for careers in cybersecurity	Training to begin within 90 days of award	Frequency: Quarterly
		5.1.5 Obtain security awareness training for end users	Training to begin within 90 days of award	Frequency: Quarterly
	5.2 Perform automated vulnerability scans	5.2.1 Obtain third-party services to provide a vulnerability scan and assessment of the environment	Obtain a vulnerability review report within 90 days Mitigations to be done with a target of 30 days of report	Source: Vulnerability assessment Frequency: Monthly
	5.3 Network and system architecture diagram and assessment	5.3.1 Obtain software to provide a network map of the environment	Network architecture documentation	Source: Asset inventory and network architecture Frequency: Once All assets and/or asset types must be identifiable on the architecture
		5.3.2 Obtain staff augmentation or have a third-party document the organizations network architecture		

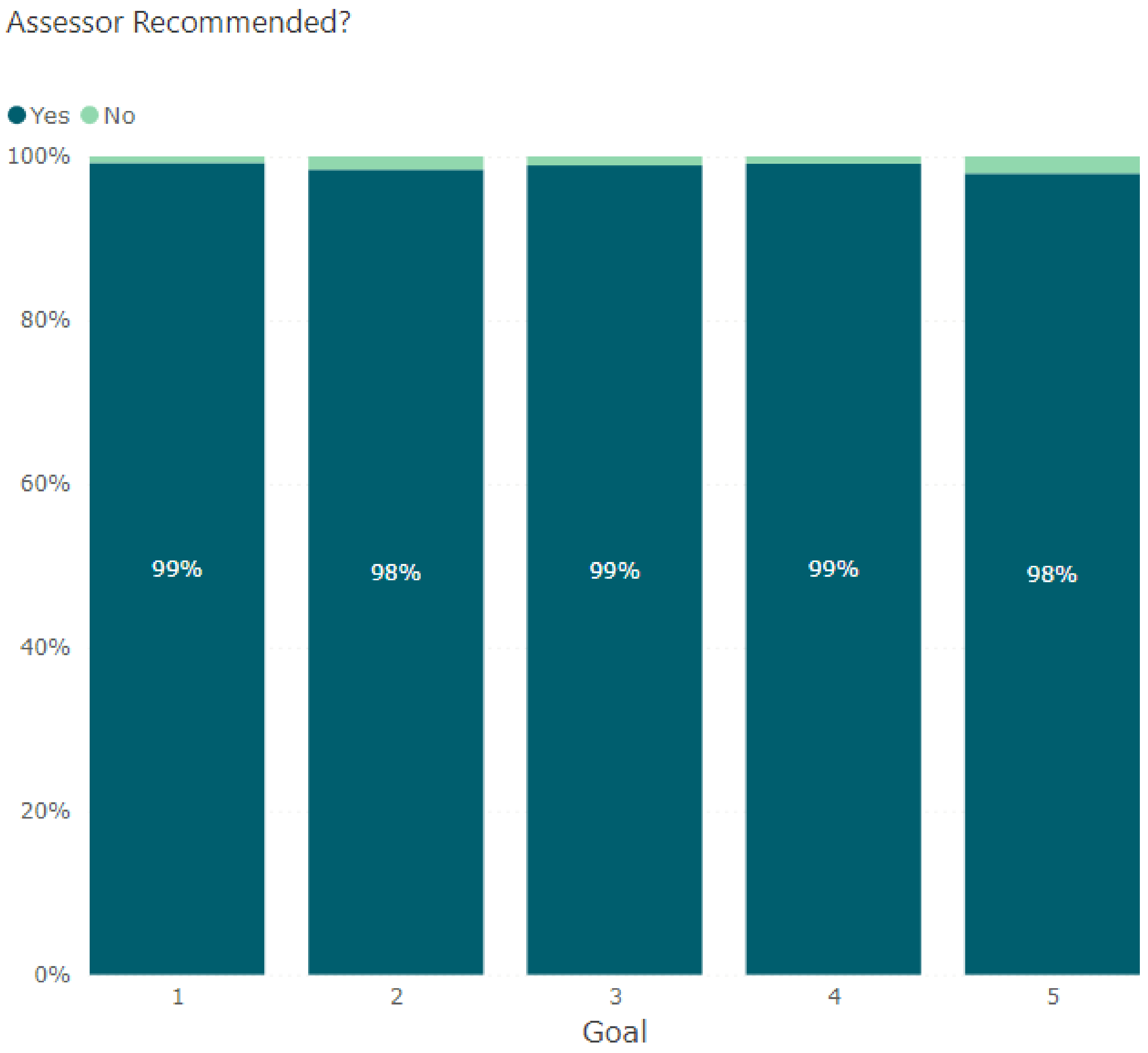
Appendix 2
Additional Data

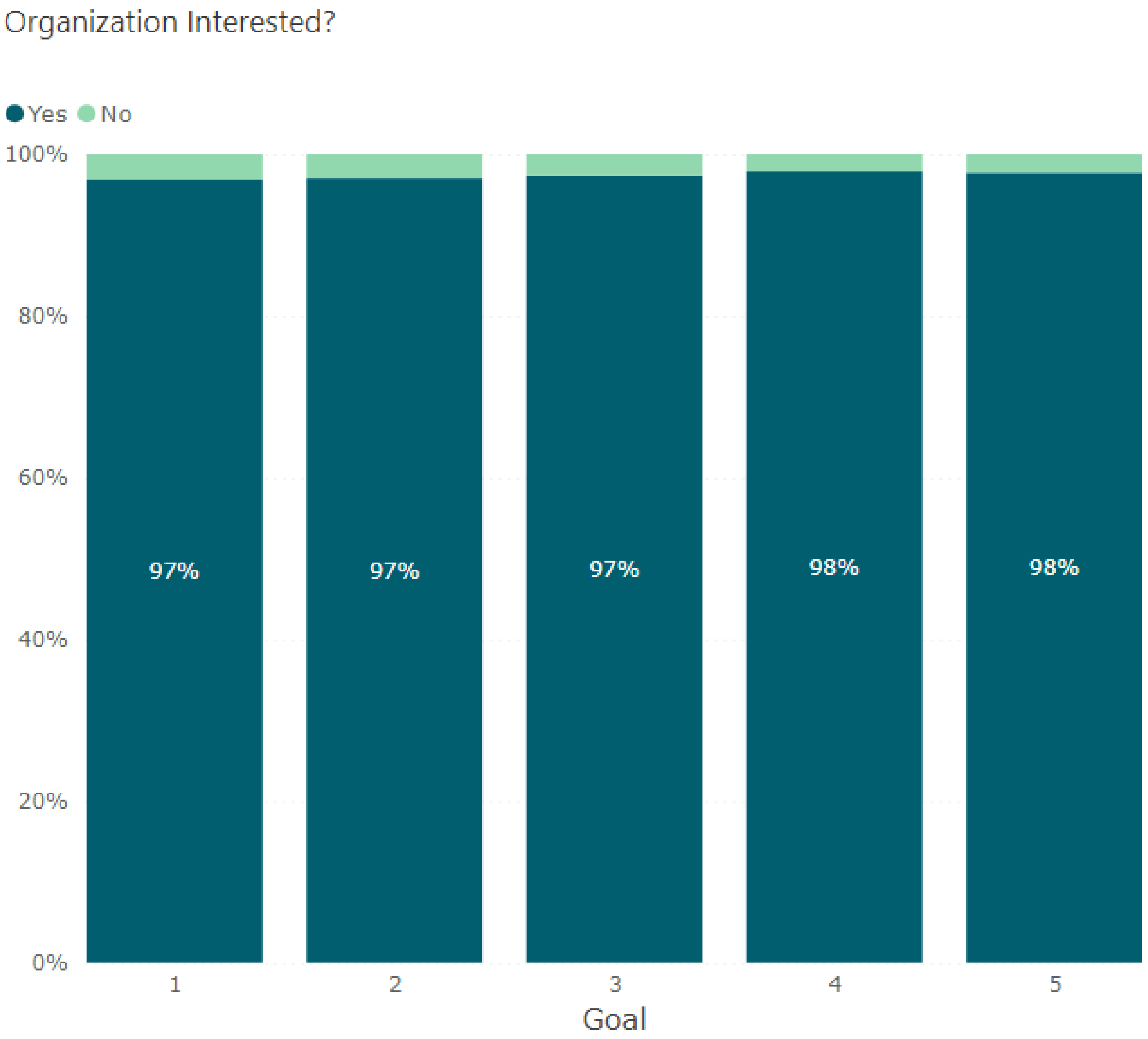
Future State Funding



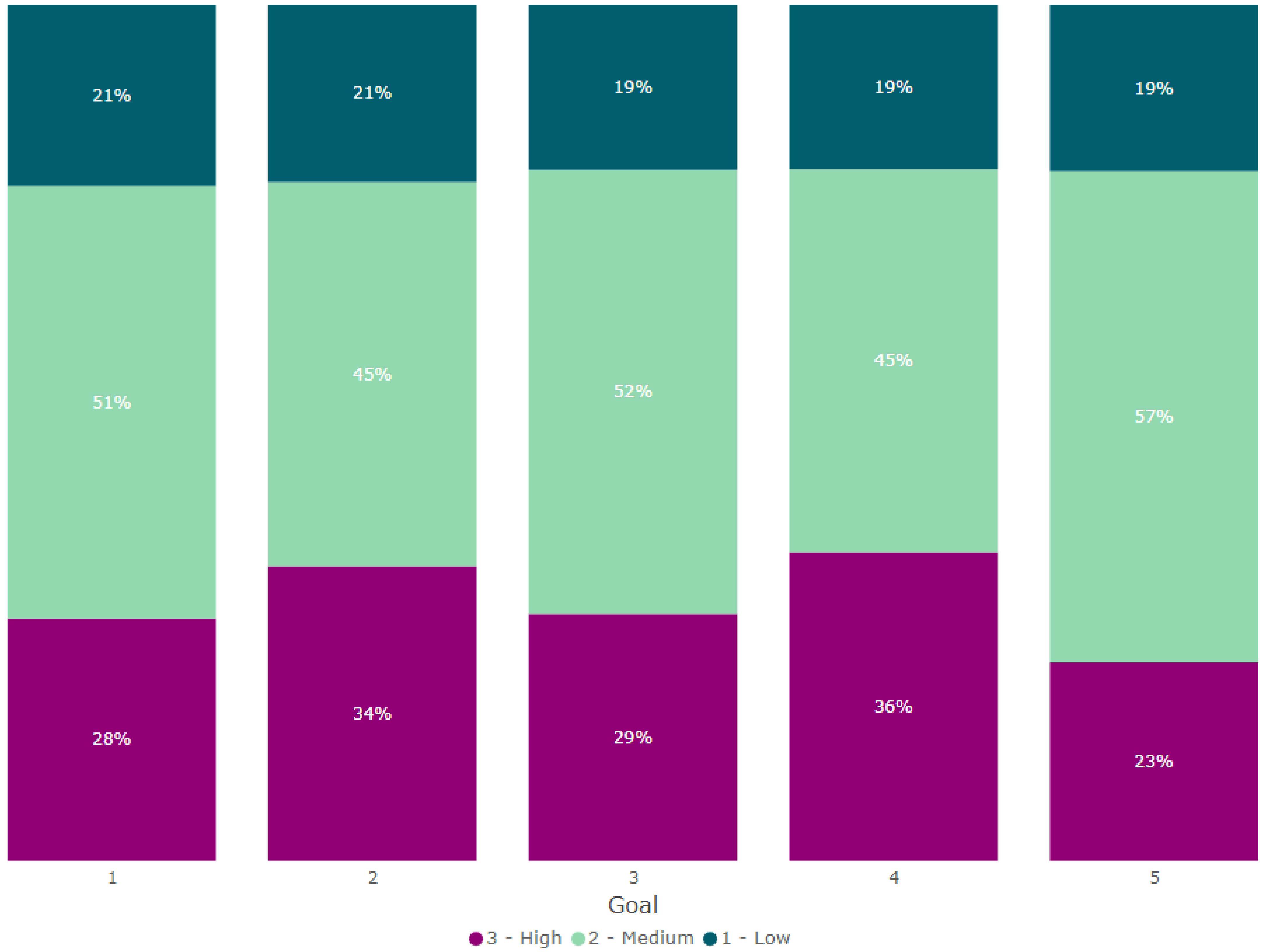


Recommended and Interested

