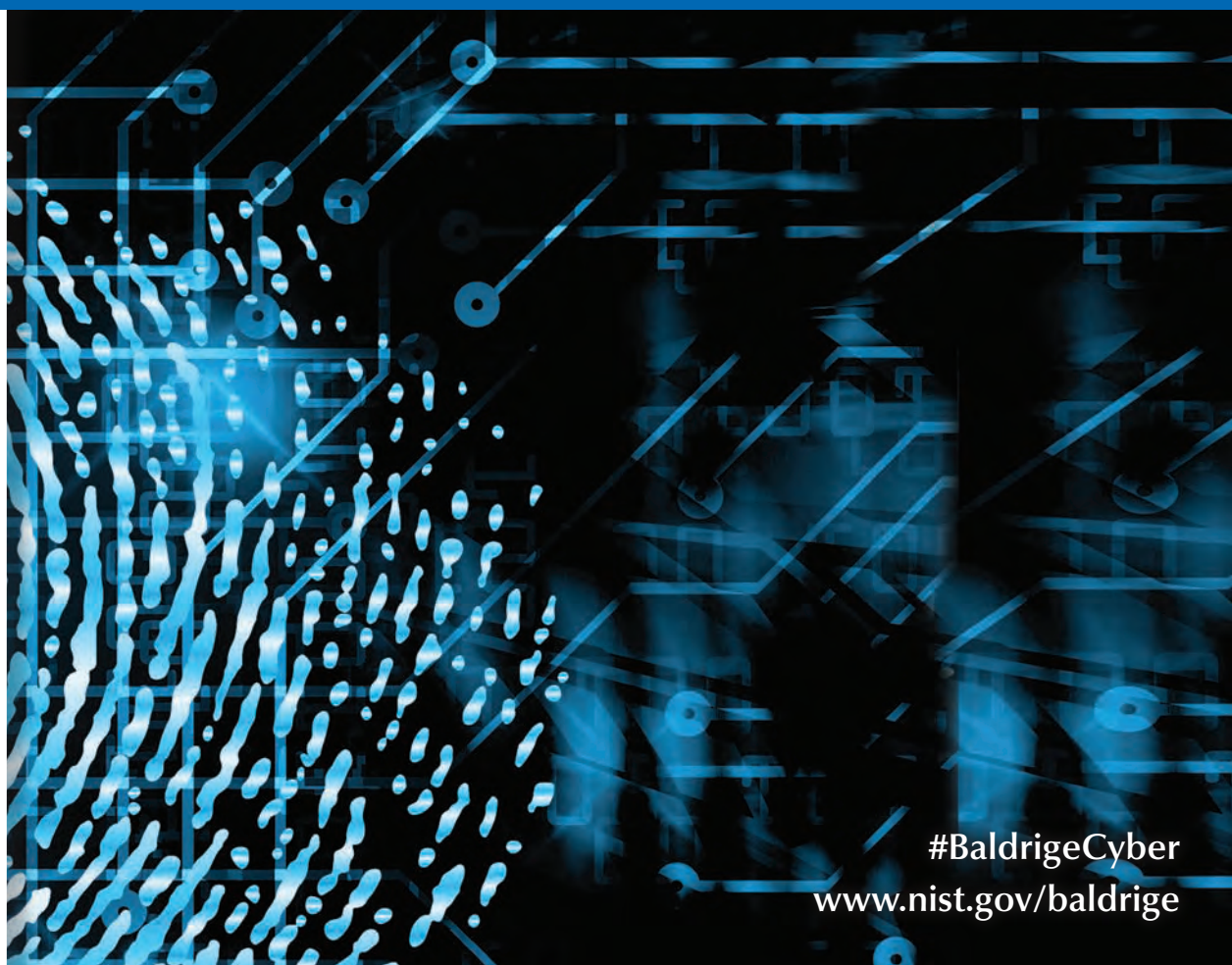
BALDRIGE
Performance Excellence Program

BALDRIGE CYBERSECURITY EXCELLENCE BUILDER

Key questions for improving your organization's cybersecurity performance



v1.1
2019

#BaldrigeCyber
www.nist.gov/baldrige

Improve Your Performance

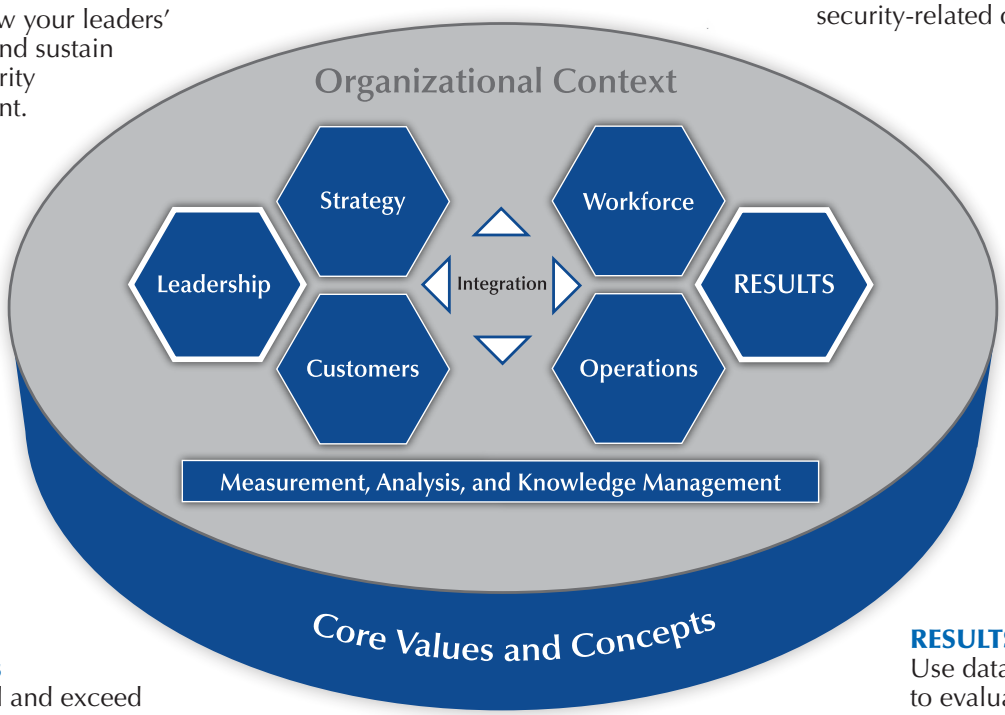
The *Baldrige Cybersecurity Excellence Builder* self-assessment helps you understand and improve what is critical to your organization's cybersecurity risk management. It is a voluntary self-assessment based on the more detailed *Framework for Improving Critical Infrastructure Cybersecurity*, managed by NIST's Information Technology Laboratory, Applied Cybersecurity Division, and the *Baldrige Excellence Framework*, compiled by the Baldrige Performance Excellence Program at NIST.

