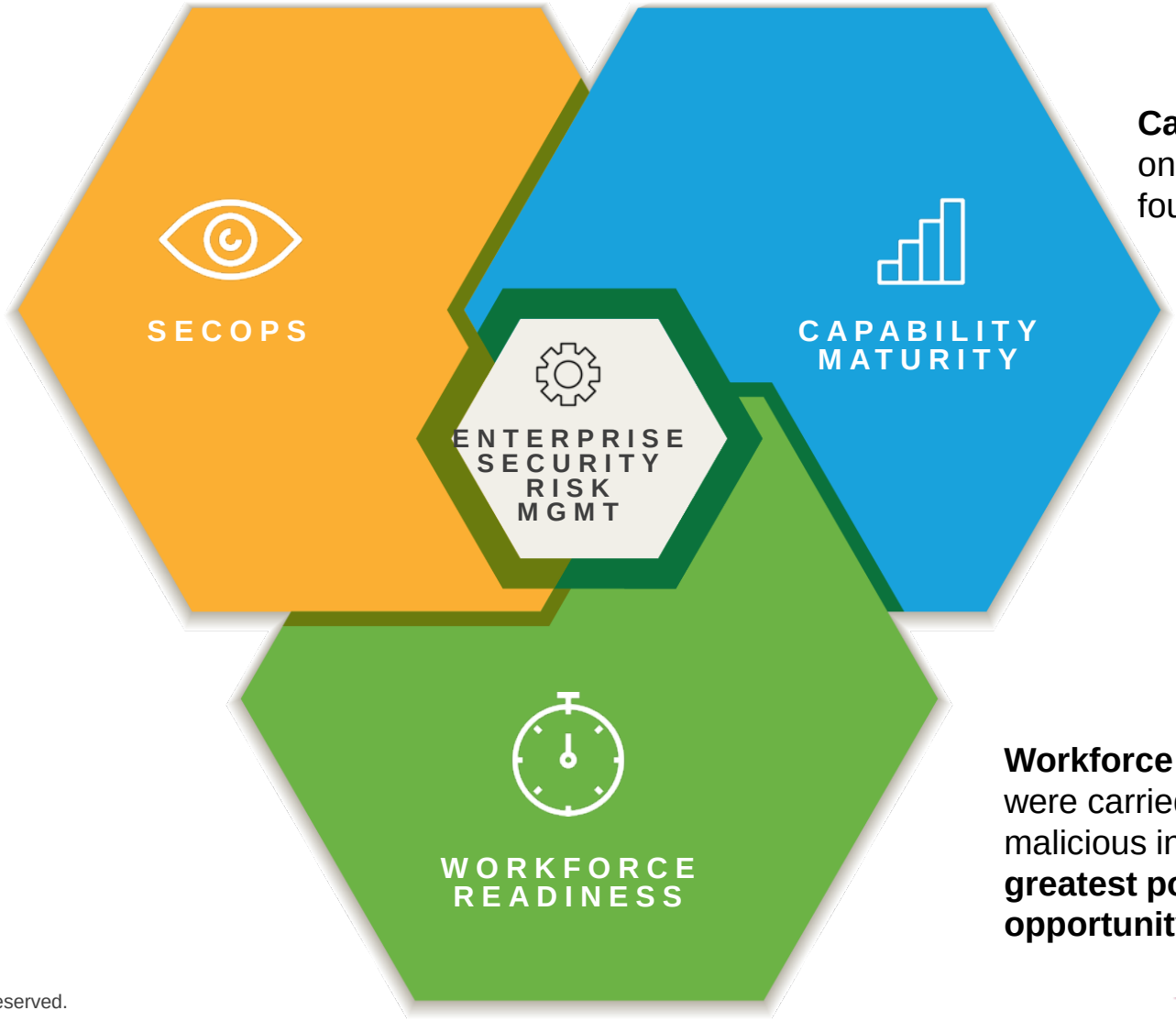
CMMI® Institute

# BUILDING CYBERSECURITY CAPABILITY, MATURITY, RESILIENCE

# CYBER SECURITY READINESS & RESILIENCE
# ASSESS THE RISKS, SCALE THE CAPABILITIES, ENTERPRISE-WIDE

**SecOps:** SecOps describes effective integration of security and IT/OT operations in **three key areas:**

- Mission priorities & dependencies
- Threat information
- Secure and available technology