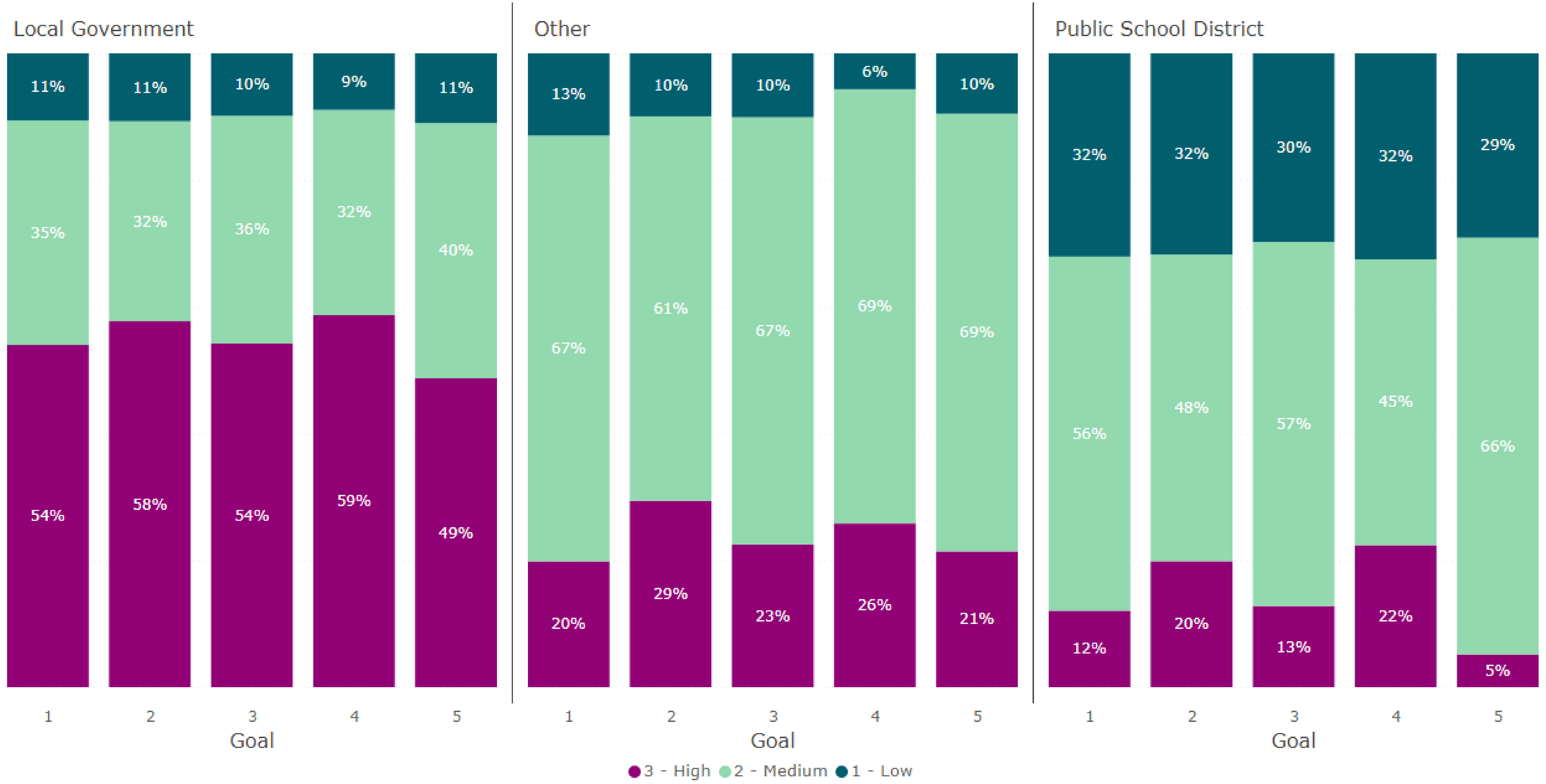




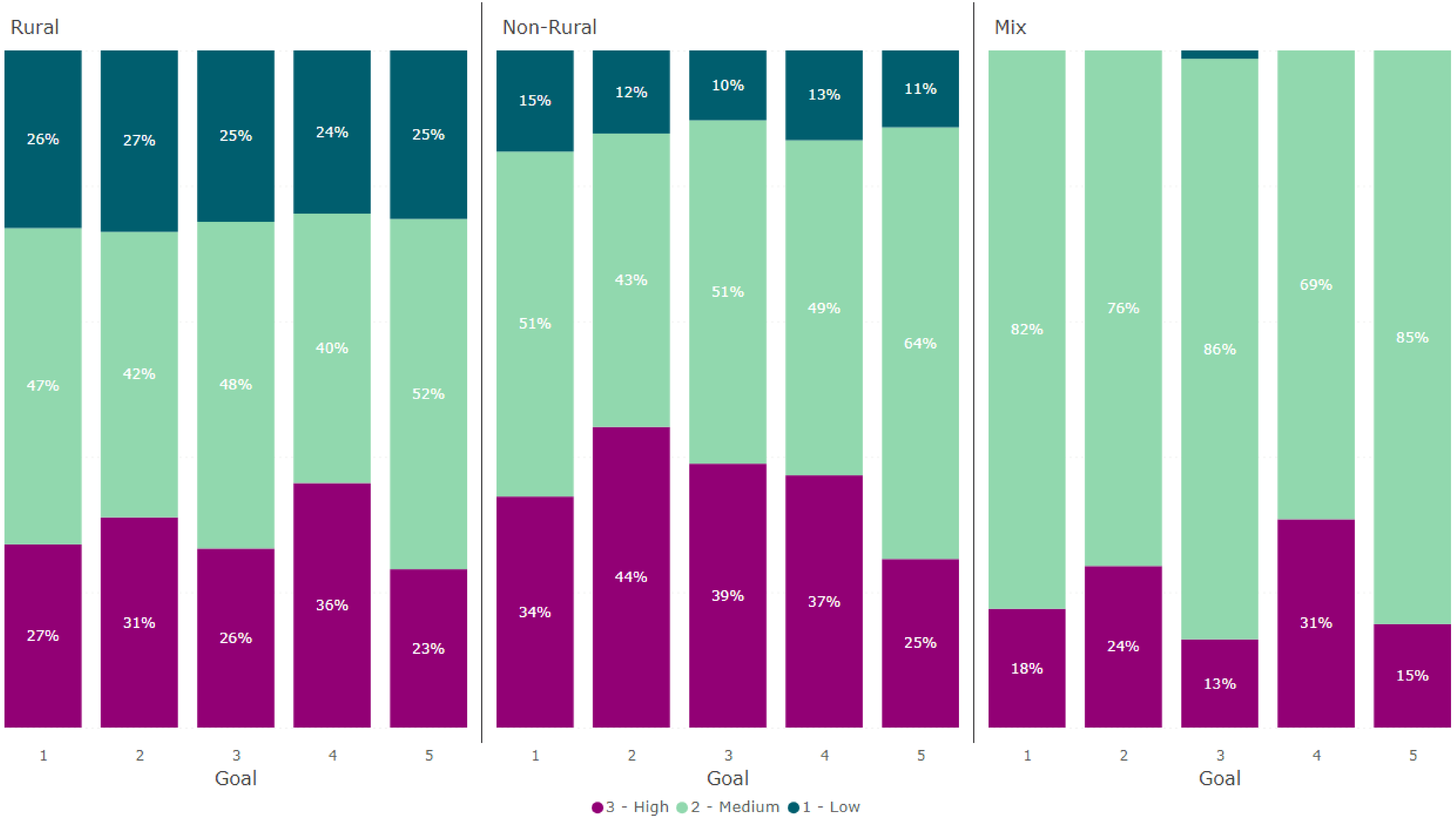
Likelihood of Success



Likelihood of Success – By Entity Type



Likelihood of Success – By Rural vs. Non-Rural


Rural
Goal
Non-Rural
Goal
Mix
Goal
● 3 - High ● 2 - Medium ● 1 - Low