Organizational Context
Understand the business factors and organizational priorities underlying your cybersecurity risk management.

Strategy
Create clear strategic priorities for your cybersecurity program.

Workforce
Engage and empower your entire workforce to achieve your cybersecurity-related objectives.

Leadership
Understand how your leaders' actions guide and sustain your cybersecurity risk management.



Customers
Understand and exceed the cybersecurity-related requirements and expectations of your customers.

RESULTS
Use data and information to evaluate and improve cybersecurity-related policies and operations in alignment with your strategy.

Measurement, Analysis, and Knowledge Management
Through measurement and analysis, align cybersecurity policies and operations with your objectives. Manage your organization's cybersecurity-related knowledge.

Operations
Design, manage, and improve your cybersecurity operations for effectiveness and efficiency.

For more information on the Baldrige Cybersecurity Initiative:

www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

The Baldrige Program thanks the Baldrige Foundation for supporting the program's mission and the following organizations for supporting the publication of this booklet.

Contents

On the Web

For spreadsheet versions of the *Baldrige Cybersecurity Excellence Builder* questions and Self-Analysis Worksheet, see www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

Introduction

What is the *Baldrige Cybersecurity Excellence Builder*?

The *Baldrige Cybersecurity Excellence Builder* (*BCEB*) is a voluntary self-assessment tool that enables organizations to better understand the effectiveness of their cybersecurity risk management efforts. It helps your organization identify strengths and opportunities for improvement in managing cybersecurity risk based on your organization's mission, needs, and objectives.

The *BCEB* combines concepts in the *Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework;* www.nist.gov/cyberframework) and the *Baldrige Excellence Framework* (www.nist.gov/baldrige/publications). Like those two sources, it is not a one-size-fits-all approach. It is adaptable and scalable to your organization's needs, goals, capabilities, and environment. It does not prescribe how you should structure your organization's cybersecurity policies and operations. Through interrelated sets of open-ended questions, it encourages you to use the approaches that best fit your organization. Version 1.1 of the *BCEB* reflects the *2019–2020 Baldrige Excellence Framework* and the *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1.

Using this self-assessment, you can

- determine cybersecurity-related activities that are important to your business strategy and critical service delivery;
- prioritize your investments in managing cybersecurity risk;
- determine how best to enable your workforce, customers, suppliers, partners, and collaborators to be risk-conscious and security-aware, and to fulfill their cybersecurity roles and responsibilities;
- assess the effectiveness and efficiency of your use of cybersecurity standards, guidelines, and practices;
- assess the cybersecurity results you achieve; and
- identify strengths to leverage and priorities for improvement.

What is the relationship between the *BCEB* and the *Framework for Improving Critical Infrastructure Cybersecurity*?

The *BCEB* blends the organizational performance and systems perspectives of the *Baldrige Excellence Framework* with the holistic, enterprise-based approach of the *Cybersecurity Framework*.

The *Cybersecurity Framework* assembles and organizes standards, guidelines, and practices that are working effectively in many organizations. It also includes informative references that are common across critical infrastructure sectors. In the Baldrige approach as applied to cybersecurity, an organization manages all areas affected by cybersecurity as a unified whole. As shown in the diagram on the inside front cover, the system consists of your cybersecurity-related approaches in the areas of leadership, strategy, customers, workforce, and operations, as well as the results you achieve. (As shown in the diagram, the Baldrige framework is based on a set of core values and concepts. For descriptions of these, see the Baldrige framework booklet, www.nist.gov/baldrige/publications.) The system foundation

is measurement, analysis, and knowledge management. The background for all of these components is the Organizational Context, in which you define your organization's distinctive characteristics and situation.

The *BCEB* incorporates the content outlined in the *Cybersecurity Framework* into those system elements. See the User Tools section for a crosswalk showing how the items in the *BCEB* relate to the elements of the *Cybersecurity Framework*.

Who in an organization should use the *BCEB*?

The *BCEB* is intended for use by the leaders and managers in your organization who are concerned with and responsible for mission-driven, cybersecurity-related policy and operations. These leaders and managers may include senior leaders, chief security officers, and chief information officers, among others. For these and other roles and functions, and the benefits to each of using the *BCEB*, see the User Tools section.

Why does the *BCEB* include questions about my organization as a whole? Why doesn't it ask only about my cybersecurity policies and operations?

Because cybersecurity is an organization-wide concern, the *BCEB* includes questions about

- your organizational *and* your cybersecurity leaders,
- cybersecurity in the context of your organization's overall strategy,
- the cybersecurity needs and expectations of internal and external customers,
- the measurement of cybersecurity performance in the context of overall performance measurement,
- your overall workforce *and* your cybersecurity workforce,
- your overall *and* your cybersecurity suppliers and partners,
- your cybersecurity operations *and* their alignment with overall operations, and
- results related to each of these areas.

The *BCEB* leads to you understand your organization's cybersecurity policies and operations in the context of its unique characteristics, strategic situation, and cybersecurity risks.

How can my organization use the *BCEB* to assess and improve its management of cybersecurity risks?

The *BCEB* asks you to describe your Organizational Context, define your processes, and report your results. As you do so, notice the linkages among these elements (e.g., describing your workforce in C.1a[3], detailing your workforce processes for in category 5, and stating your workforce results in item 7.3). The linkages among these categories help you align your processes and results with your unique organizational characteristics and situation. For examples of these linkages, see page 31.

1. Scope

The *BCEB* is most valuable as a voluntary assessment of an entire organization's cybersecurity risk management program, but it is also useful in assessing a subunit, multiple subunits, or parts of an organization.

2. Organizational Context

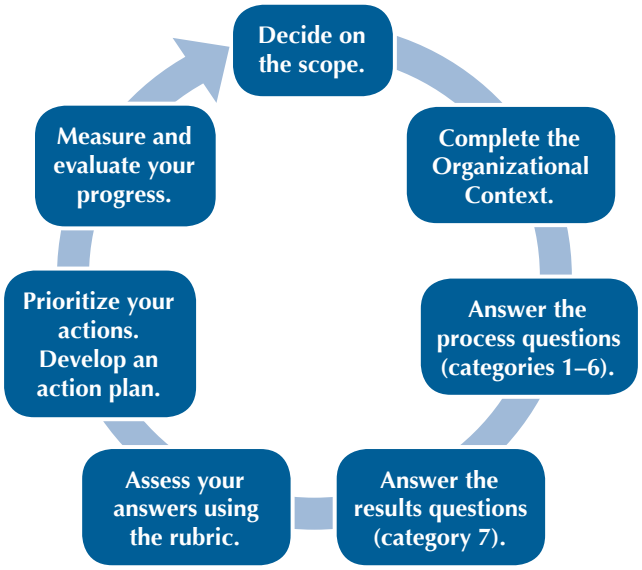
The Organizational Context section is critically important for the following reasons:

- It helps you identify gaps in key information and focus on key cybersecurity performance requirements and results.
- You can use it as an initial self-assessment. If you identify topics for which conflicting, little, or no information is available, you can use these topics for action planning.
- It sets the context for understanding your organization's cybersecurity-related needs and responding to the questions in the rest of the *BCEB*.