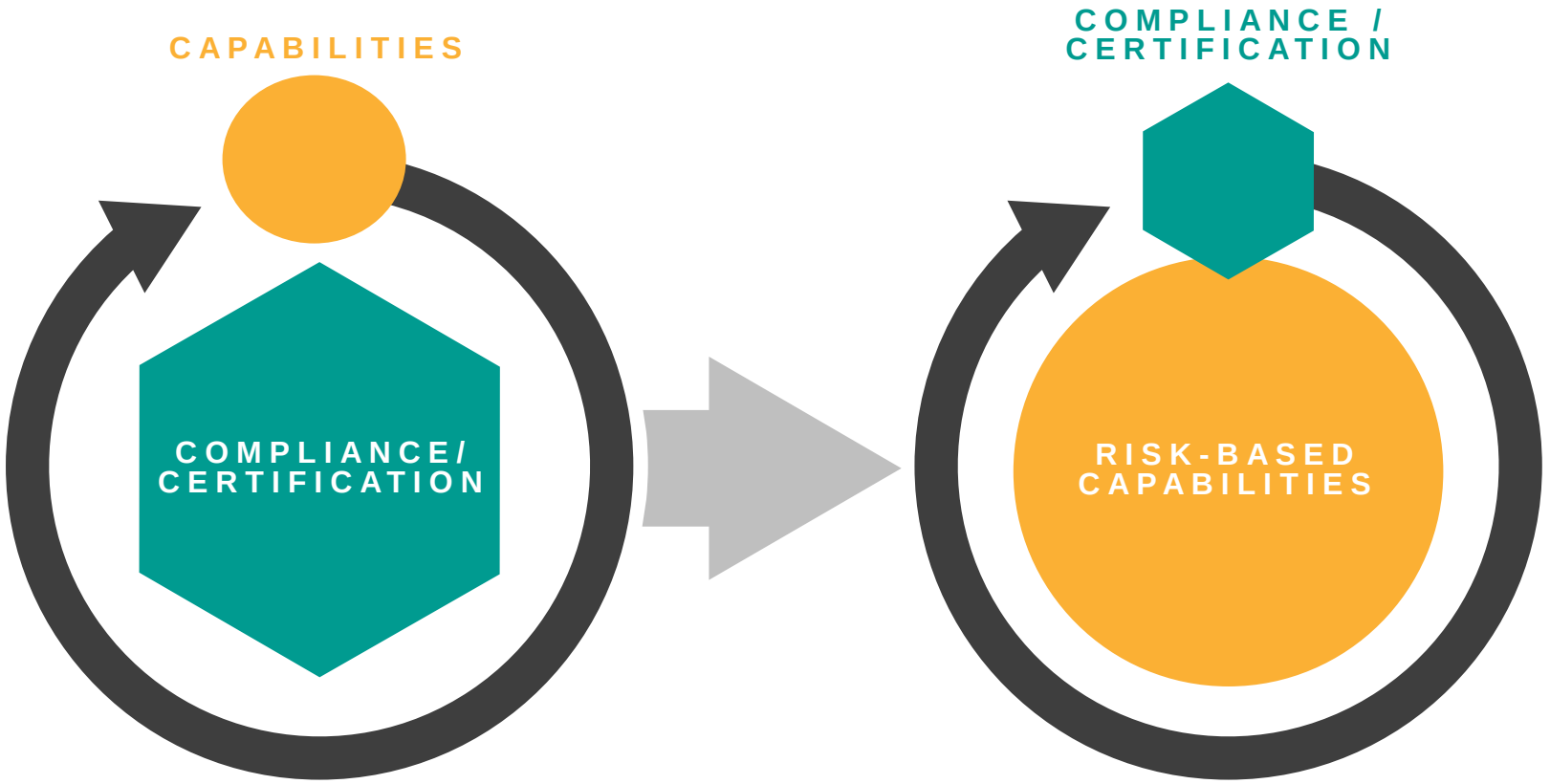



**Capability Maturity:** Focusing on **risk-based capabilities** is foundational to building resilience

**Workforce Readiness: 60%** of all attacks were carried out by insiders. **75%** involved malicious intent. The **workforce** is **our greatest point of vulnerability and opportunity**.

# FROM COMPLIANCE TO RESILIENCE

## "COPERNICAN SHIFT"

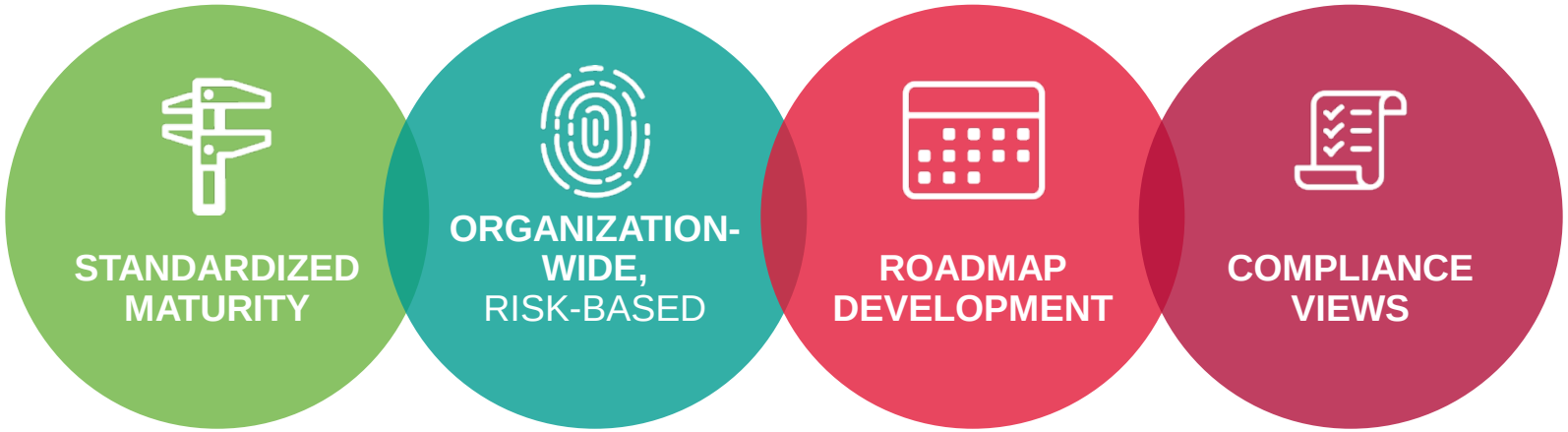



**COMPLIANCE-BASED RISK REDUCTION**

**RESILIENCE-DRIVEN RISK REDUCTION**

# Cyber Security Assessment Solution

## BENEFITS AND IMPACT




Defines maturity for people, process and technology; includes hygiene; enables industry benchmarking

t

Defines the organization's risk profile and sets maturity targets

Provides risk-based prioritization of gaps in capabilities, maturity to support roadmap development, investment options.

Provides views into compliance with industry-standard COBIT 5, ISO27001, NIST CSF, CMMI Threat Kill Chain, etc.

WE PRESENT OUR RESULTS IN

**LAYPERSON'S TERMS**

SIMPLE GRAPHICS TO SUPPORT BOARD COMMUNICATION

OUR

**COMPREHENSIVE SCOPE**

LEVERAGES LEADING FRAMEWORKS, STANDARDS AND CONTROLS

CMMI® Institute

# CMMI CYBER SECURITY CAPABILITY ASSESSMENT SUPPORTS THE LEADING INDUSTRY STANDARDS







CMMI® Institute

ISACA®

# COMPREHENSIVE CYBER ASSESSMENT ARCHITECTURE

## 1. ENSURE GOVERNANCE FRAMEWORK

| ESTABLISH GOVERNANCE | EST. BUSINESS EVALUATE RESOURCE ENVIRONMENT | GOVERN CYBERSECURITY RESOURCES | ESTABLISH STAKEHOLDER REPORTING |
|---|---|---|---|
| Establish Information Security Management Policy Process | Identify Supply Chain Role | Evaluate Resource Management Needs | Establish Stakeholder Reporting Requirements |
| Establish Governance System | Identify Critical Infrastructure Participation | Direct Resource Management Needs | Direct stakeholder communication and reporting |
| Direct Governance System | Identify Organizational Priorities | Monitor Resource Management Needs | Monitor stakeholder communication |
| Monitor Governance System | Identify Critical Dependencies | | |