3. Process Questions (Categories 1–6)

Many of the questions in these 12 items begin with "how." In answering the questions, give information on your organization's key cybersecurity-related *processes*:

- *Approach:* How do you accomplish your organization's cybersecurity-related work? How systematic are the key processes you use?
- *Deployment:* How consistently are your key cybersecurity-related processes used in relevant parts of your organization?
- *Learning:* How well have you evaluated and improved your key cybersecurity-related processes? How well have improvements been shared within your organization?
- *Integration:* How well do your cybersecurity-related processes address your current and future organizational needs?



4. Results Questions (Category 7)

For these five items, give information on the cybersecurity-related *results* that are the most important to your organization's success:

- *Levels:* For your key measures of the effectiveness and efficiency of cybersecurity-related processes, what is your current performance?
- *Trends:* Are the results improving, staying the same, or getting worse?
- *Comparisons:* How does your performance compare with that of other organizations and competitors, or with benchmarks?
- *Integration*: Are you tracking cybersecurity-related results that are important to your organization and consider the expectations and needs of your key stakeholders? Are you using the results in decision making?

5. Assess Your Responses

Using the process and results assessment rubrics on pages 26 and 27, assign a descriptor (Reactive, Early, Developing, Mature, Leading, or Exemplary) to your responses to each item.

6. Prioritize Your Actions; Develop an Action Plan

Then determine the importance of areas of strength and opportunities for improvement. Celebrate the strengths of your cybersecurity risk management program, and build on them to improve what you do well. Sharing what you do well with the rest of your organization can speed improvement. Also, prioritize your opportunities for improving your cybersecurity-related processes and results; you cannot do everything at once. Think about what is most important for your organization as a whole at this time, balancing the differing needs and expectations of your stakeholders and your expected results, and decide what to work on first.

7. Measure and Evaluate Your Progress

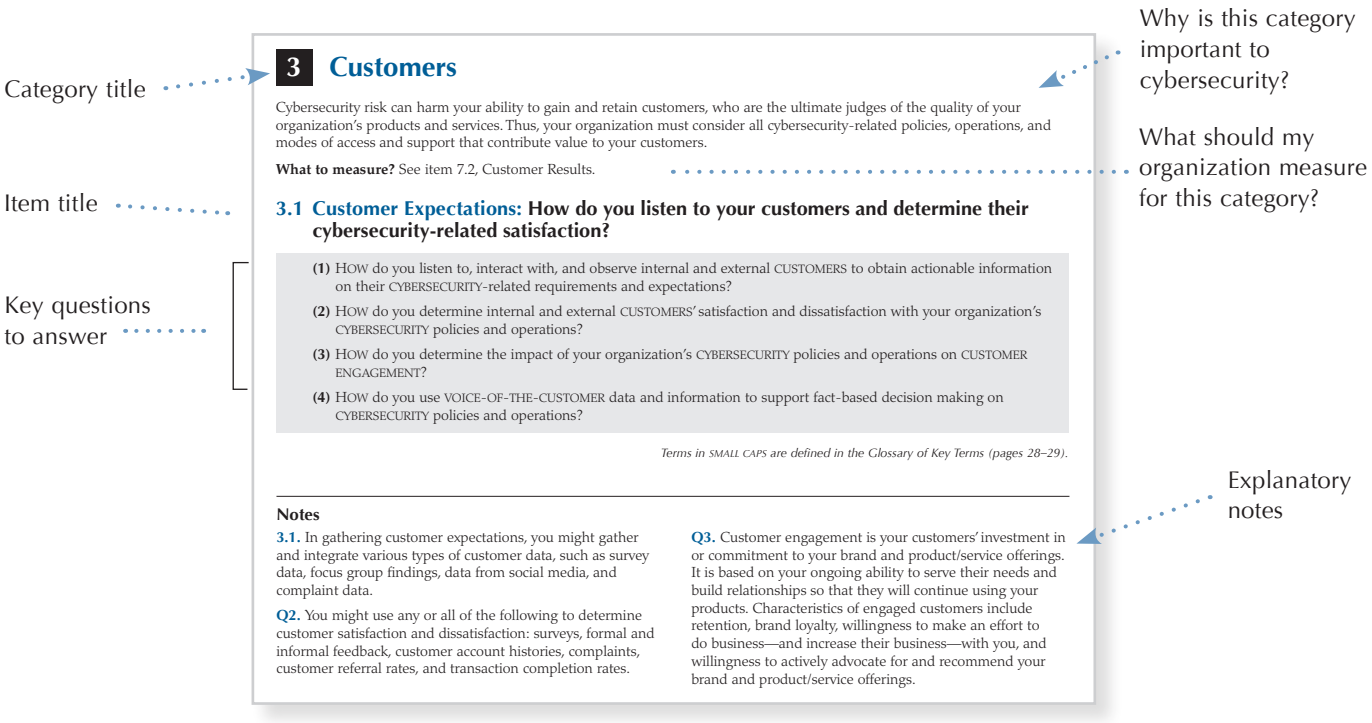
As you respond to the questions and gauge your responses against the rubric, you will begin to identify strengths and gaps—first within the categories and then among them. The coordination of key processes, and linkages between your processes and your results, can lead to cycles of improvement. As you continue, you will begin to define the best ways to build on your strengths, close gaps, and innovate.

You might also consult relevant informative references listed in the *Cybersecurity Framework.* These specific sections of standards, guidelines, and practices common among critical infrastructure sectors illustrate methods to achieve the outcomes associated with cybersecurity functions.

In addition, completing this voluntary self-assessment might serve as a first step in carrying out these suggestions in the *Cybersecurity Framework*, section 3.0 ("How to Use the Framework"):

- 3.1 Basic Review of Cybersecurity Practices: Use your answers to the self-assessment questions to compare your current cybersecurity-related activities with those outlined in the *Cybersecurity Framework* Core.
- 3.2 Establishing or Improving a Cybersecurity Program: Use your answers to the self-assessment questions to inform the seven steps outlined in that subsection.
- 3.3 Communicating Cybersecurity Requirements with Stakeholders: Your answers to the questions might inform the creation of a Target Profile.

Baldrige Cybersecurity Excellence Builder Category Structure



C Organizational Context

The Organizational Context is a snapshot of your organization and its strategic environment. With a clear understanding of your organization, why it exists, where your senior leaders want to take it in the future, who your key stakeholders are, what their expectations are, and what resources support critical functions, you will be better able to make and implement strategic decisions about cybersecurity risks, policies, and operations.