## 2. ESTABLISH RISK MANAGEMENT

| ESTABLISH RISK STRATEGY | ESTABLISH BUSINESS RISK CONTEXT | IMPLEMENT RISK MANAGEMENT |
|---|---|---|
| Establish Risk Management Strategy | Determine Mission Dependencies | Establish Organization Risk Mgmt. Process |
| Establish Risk Management | Determine Legal / Regulatory Requirements | Integrate Risk Mgmt. Program |
| Define Organizational Risk Tolerance | Determine Strategic Risk Objectives | Manage External Participation |
| Determine Critical Infrastructure | | Establish Risk Mgmt. Responsibilities |

## 3. IDENTIFY AND MANAGE RISKS

| IMPLEMENT RISK IDENTIFICATION | ENSURE ACCESS CONTROL MANAGEMENT | ESTABLISH ORGANIZATIONAL TRAINING | ESTABLISH DATA SECURITY PROTECTION |
|---|---|---|---|
| Asset Discovery & Identification | Manage Identities and Credentials | General User Training | Safeguard Data at Rest |
| Vulnerability Identification | Manage Access to Systems | Privileged User Training | Safeguard Data in Transit |
| Supply Chain Risk Identification | Manage Access Permissions | 3rd Party Training | Manage Asset Lifecycle |
| Identification of Roles & Responsibilities | Manage Network Integrity & Segregation | Senior Leader Training | Capacity Planning |
| Information Classification Considerations | Manage Communication Protections | Physical Security Training | Integrity and Data Leak Prevention |

## 4. ENSURE RISK MITIGATION

| ESTABLISH SECURE APPLICATION | ESTABLISH INFORMATION PROTETCION PROVISIONS | ESTABLISH PROTECTION PLANNING | ESTABLISH PROTECTIVE TECHNOLOGY PROVISIONS |
|---|---|---|---|
| Secure Application Development | Establish Configuration Baselines | Establish Information Sharing | Establish Audit Processes |
| Manage System Engineering Process | Establish Change Control | Develop and Maintain Response / Recovery Plans | Safeguard Removable Media |
| Safeguard Development Environment | Establish Backup Processes | Integrate HR Security Components | Safeguard Operational Environment |
| Manage Software Update/Release Processes | Establish Maintenance Processes | Establish Vulnerability Mgmt. (Patch) Process | |
| | Establish Mobile Device Management | | |

## 5. ENSURE RISK DETECTION

| ESTABLISH CYBERSECURITY INCIDENT DETECTION | ESTABLISH CONTINUOUS MONITORING | ESTABLISH DETECTION |
|---|---|---|
| Establish Network Baselines | Monitor Networks | Establish Detection Roles |
| Aggregate / Correlate Data | Monitor Physical | Detect Malicious Code |
| Determine Impacts | Monitor Personnel | Detect Mobile Code and Browser Protection |
| Alert Thresholds | Monitor 3rd Parties | Implement Vulnerability Scanning |
| Est. Security Review Processes | Test Detection processes | |

## 6. ENSURE RISK RESPONSE

| ESTABLISH INCIDENT RESPONSE | ESTABLISH INCIDENT ANALYSIS | MITIGATE DETECTED INCIDENTS |
|---|---|---|
| Execute Response Plan | Implement Investigation Processes | Ensure Incident Containment |
| Response Roles & Resp. | Analyze Risk Events | Ensure Incident Mitigation |
| Incident Reporting | Implement Forensics Capability | |
| Ensure Information Sharing | Establish Response Categorization | |
| | | |

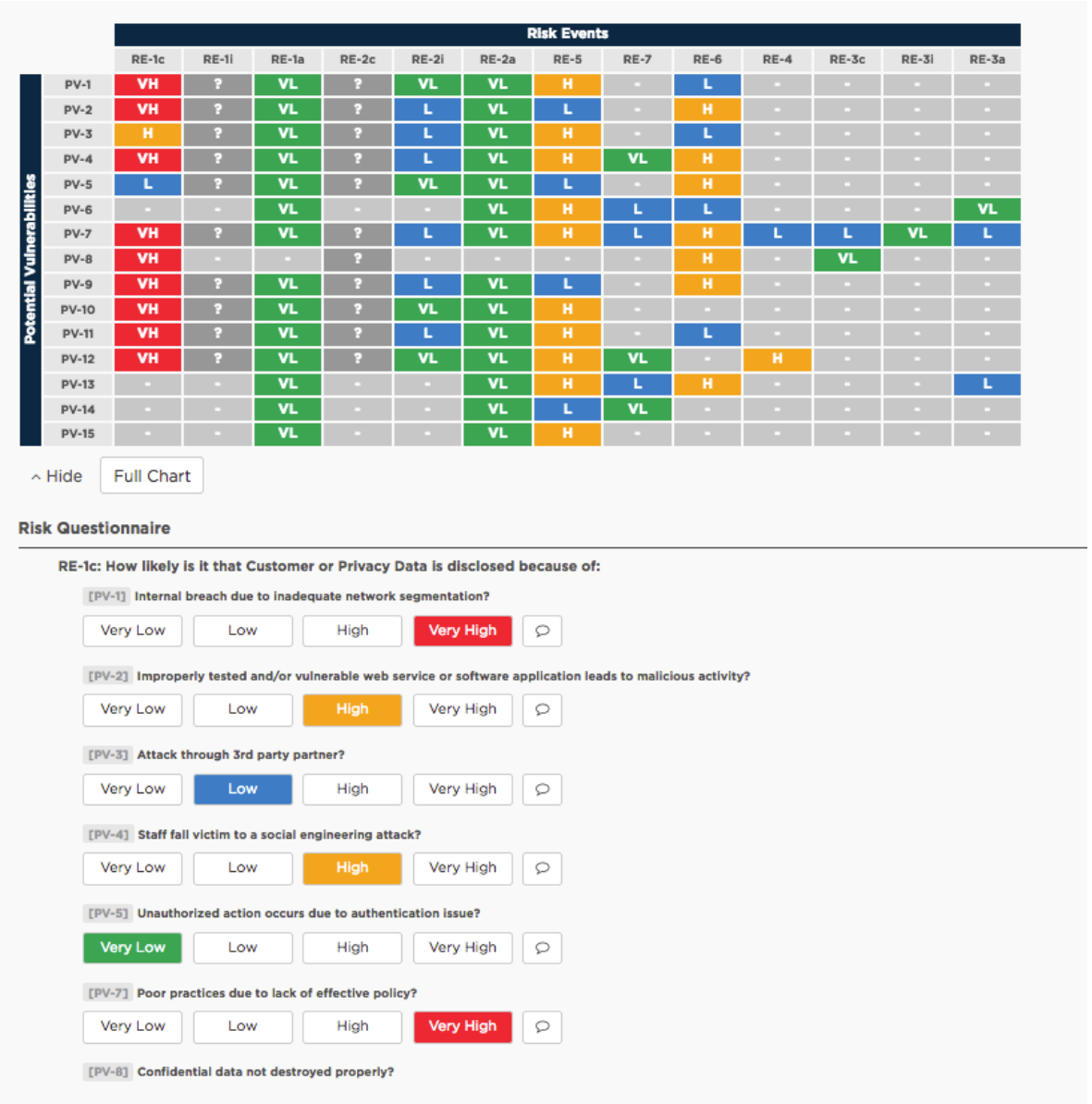
## 7. ENSURE RESILIENCE

| ESTABLISH INCIDENT RECOVERY |
|---|
| Execute Recovery Plan |
| Recovery Communications |