C.1 Organizational Description: What are your key organizational characteristics?

a. Organizational Environment

(1) Product Offerings What are your organization's main product and service offerings? What is the relative importance of each to your success? What mechanisms do you use to deliver your products and services?

(2) MISSION, VISION, and VALUES What are your stated MISSION, VISION, and VALUES? Other than VALUES, what are the characteristics of your organizational culture, if any? What are your organization's CORE COMPETENCIES, and what is their relationship to your MISSION?

(3) WORKFORCE Profile What is your overall WORKFORCE profile? What is your CYBERSECURITY WORKFORCE profile? What recent changes have you experienced in the composition of your overall and your CYBERSECURITY WORKFORCE or in your needs for them? What are

- your overall WORKFORCE and CYBERSECURITY WORKFORCE employee groups and SEGMENTS; and
- the KEY drivers that engage them in accomplishing their work, including CYBERSECURITY-related work, and in achieving your MISSION and VISION?

(4) Assets What are your organization's major physical and virtual assets, including its data, knowledge, devices, systems, and facilities? What are your priorities for protecting these assets, based on their criticality and business VALUE?

(5) Legal and Regulatory Requirements What are the KEY laws and regulations relating to CYBERSECURITY in your industry? Relating to CYBERSECURITY, what are the KEY applicable

- safety regulations;
- accreditation, certification, or registration requirements;
- industry standards; and
- environmental, financial, and product regulations?

b. Organizational Relationships

(1) Organizational Structure What are your overall organizational leadership structure and GOVERNANCE structure? What are the reporting relationships among your GOVERNANCE board, SENIOR LEADERS, and parent organization, as appropriate? What is the structure of your CYBERSECURITY operations? What are the reporting relationships among your SENIOR LEADERS and your CYBERSECURITY leaders and managers?

(2) CUSTOMERS and STAKEHOLDERS What are your KEY internal and external CUSTOMER groups and STAKEHOLDER groups, as appropriate? What are their KEY requirements and expectations for your CYBERSECURITY policies and operations, including any differences among these groups?

(3) Suppliers, PARTNERS, and COLLABORATORS What are your KEY types of suppliers, PARTNERS, and COLLABORATORS for your organization as a whole and for your CYBERSECURITY operations? What role do they play in producing and delivering your KEY products and services and your CUSTOMER support services? What roles do they play in your CYBERSECURITY operations? What are your KEY CYBERSECURITY requirements for suppliers? What are your KEY supply-network requirements?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

C.1a(2). Core competencies are your organization's areas of greatest expertise. They are those strategically important, possibly specialized capabilities that are central to fulfilling your mission or that provide an advantage in your marketplace or service environment. Your core competencies should inform the decisions you make about cybersecurity roles, responsibilities, and risks.

C.1a(3). "Workforce" refers to the people actively involved in accomplishing your organization's work. It includes permanent, temporary, and part-time personnel, as well as any contract employees you supervise. You should describe your suppliers in response to C.1b(3).

C.1a(3). Workforce or employee groups and segments might be based on type of employment or contract-reporting relationship, location (including telework), tour of duty, work environment, or other factors. Your cybersecurity workforce profile might include information on education, tenure, certifications, and other key characteristics. This information will help you establish and manage cybersecurity roles and responsibilities for the entire workforce.

C.1a(4). Assets include physical devices and systems, software platforms and applications, operational technologies, intellectual property, organizational communication and data flows, external information systems (including "cloud services"), and data and information. Your responses should include those high-value assets that support the strategically important products and services you describe in C.1a(1).

C.1b(2). Customer groups might be based on common expectations, behaviors, preferences, or profiles.

C.2 Organizational Situation: What is your organization's strategic situation?

a. Competitive Environment

(1) Competitive Position What are your relative size and growth in your industry or the markets you serve? How many and what types of competitors do you have?

(2) Competitiveness Changes What KEY changes, if any, are affecting your competitive situation?

(3) Comparative Data What KEY sources of comparative and competitive CYBERSECURITY data are available from within your industry? What KEY sources of comparative CYBERSECURITY data are available from outside your industry? What limitations, if any, affect your ability to obtain or use these data?

b. Strategic Context

What are your KEY STRATEGIC CHALLENGES and ADVANTAGES in the areas of business, operations, and CYBERSECURITY?

c. Performance Improvement System

What is your PERFORMANCE improvement system, including your PROCESSES for evaluation and improvement of KEY CYBERSECURITY-related projects and PROCESSES?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

C.2a(3). While comparative data about cybersecurity may be relatively sparse and difficult to obtain, their use is important for the following reasons: (1) Your organization needs to know where it stands relative to competitors and to best practices; (2) comparative information and information obtained from benchmarking often provide the impetus for significant improvement or transformational change; (3) comparing your organization's performance to that of others frequently leads to a better understanding of your processes and their performance; (4) data on competitors' performance may reveal organizational advantages as well as challenge areas; and (5) comparative information may support business analysis and decisions relating to core competencies, partnering, and outsourcing.

C.2c. Your performance improvement system refers to your overall approach to improving processes and projects within your organization. The approach you use should be related to your organization's needs. Some examples of approaches that are compatible with the overarching systems approach provided by this self-assessment are Lean, Six Sigma, Plan-Do-Check-Act, ISO standards, and decision science, among others.

1 Leadership

The personal actions of your senior leaders and cybersecurity leaders, as well as the characteristics of your governance system, demonstrate and reinforce accountability, and guide and sustain your cybersecurity policies and operations.

What to measure? See category 7 for organizational performance results to report. See item 7.4 for results specifically related to leadership and governance.

1.1 Leading for Cybersecurity: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?

(1) HOW do your leaders DEPLOY the organization's MISSION, VISION, and VALUES to the WORKFORCE, to KEY suppliers and PARTNERS, and to KEY CUSTOMERS and other STAKEHOLDERS, as appropriate?

(2) HOW do your leaders' actions demonstrate their commitment to CYBERSECURITY?

(3) HOW do your leaders' actions demonstrate their commitment to legal and ETHICAL BEHAVIOR?

(4) HOW do your leaders communicate with and engage other organizational leaders, the entire WORKFORCE, KEY PARTNERS, and KEY CUSTOMERS and STAKEHOLDERS regarding CYBERSECURITY?

(5) HOW do your leaders create an environment for CYBERSECURITY policies and operations that are successful now and in the future?

(6) HOW do your leaders create a focus on action that will achieve the organization's CYBERSECURITY objectives in ALIGNMENT with its MISSION?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

1.1. In this item, "leaders" include your organization's senior leaders *and* those specifically responsible for overseeing and executing cybersecurity risk management and operations. Leadership on cybersecurity policies and approaches ideally resides at multiple organizational levels. Your organization should decide whether each question refers to all senior leaders or your cybersecurity leaders.

Q1. Your organization's mission and vision should set the context for the cybersecurity-related strategic objectives and action plans you describe in items 2.1 and 2.2.

Q4. This includes encouraging frank, two-way communication about cybersecurity; communicating key decisions; and taking a direct role in motivating the workforce.

Q5. To create an environment for success now and in the future, leaders should create an environment for the achievement of the mission; create and reinforce the organization's culture; foster engagement in cybersecurity matters; cultivate organizational agility, accountability, learning, innovation, and intelligent risk taking; and participate in succession planning and the development of future organizational leaders.

Q6. Leaders should create a focus on action that will improve your organization's cybersecurity performance in the context of its mission and strategy; identify needed actions; set expectations for performance that create and balance value for customers and other stakeholders; and demonstrate personal accountability for the organization's actions.

1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and make cybersecurity-related societal contributions?

(1) HOW does your organization ensure responsible GOVERNANCE of its CYBERSECURITY policies and operations?

(2) HOW do you address current and anticipate future legal, regulatory, and community concerns with your CYBERSECURITY-related policies and operations?

(3) HOW do you promote and ensure ETHICAL BEHAVIOR in all CYBERSECURITY-related interactions?

(4) HOW do you actively support and strengthen the CYBERSECURITY infrastructure of your KEY communities?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

Q1. Responsible governance includes accountability for cybersecurity policies and operations, accountability for strategic plans, fiscal accountability, transparency, and protection of stakeholder and stockholder interests, as appropriate. In protecting stakeholder interests, the governance system should consider and sanction appropriate levels of risk for the organization, recognizing the need to accept risk as part of running a successful organization.

Q3. Some examples of measures of ethical behavior are instances of ethical conduct or compliance breaches and responses to them, survey results showing workforce perceptions of organizational ethics, ethics hotline use, and results of ethics reviews and audits.

Q4. To support and strengthen key communities, an organization might identify its key communities, determine areas for external participation in improving cybersecurity infrastructure, and contribute to the improvement of cybersecurity in those key communities by actively sharing information. This might include contributing comparative data on cybersecurity outcomes and actively sharing information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before an event occurs.

2 Strategy

Managing cybersecurity risk requires clear and robust planning and implementation, particularly when improvement alternatives and the need to respond to unanticipated needs compete for limited resources.

What to measure? Many results covered in category 7 will flow from your strategy. See item 2.2, Q5, on establishing measures for the achievement and effectiveness of your cybersecurity-related action plans. See item 7.5, Q3, for results for strategy achievement.

2.1 Strategy Development: How do you include cybersecurity considerations in your strategy development?

(1) HOW do you include CYBERSECURITY planning in your overall organizational strategic planning PROCESS?

(2) HOW do you ensure ALIGNMENT between your CYBERSECURITY planning and your organization's overall strategic planning?

(3) HOW does your strategy development PROCESS stimulate and incorporate INNOVATION in CYBERSECURITY policies and operations?

(4) HOW do you collect and analyze relevant data and develop information on CYBERSECURITY for your strategic planning PROCESS?

(5) HOW do you decide which KEY CYBERSECURITY PROCESSES will be accomplished by your WORKFORCE and which by external suppliers and PARTNERS?

(6) What are your organization's KEY CYBERSECURITY-related STRATEGIC OBJECTIVES and timetable for achieving them?

(7) How do your organization's KEY CYBERSECURITY-related STRATEGIC OBJECTIVES align with your organization's overall STRATEGIC OBJECTIVES?

(8) HOW do your STRATEGIC OBJECTIVES achieve appropriate balance among varying and potentially competing CYBERSECURITY needs, CUSTOMER and STAKEHOLDER requirements, and business objectives?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

2.1. Strategy development refers to your organization's approach to preparing for the future. This item asks how your strategic planning considers your organization's cybersecurity needs in alignment with your organization's overall strategy.

2.1. In developing your cybersecurity strategy, you should consider your level of acceptable enterprise risk. As appropriate, you might involve key suppliers, distributors, partners, and customers in your cybersecurity strategy development.

Q3. Stimulating and incorporating innovation includes identifying strategic opportunities (prospects for new or changed cybersecurity policies, procedures, technologies, and processes) and deciding which ones are intelligent risks to pursue. Innovation refers to making meaningful change to improve products/services, processes, or organizational effectiveness and create new value for stakeholders. The outcome of innovation is a discontinuous or "breakthrough" change.

Q4. Your collection and analysis should include these key elements of risk: your strategic challenges and strategic advantages with regard to cybersecurity, potential relevant changes in your regulatory and external business environment, potential blind spots with regard to cybersecurity, and your ability to execute the cybersecurity-related parts of the plan. Analysis of these factors is the basis for managing strategic cybersecurity-related risk in your organization.

Q5. Decisions on which key cybersecurity processes will be accomplished by your workforce and which externally should consider your core competencies and those of potential suppliers and partners. These decisions are strategic and involve protecting intellectual property, capitalizing on core competencies, and mitigating risk.

2.2 Strategy Implementation: How do you implement the cybersecurity-related elements of your strategy?

(1) What are your KEY short- and longer-term CYBERSECURITY-related ACTION PLANS?

(2) HOW do you DEPLOY your CYBERSECURITY-related ACTION PLANS?

(3) HOW do you ensure that financial and other resources are available to support the achievement of your CYBERSECURITY-related ACTION PLANS while you meet current obligations?

(4) What are your KEY WORKFORCE plans to support your short- and longer-term CYBERSECURITY-related STRATEGIC OBJECTIVES and ACTION PLANS?

(5) What KEY PERFORMANCE MEASURES or INDICATORS do you use to track the achievement and EFFECTIVENESS of your CYBERSECURITY-related ACTION PLANS?

(6) For these KEY PERFORMANCE MEASURES or INDICATORS, what are your PERFORMANCE PROJECTIONS for your short- and longer-term planning horizons?

(7) HOW do you recognize and respond when circumstances require a shift in CYBERSECURITY-related plans and rapid execution of new plans?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

2.2. The development and deployment of your cybersecurity strategy (described in item 2.1) and action plans are closely linked to other items. The following are examples of key linkages:

- Item 1.1: how your leaders communicate organizational direction with regard to cybersecurity
- Category 3: how you gather internal and external customer knowledge as input to your strategy and action plans and to use in deploying action plans
- Category 4: how you measure and analyze cybersecurity data and manage cybersecurity knowledge to support key information needs, support the development of your strategy, provide an effective basis for cybersecurity performance measurements, and track progress on achieving cybersecurity-related strategic objectives and action plans
- Category 5: how you meet cybersecurity workforce capability and capacity needs; determine cybersecurity-related development and learning needs, and design your workforce development and learning system accordingly; and implement workforce-related changes resulting from action plans
- Category 6: how you address changes to your cybersecurity work processes resulting from action plans
- Item 7.5: specific accomplishments on the cybersecurity-related elements of your strategy and action plans

3 Customers

Cybersecurity risk can harm your ability to gain and retain customers, who are the ultimate judges of the quality of your organization's products and services. Thus, your organization must consider all cybersecurity-related policies, operations, and modes of access and support that contribute value to your customers.