# CYBERSECURITY MATURITY ASSESSMENT


ISACA | CMMI Institute

# SELECT YOUR COMPANY'S UNIQUE RISK PROFILE



| Potential Vulnerabilities | Risk Events | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | RE-1c | RE-1i | RE-1a | RE-2c | RE-2i | RE-2a | RE-5 | RE-7 | RE-6 | RE-4 | RE-3c | RE-3i | RE-3a |
| PV-1 | VH | ? | VL | ? | VL | VL | H | - | L | - | - | - | - |
| PV-2 | VH | ? | VL | ? | L | VL | L | - | H | - | - | - | - |
| PV-3 | H | ? | VL | ? | L | VL | H | - | L | - | - | - | - |
| PV-4 | VH | ? | VL | ? | L | VL | H | VL | H | - | - | - | - |
| PV-5 | L | ? | VL | ? | VL | VL | L | - | H | - | - | - | - |
| PV-6 | - | - | VL | - | - | VL | H | L | L | - | - | - | VL |
| PV-7 | VH | ? | VL | ? | L | VL | H | L | H | L | L | VL | L |
| PV-8 | VH | - | - | ? | - | - | - | - | H | - | VL | - | - |
| PV-9 | VH | ? | VL | ? | L | VL | L | - | H | - | - | - | - |
| PV-10 | VH | ? | VL | ? | VL | VL | H | - | - | - | - | - | - |
| PV-11 | VH | ? | VL | ? | L | VL | H | - | L | - | - | - | - |
| PV-12 | VH | ? | VL | ? | VL | VL | H | VL | - | H | - | - | - |
| PV-13 | - | - | VL | - | - | VL | H | L | H | - | - | - | L |
| PV-14 | - | - | VL | - | - | VL | L | VL | - | - | - | - | - |
| PV-15 | - | - | VL | - | - | VL | H | - | - | - | - | - | - |

Hide | Full Chart

**Risk Questionnaire**

**RE-1c: How likely is it that Customer or Privacy Data is disclosed because of:**

[PV-1] **Internal breach due to inadequate network segmentation?**
Very Low | Low | High | **Very High**

[PV-2] **Improperly tested and/or vulnerable web service or software application leads to malicious activity?**
Very Low | Low | **High** | Very High

[PV-3] **Attack through 3rd party partner?**
Very Low | **Low** | High | Very High

[PV-4] **Staff fall victim to a social engineering attack?**
Very Low | Low | **High** | Very High

[PV-5] **Unauthorized action occurs due to authentication issue?**
**Very Low** | Low | High | Very High

[PV-7] **Poor practices due to lack of effective policy?**
Very Low | Low | High | **Very High**

[PV-8] **Confidential data not destroyed properly?**

For each Potential Vulnerability, **users will assign the likelihood** of each Risk Event resulting from Security Scenario

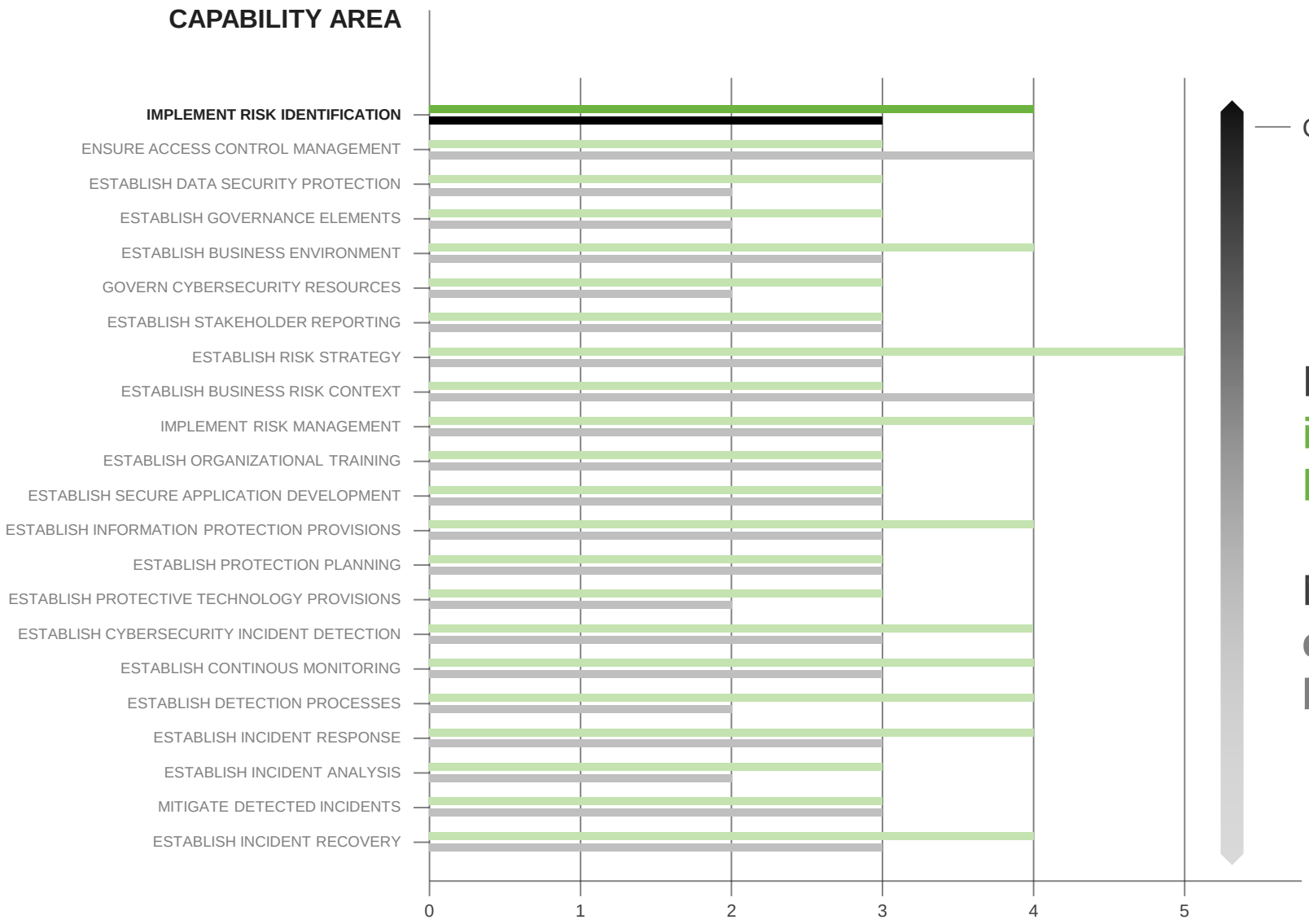
VL VERY LOW | L LOW | H HIGH | VH VERY HIGH

Once likelihood of Security Scenarios have been assigned, **users will assign an impact for each Risk Event**



ISACA | CMMI Institute

# RISK PROFILE DEFINES THE MATURITY TARGETS




Risk Profile establishes **initial target maturity by capability** area

Maturity targets can be **compared to industry benchmarks** for maturity

ISACA | CMMI Institute

# STANDARDIZED DEFINITIONS OF MATURITY

## PEOPLE, PROCESS, TECHNOLOGY

| | LEVEL 1 PERFORMED | LEVEL 2 MANAGED | LEVEL 3 DEFINED | LEVEL 4 QUANTITATIVELY MANAGED | LEVEL 5 OPTIMIZED |
|---|---|---|---|---|---|
| PEOPLE | General personnel capabilities may be performed by an individual, but are not well defined | Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization | Roles and responsibilities are identified, assigned, and trained across the organization | Achievement and performance of personnel practices are predicted, measured, and evaluated | Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external) |
| PROCESS | General process capabilities may be performed by an individual, but are not well defined | Adequate procedures documented within a subset of the organization | Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy | Policy compliance is measured and enforced<br>Procedures are monitored for effectiveness | Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured. |
| TECHNOLOGY | General technical mechanisms are in place and may be used by an individual | Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place | Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization | Effectiveness of technical mechanisms are predicted, measured, and evaluated | Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external) |

ISACA | CMMI Institute

# MEASURING MATURITY
## BASED ON ACTIVITY

IDENTIFY AND MANAGE RISKS ▶ IMPLEMENT RISK IDENTIFICATION ▶ **VULNERABILY IDENTIFICATION**

| MATURITY LEVEL | ACTIVITY AUDIT | |
|---|---|---|
| 5 | The organization collaborates with relevant partners (e.g., facilities management, system operations staff) to periodically catalog known vulnerabilities. | ☐ |
| 5 | Staff have been trained and qualified to perform vulnerability identification activities as planned. | ☐ |
| 5 | Relevant managers oversee performance of the vulnerability identification activities. | ☐ |
| 4 | Issues related to vulnerability identification are tracked and reported to relevant managers. | ☐ |
| 4 | Underlying causes for vulnerabilities are identified (e.g., through root-cause analysis) | ☐ |
| 4 | Risks related to the performance of vulnerability identification activities are identified, analyzed, disposed of, monitored, and controlled. | ☐ |
| 4 | Vulnerability identification activities are periodically reviewed to ensure they are adhering to the plan. | ☐ |
| 3 | Stakeholders for vulnerability management activities have been identified and made aware of their roles. | ☐ |
| 3 | A standard set of tools and/or methods is used to identify vulnerabilities. | ☐ |
| 3 | Vulnerability management tools identify those types of platform (e.g., OS, application, device) affected by known vulnerabilities | ☐ |
| 2 | Approved and diverse vulnerability sources are identified and documented. | ■ |
| 2 | **Automated vulnerability scanning tools review all applicable systems on the network (a & b required)** | ■ |
| | **a. An SCAP-validated vulnerability scanner is used that looks for both code-based vulnerabilities and configuration-based vulnerabilities** | ■ |
| | **b. Vulnerability scans are executed on all applicable devices on a weekly or more frequent basis** | ■ |
| 2 | Risk scores compare the effectiveness of system administrators and departments in reducing risk. | ■ |
| 2 | **Vulnerability scanning occurs in authenticated mode using a dedicated account with administrative rights. (a1 OR a2 & b required)** | ☐ |
| | **a1. Vulnerability Agents operate locally on each applicable end system to analyze the security configuration** | ■ |
| | **a2. Remote scanners have administrative rights on each applicable end system to analyze the security configuration** | ☐ |
| | **b. Dedicated account is used for authenticated vulnerability scans (not used for any other activities)** | ☐ |
| 2 | Only authorized employees have access to the vulnerability management user interface and that roles are applied to each user. | ■ |
| 2 | There exists a documented plan for performing vulnerability identification activities. | ■ |
| 2 | Vulnerabilities are categorized and prioritized. | ■ |
| 2 | Specific vulnerabilities that may impact mission-critical personnel, facilities, and resources are identified and catalogued. | ■ |
| 1 | A repository is used for recording information about vulnerabilities and their resolutions. | ■ |
| 1 | Vulnerability management tools identify those types of platform (e.g., OS, application, device) affected by known vulnerabilities | ■ |
| 1 | The organization has identified potential logical vulnerabilities that might lead to known risks. | ■ |
| 1 | Tools are in place to periodically identify new/updated vulnerabilities that may impact organizational systems. | ■ |
| 1 | Subscription mechanisms ensure that current vulnerability lists are maintained. | ■ |