What to measure? See item 7.2, Customer Results.

3.1 Customer Expectations: How do you listen to your customers and determine their cybersecurity-related satisfaction?

(1) HOW do you listen to, interact with, and observe internal and external CUSTOMERS to obtain actionable information on their CYBERSECURITY-related requirements and expectations?

(2) HOW do you determine internal and external CUSTOMERS' satisfaction and dissatisfaction with your organization's CYBERSECURITY policies and operations?

(3) HOW do you determine the impact of your organization's CYBERSECURITY policies and operations on CUSTOMER ENGAGEMENT?

(4) HOW do you use VOICE-OF-THE-CUSTOMER data and information to support fact-based decision making on CYBERSECURITY policies and operations?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

3.1. In gathering customer expectations, you might gather and integrate various types of customer data, such as survey data, focus group findings, data from social media, and complaint data.

Q2. You might use any or all of the following to determine customer satisfaction and dissatisfaction: surveys, formal and informal feedback, customer account histories, complaints, customer referral rates, and transaction completion rates.

Q3. Customer engagement is your customers' investment in or commitment to your brand and product/service offerings. It is based on your ongoing ability to serve their needs and build relationships so that they will continue using your products. Characteristics of engaged customers include retention, brand loyalty, willingness to make an effort to do business—and increase their business—with you, and willingness to actively advocate for and recommend your brand and product/service offerings.

3.2 Customer Engagement: How do you build relationships with internal and external customers around cybersecurity?

(1) HOW do you build and manage internal and external CUSTOMER relationships to retain CUSTOMERS, meet their requirements, and exceed their expectations with regard to CYBERSECURITY?

(2) HOW do you enable internal and external CUSTOMERS to seek information and support related to your CYBERSECURITY policies and operations?

(3) HOW do you ensure that internal and external CUSTOMERS understand and fulfill their CYBERSECURITY roles and responsibilities?

(4) HOW do you manage internal and external CUSTOMER complaints about your CYBERSECURITY policies and operations?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Note

Q2. Your approach to enabling customers to seek information and support should include provisions to protect privacy and civil liberties when personal information is used, collected, processed, maintained, or disclosed in connection with your organization's cybersecurity activities. Some examples of activities with privacy or civil liberties considerations include cybersecurity activities that may result in the overcollection or overretention of personal information; disclosure or use of personal information unrelated to cybersecurity activities; and cybersecurity mitigation activities that result in denial of service or other similar potentially adverse impacts, including incident detection or monitoring that may impact freedom of expression or association.

Privacy principles to consider incorporating in cybersecurity policies and operations include establishing and maintaining a privacy program that ensures compliance with applicable requirements, coordination between privacy and other organizational programs, and integration of privacy policy regarding what privacy-related data may be used by whom and for what purposes (see *Security and Privacy Controls for Information Systems and Organizations*, SP 800-53 Rev. 5 (Draft), https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft).

4 Measurement, Analysis, and Knowledge Management

This category is the "brain center" for aligning your cybersecurity operations with your objectives. Measuring and analyzing how your organization is performing on a comprehensive yet carefully culled set of cybersecurity-related measures helps you make decisions that improve performance.

What to measure? Q2 and Q3 ask for your *key* cybersecurity performance measures, including your key financial measures. See the notes to Q2 and Q3 for an explanation.

4.1 Measurement, Analysis, and Improvement of Performance: How do you measure, analyze, and then improve cybersecurity-related performance?

(1) HOW do you track data and information on daily CYBERSECURITY operations and overall CYBERSECURITY PERFORMANCE?

(2) What are your KEY CYBERSECURITY PERFORMANCE MEASURES, including your KEY financial MEASURES for your CYBERSECURITY operations?

(3) What are your KEY MEASURES for the impact of CYBERSECURITY PERFORMANCE on your organization's overall KEY PERFORMANCE MEASURES?

(4) HOW do you select comparative data and information to support fact-based decision making on CYBERSECURITY policies and operations?

(5) HOW do you ensure that your measurement of CYBERSECURITY PERFORMANCE can respond to rapid or unexpected organizational or external changes and provide timely data?

(6) HOW do you review your organization's CYBERSECURITY PERFORMANCE and capabilities?

(7) HOW do you project your organization's future CYBERSECURITY PERFORMANCE?

(8) HOW do you use findings from PERFORMANCE reviews to develop priorities for continuous improvement and opportunities for INNOVATION in your CYBERSECURITY policies and operations?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

4.1. This item asks how you measure and analyze cybersecurity-related performance as part of your organization's overall performance measurement and analysis system. The questions are closely linked to each other and to other items:

- Your measurement of cybersecurity performance (Q1–Q5) should inform your reviews (Q6).
- Your key cybersecurity performance measures are those that are critical to achieving your cybersecurity-related strategic objectives (item 2.1, Q6).
- Your performance reviews (Q6) should reflect your cybersecurity-related strategic objectives and action plans (category 2), and the results of cybersecurity performance analysis and review should inform your strategy development and implementation, your priorities for improvement, and your opportunities for innovation (Q7, Q8).
- Your performance results should be reported in items 7.1–7.5.

Q2. Depending on your organization's strategy and goals, these might include measures of customer and process performance; operational performance; supplier, workforce, partner, cost, and financial performance; and governance and compliance results.

Q2, Q3. Key financial measures might include measures of performance to budget. Measures for the impact of cybersecurity performance on your organization's overall performance might include the financial impact of cybersecurity operations and incidents on organization-wide operations, as well as on your ability to meet customer and stakeholder requirements and business objectives. See the notes to item 7.5 for examples.

Q4. Organizations obtain comparative data and information by benchmarking and by seeking competitive comparisons. *Benchmarking* is identifying processes and results that represent best practices and performance for similar activities, inside or outside your industry. *Competitive comparisons* relate your performance to that of competitors and other organizations providing similar products and services.

4.2 Knowledge Management: How do you manage your organization's cybersecurity-related knowledge assets?

(1) HOW do you verify and ensure the quality of organizational data and information related to CYBERSECURITY?

(2) How do you ensure the availability of organizational data and information related to CYBERSECURITY?

(3) HOW do you build, manage, and update your organization's CYBERSECURITY-related knowledge and awareness?

(4) HOW do you share CYBERSECURITY best practices in your organization and with CUSTOMERS, suppliers, PARTNERS, and COLLABORATORS, as appropriate?