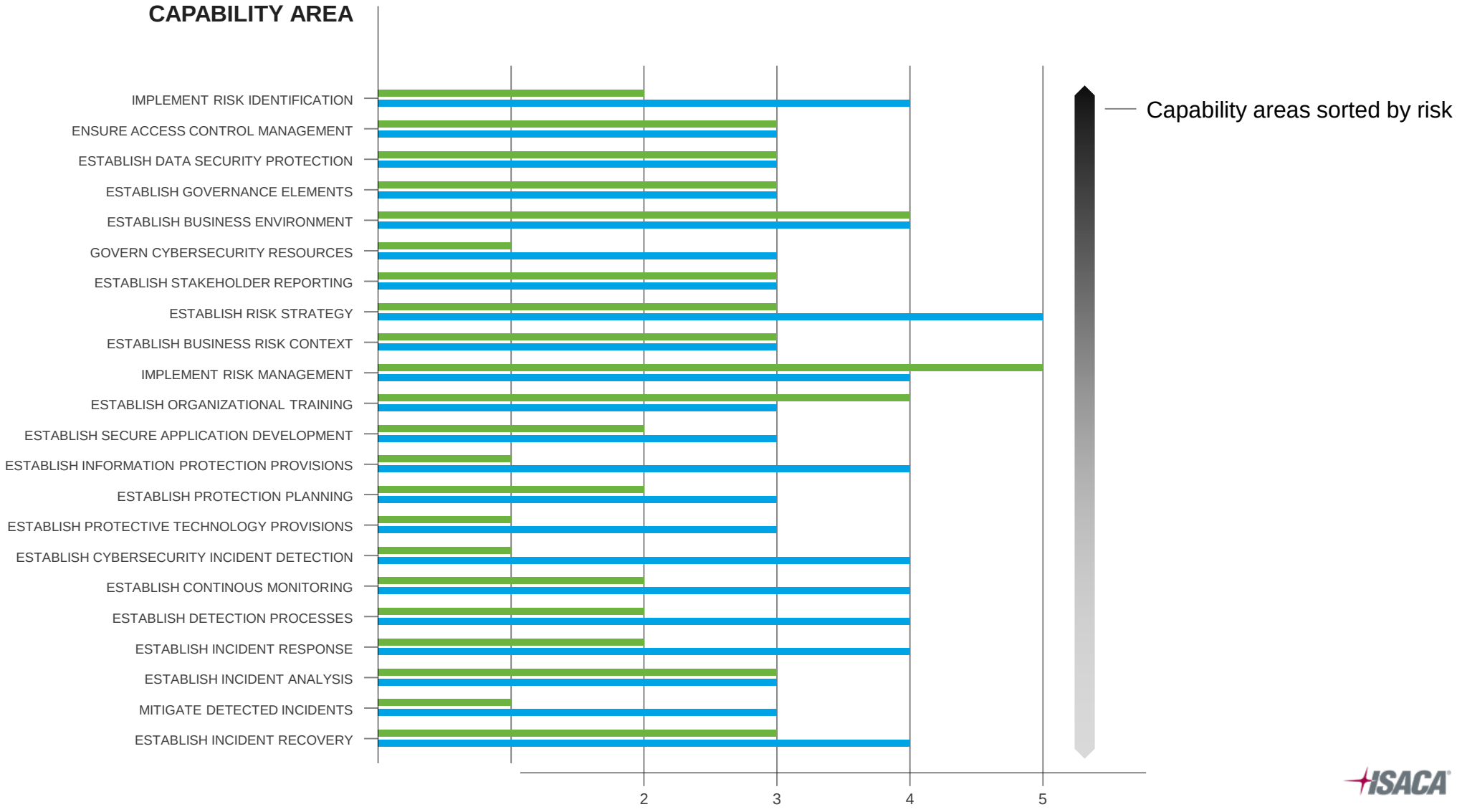
PRACTICE AREA MATURITY

# LEVEL 1

OVERALL MATURITY FOR THIS PRACTICE AREA IS L1 AS NOT ALL BOXES WERE CHECKED FOR L2

# OUTPUT REPORTS

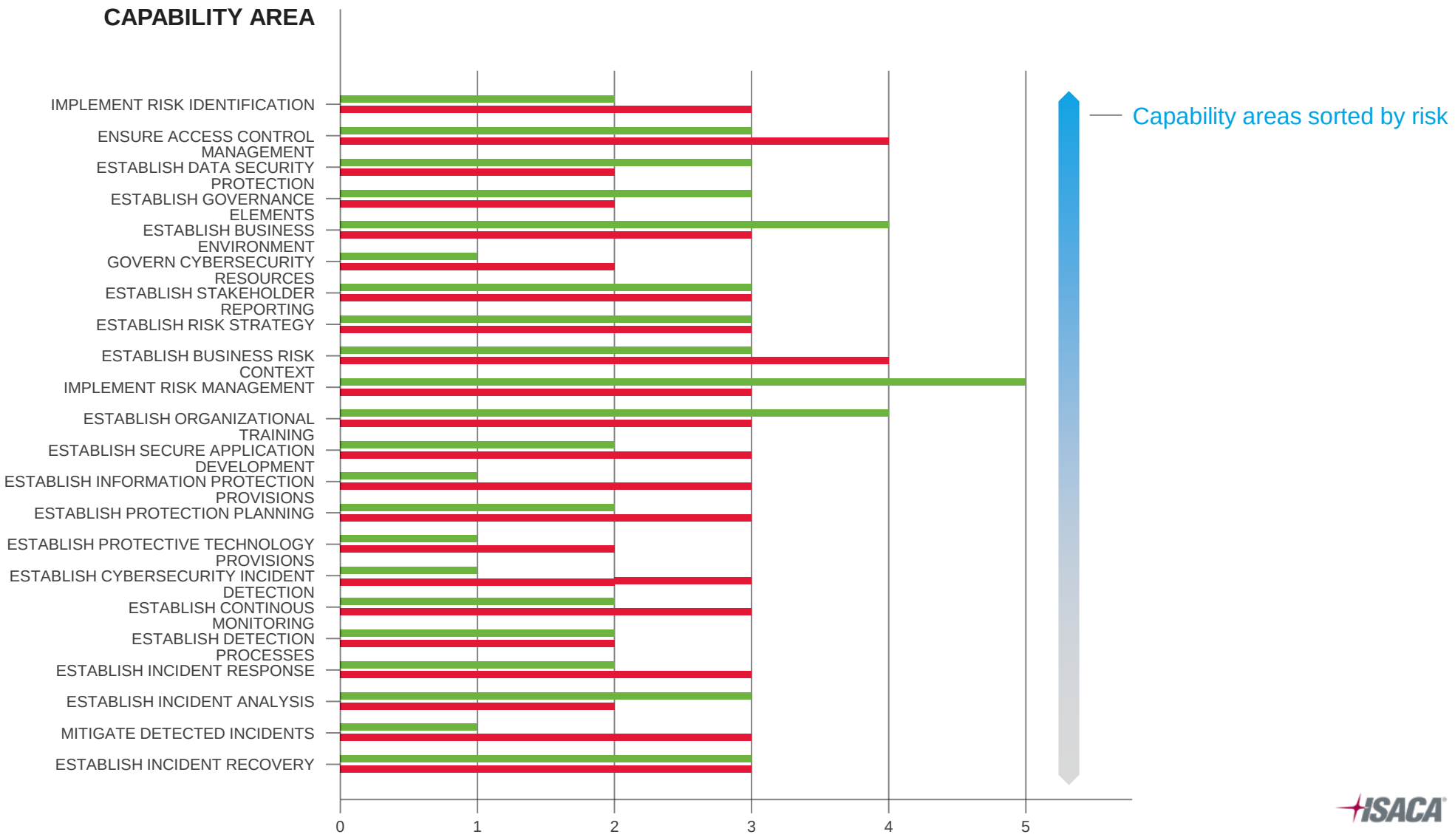
## MEASURED MATURITY VS. RISK-BASED TARGET