(5) HOW do you use your knowledge and resources to embed LEARNING in the way your CYBERSECURITY operations function?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

Q3. Building, managing, and updating cybersecurity-related knowledge allows you to maintain your organization's awareness of a continually changing cybersecurity threat environment. It involves collecting and transferring workforce knowledge related to cybersecurity; blending and correlating cybersecurity-related data from different sources to build new knowledge; transferring relevant cybersecurity-related knowledge from and to customers, suppliers, partners, and collaborators; and assembling and transferring relevant cybersecurity-related knowledge for use in innovation and strategic planning processes.

Sources for building and updating your organization's cybersecurity-related knowledge and awareness may include, for example, cybersecurity information learned from other organizations, service tickets reported to the help desk, lessons learned from recovery exercises, and data reported by customers. An important element of cybersecurity risk management includes the ability to predict and avoid cybersecurity incidents based on lessons learned and/or information shared by partners and others.

Q5. Embedding learning in the way your cybersecurity operations function means that learning (1) is a part of everyday cybersecurity work; (2) results in solving problems at their source; (3) is focused on building and sharing cybersecurity knowledge throughout your organization; and (4) is driven by opportunities to bring about significant, meaningful change and to innovate with regard to cybersecurity. Organizational learning takes place when processes intentionally include mechanisms that monitor performance and conformance, identify improvement targets, analyze gaps, and prioritize improvements.

5 Workforce

Success in achieving your cybersecurity-related objectives depends on an engaged workforce—including workforce members involved directly in cybersecurity-related operations and members of your overall workforce. Workforce members benefit from meaningful work, clear organizational direction, the opportunity to learn, and accountability for performance.

What to measure? See item 7.3, Workforce Results.

5.1 Workforce Environment: How do you build an effective and supportive environment for your cybersecurity workforce?

(1) HOW do you assess your CYBERSECURITY WORKFORCE CAPABILITY and CAPACITY needs?

(2) HOW do you recruit, hire, onboard, and retain new CYBERSECURITY WORKFORCE members?

(3) HOW do you prepare your CYBERSECURITY WORKFORCE for changing CAPABILITY and CAPACITY needs?

(4) HOW do you organize and manage your CYBERSECURITY WORKFORCE to establish roles and responsibilities?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

5.1. The questions in this item refer to your cybersecurity workforce. See item 5.2 for questions on your entire workforce.

5.1. Your cybersecurity workforce consists of the people actively involved in accomplishing your organization's cybersecurity work. It includes permanent, temporary, and part-time personnel, as well as any contract employees you supervise. It includes team leaders, supervisors, and managers at all levels. Suppliers and people supervised by a contractor should be addressed in categories 2 and 6.

Q1. Cybersecurity workforce capability is your organization's ability to carry out its cybersecurity work processes through its people's knowledge, skills, abilities, and competencies. Cybersecurity workforce capacity is your organization's ability to ensure sufficient staffing levels to carry out its cybersecurity work processes, including the ability to meet seasonal or varying demand levels. In assessing your capability and capacity needs, you should consider not only current needs but also future requirements based on the strategic objectives and action plans you identify in category 2.

Q3. Preparing your cybersecurity workforce for changing capability and capacity needs involves ensuring continuity, preventing workforce reductions, and minimizing the impact of any reductions that occur. It also involves preparing for and managing any periods of workforce growth, as well as preparing your workforce for changes in organizational structure and work systems, as needed.

5.2 Workforce Engagement: How do you engage your workforce for high performance in support of cybersecurity policies and operations?

(1) HOW do you assess the ENGAGEMENT of your organization's overall WORKFORCE in CYBERSECURITY matters?

(2) HOW do you foster an organizational culture that is characterized by open communication, HIGH PERFORMANCE, and ENGAGEMENT in CYBERSECURITY matters?

(3) HOW does your WORKFORCE PERFORMANCE management system support HIGH PERFORMANCE in fulfilling CYBERSECURITY roles and responsibilities?

(4) HOW does your CYBERSECURITY LEARNING and development system support your organization's needs, and support WORKFORCE members in fulfilling their CYBERSECURITY roles and responsibilities?

(5) HOW do you evaluate the EFFECTIVENESS and efficiency of your CYBERSECURITY LEARNING and development system?

(6) HOW do you carry out succession planning for KEY CYBERSECURITY management, leadership, and other KEY positions?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

5.2. The questions in this item refer to your organization's entire workforce.

Q1. Drivers of workforce engagement (identified in C.1a[3]) refer to the drivers of workforce members' commitment, both emotional and intellectual, to accomplishing the organization's work (including cybersecurity-related work), mission, and vision.

Q2. Fostering such a culture includes empowering your workforce and ensuring a safe, trusting, and cooperative environment.

Q3. Your workforce performance management system should consider compensation, reward, recognition, and retention practices. It should reinforce intelligent risk taking, a customer and business focus, and achievement of your action plans.

Q4. Learning and development needs include the knowledge, skills, and abilities workforce members need to fulfill their cybersecurity roles and responsibilities. Organizations benefit when an understanding of these needs becomes part of the organizational culture, evolving from lessons learned from previous security activities, information shared by other sources, and continuous awareness of activities on their systems and networks.

6 Operations

Designing, managing, and improving your cybersecurity-related operations for effectiveness and efficiency helps you achieve your cybersecurity-related objectives, in turn supporting your organization's overall goals and objectives.

What to measure? See item 7.1, Cybersecurity Process Results.

6.1 Work Processes: How do you design, manage, and improve your key cybersecurity work processes?

a. CYBERSECURITY PROCESS Design, Management, and Improvement

(1) HOW do you determine the requirements for your KEY CYBERSECURITY WORK PROCESSES (listed in sections b–d)?

(2) HOW do you design your CYBERSECURITY WORK PROCESSES to meet requirements?

(3) HOW does your day-to-day operation of CYBERSECURITY WORK PROCESSES ensure that they meet KEY PROCESS requirements?

(4) HOW do you determine the KEY support PROCESSES that enable your CYBERSECURITY operations?

(5) HOW do you improve your CYBERSECURITY WORK PROCESSES to improve their PERFORMANCE and reduce variability?

(6) HOW do you pursue opportunities for INNOVATION in your CYBERSECURITY operations?

b. PROTECTION

(1) HOW do you limit access to physical and logical assets and associated facilities to authorized users, PROCESSES, and devices consistent with the risk of unauthorized access?

(2) HOW do you manage information and records (data) consistent with your risk strategy to PROTECT the confidentiality, integrity, and availability of information?

(3) HOW do you maintain and use security policies (addressing purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), PROCESSES, and procedures to manage PROTECTION of information systems and assets?

(4) HOW do you maintain and repair industrial control and information system components consistent with policies and procedures?