ISACA | CMMI Institute

# OUTPUT REPORTS (BENCHMARKS)

## MEASURED MATURITY VS. INDUSTRY MATURITY



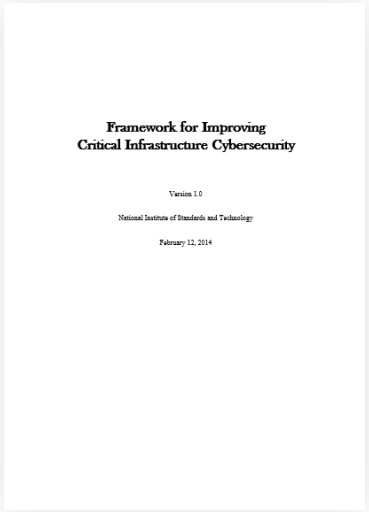
# ROADMAP DEVELOPMENT

## SPECIFIC PRACTICES AND PRIORITIZED FIRST BY RISK


ISACA | CMMI Institute

# NIST CYBERSECURITY ALIGNMENT BY PRACTICE AREA

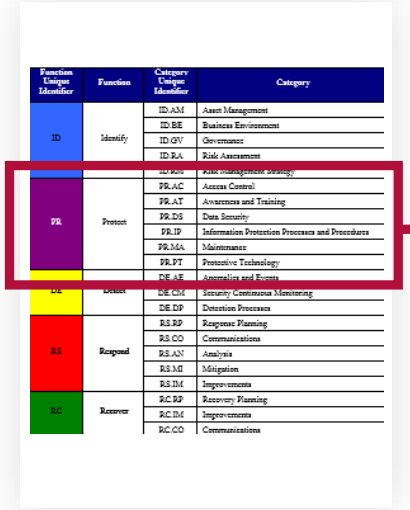
## FILTERED RESULTS


Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014



| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

| | | MEASURED | RISK-BASED TARGET | SELECTED MATURITY LEVEL 4 |
|---|---|---|---|---|
| PR.IP | Information Protection Processes and Procedures | | | |
| PR.IP-2 | A System Development Life Cycle to manage systems is implemented | 16 | 25 | 37 |
| PR.AT | 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. | | | |
| PR.AT-2 | Privileged users understand roles & responsibilities | 1 | 2 | 4 |
| PR.DS | Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. | | | |
| PR.DS-7 | The development and testing environment(s) are separate from the production environment | 1 | 1 | 3 |

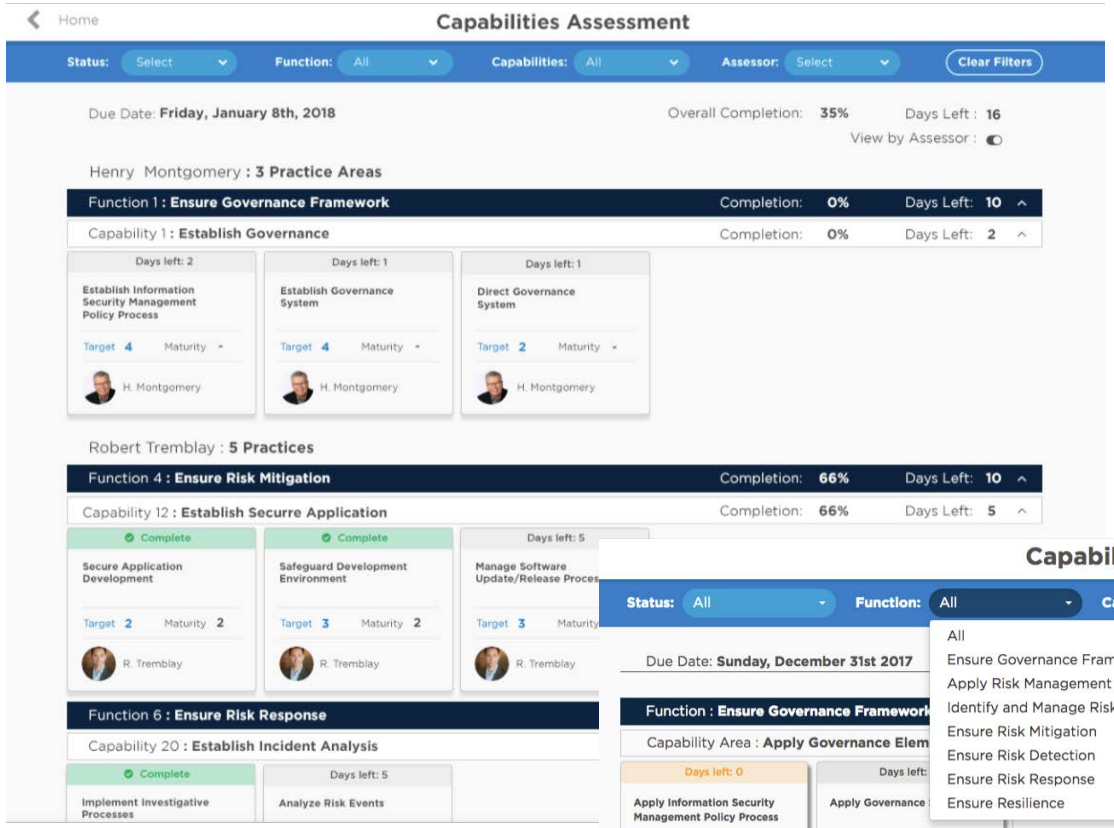
NIST Cybersecurity Framework

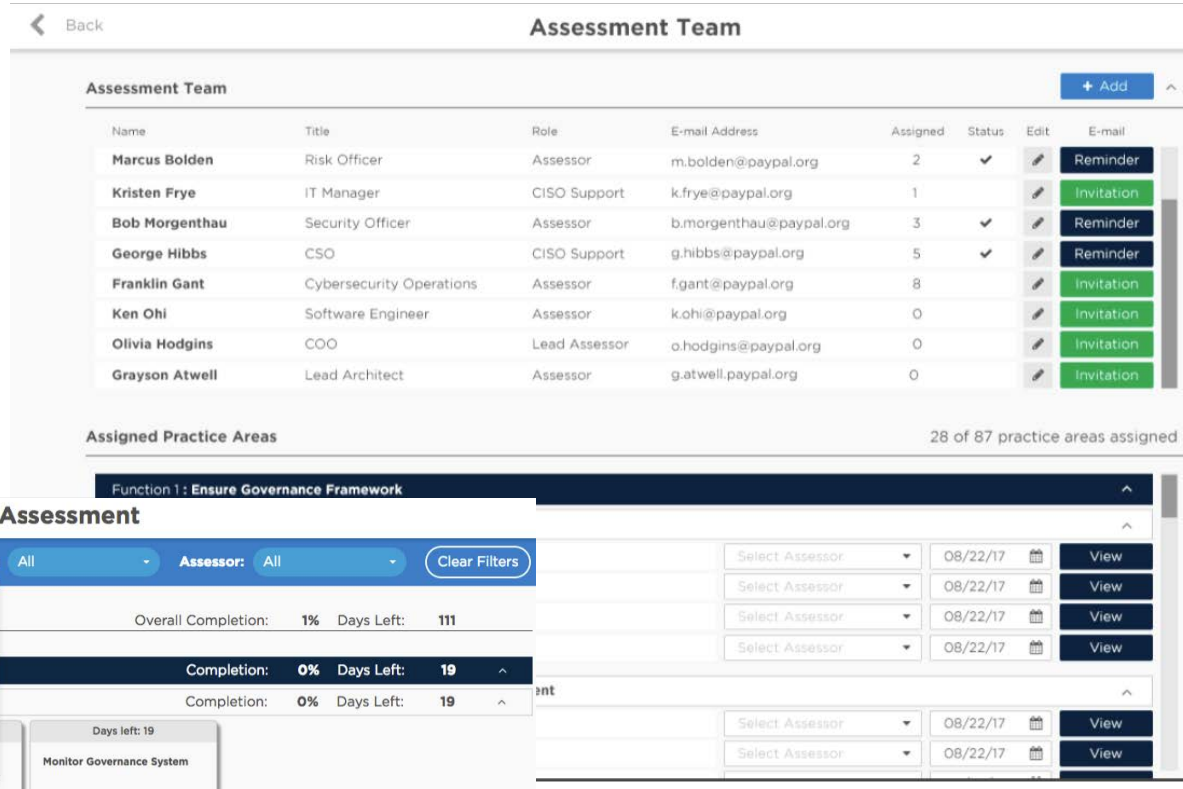
## PRACTICES

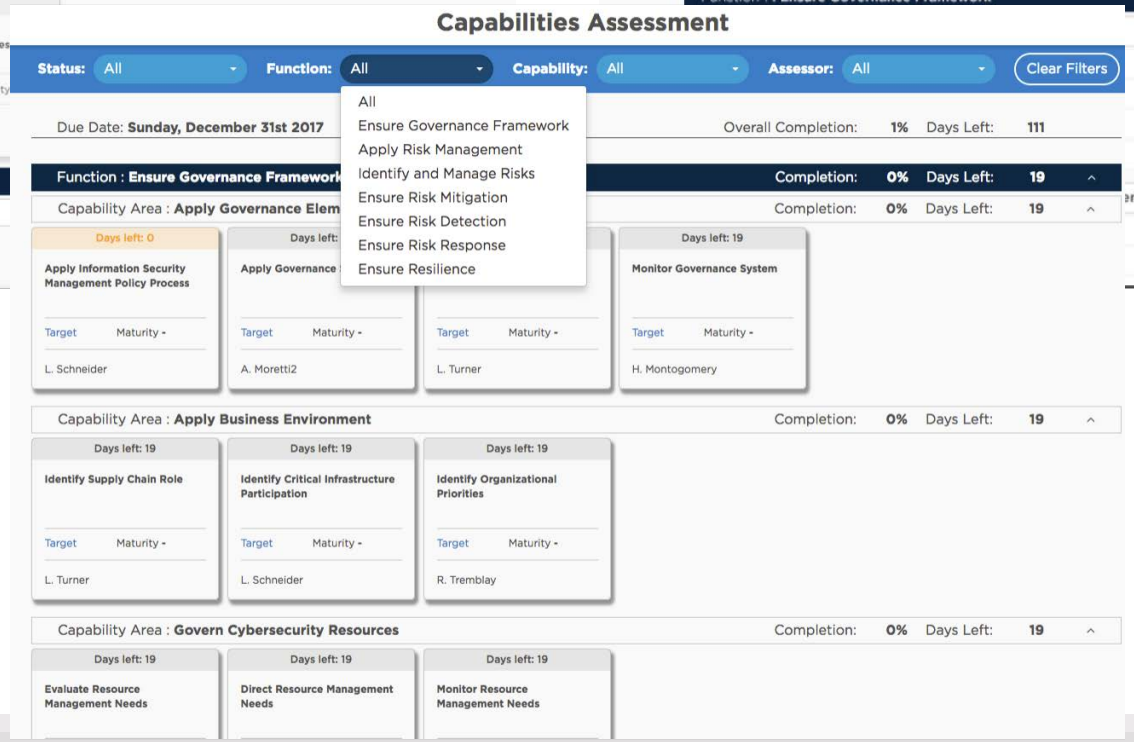
| | |
|---|---|
| Users are formally assigned roles and responsibilities aligned to their work role | ☐ |
| Staff with supply chain risk management responsibilities are trained on the objectives of the supply chain risk management program | ■ |

ISACA

# TRACKING TOOLS KEEP TEAM ON-TRACK




ISACA | CMMI Institute

# CYBER SECURITY READINESS & RESILIENCE
# ASSESS THE RISKS, SCALE THE CAPABILITIES

# QUESTION-FEEDBACK SUMMARY