(5) HOW do you manage technical security solutions to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements?

c. DETECTION

(1) HOW do you DETECT anomalies in a timely manner and assess the potential impact of CYBERSECURITY EVENTS?

(2) HOW do you monitor information systems and assets to identify CYBERSECURITY EVENTS and verify the effectiveness of protective measures?

(3) HOW do you maintain and test DETECTION PROCESSES and procedures to ensure awareness of anomalies?

d. RESPONSE

(1) HOW do you execute and maintain RESPONSE PROCESSES and procedures to ensure RESPONSE to detected CYBERSECURITY EVENTS?

(2) HOW do you coordinate RESPONSE activities with other WORKFORCE units, CUSTOMERS, and STAKEHOLDERS, as appropriate, including external law enforcement agencies?

(3) HOW do you analyze your RESPONSE activities to ensure EFFECTIVE RESPONSE and support RECOVERY activities?

(4) HOW do you prevent expansion of an event, mitigate its effects, and resolve the incident?

(Continued on the next page)

e. RECOVERY

(1) HOW do you execute and maintain RECOVERY PROCESSES and procedures to ensure restoration of systems or assets affected by CYBERSECURITY incidents?

(2) HOW do you coordinate RECOVERY activities with other WORKFORCE units, CUSTOMERS, and STAKEHOLDERS, such as coordinating centers, Internet service providers, owners of attacking systems, victims, other computer security incident RESPONSE teams, and vendors?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

6.1a(1), 6.1a(2). The design of your key cybersecurity work processes should consider your customers' and stakeholders' requirements and expectations of your organization.

6.1a(3). To ensure that the operation of cybersecurity work processes meets requirements, an organization would establish key performance measures or in-process measures, monitor them, and use the results (see item 7.1) to control and improve the processes.

6.1a(4). Support processes might include, for example, physical security, human resources, and procurement.

6.1a(5). To improve process performance and reduce variability, you might implement approaches such as a Lean Enterprise System, Six Sigma methodology, ISO quality system standards, PDCA methodology, decision sciences, or other process improvement tools. These approaches might be part of the performance improvement system you describe in C.2c in the Organizational Context section.

6.1b–6.1e. The *Cybersecurity Framework* Core includes the functions of Identify, Protect, Detect, Respond, and Recover (identified as key work processes in this item). These functions organize basic cybersecurity activities at their highest level. The Core identifies underlying key categories and subcategories for each function, and matches them with examples of informative references, such as existing standards, guidelines, and practices. Protect, Detect, Respond, and Recover are covered in this item. The Identify function is covered by questions in the Organizational Context and in categories 1, 2, 3, and 5.

6.1b–6.1e. Your responses should include aspects of your work processes that involve external suppliers and partners, such as third-party connections into your organization's networks and systems.

6.2 Operational Effectiveness: How do you ensure effective management of your cybersecurity operations?

a. PROCESS Efficiency and Effectiveness

(1) HOW do you manage the cost and efficiency of your CYBERSECURITY operations?

(2) HOW do you ensure that your CYBERSECURITY operations consider their impact on and align with your organization's overall operations?

b. Supply-Network Management

(1) HOW do you select and prioritize suppliers that are qualified and positioned to meet your CYBERSECURITY needs and achieve your CYBERSECURITY objectives?

(2) HOW do you promote ALIGNMENT and collaboration on CYBERSECURITY within your supply network?

(3) How do you ensure supply-network agility in responding to changes in CUSTOMER, market, and organizational CYBERSECURITY requirements?

(4) HOW do you communicate CYBERSECURITY PERFORMANCE expectations, measure and evaluate suppliers' PERFORMANCE, provide feedback to help them improve, and deal with poorly performing suppliers?

c. Safety and Emergency Management

(1) HOW do you ensure that your CYBERSECURITY operations consider and align with your organization's overall operational safety system?

(2) HOW do you ensure that your organization incorporates CYBERSECURITY-related considerations and operations in its preparation for disasters or emergencies?

(3) In the event of an emergency, HOW do you ensure that systems and assets continue to be secure and available to serve CUSTOMERS and business needs?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

6.2a. Managing efficiency includes

- incorporating cycle time, productivity, and other efficiency and effectiveness factors into your work processes;
- preventing rework; and
- balancing the need for cost control and efficiency with the cybersecurity needs of your organization and customers.

6.2b. Your supply network (see also C.1b[3] in the Organizational Context section) consists of the entities involved in producing your products and services (including your cybersecurity operations) and delivering them to your customers. Increasingly, these entities are interlinked and exist in interdependent rather than linear relationships. The term supply network, rather than supply chain, emphasizes the interdependencies among organizations and their suppliers.

6.2b(4). Your monitoring of supplier effectiveness should relate to achievement of the key requirements described in 6.1, including methods for periodically reviewing supplier performance to confirm that they are performing cybersecurity responsibilities assigned to them and contributing to the achievement of cybersecurity-related objectives.

6.2c. Your preparation for disasters and emergencies should consider all systems and assets that are needed to provide your products and services to customers, including supply-network availability. It should also consider the extent to which your organization is part of customers' critical infrastructure.

7 Results

Results provide data and information (measures of progress) for evaluating, improving, and innovating cybersecurity-related processes, policies, and operations in alignment with your cybersecurity and organizational strategy.

7.1 Cybersecurity Process Results: What are your cybersecurity performance and process effectiveness results?

(1) What are your RESULTS for the PROTECTION of your systems and assets?

(2) What are your RESULTS for the DETECTION of CYBERSECURITY EVENTS?

(3) What are your RESULTS for your RESPONSE to CYBERSECURITY EVENTS?

(4) What are your RESULTS for your RECOVERY from CYBERSECURITY EVENTS?

(5) What are your PROCESS EFFECTIVENESS and efficiency RESULTS for your CYBERSECURITY operations?

(6) What are your emergency preparedness RESULTS for your CYBERSECURITY operations?

(7) What are your RESULTS for suppliers' and PARTNERS' understanding and fulfillment of their CYBERSECURITY roles and responsibilities?

(8) What are your RESULTS for management of your CYBERSECURITY supply network?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

7. The results you report in items 7.1–7.5 should provide key information for analyzing and reviewing your cybersecurity-related performance (item 4.1), demonstrate use of cybersecurity knowledge (item 4.2), and provide the operational basis for customer-focused results (item 7.2) and financial results (item 7.5). There is not a one-to-one correspondence between results items and categories 1–6. Results should be considered systemically. Contributions to individual results items frequently stem from processes in more than one category.

Q1–Q8. The results you report here should address the key operational requirements you identify in the Organizational Context section and in category 6.

Q1. Results for the protection of systems and assets should relate to the protection processes you describe in category 6. These results might include, for example, the percentage of devices and/or software accurately recorded in inventory, the percentage of devices configured according to policy, the percentage of critical information servers supported by strong authentication, the number of business systems securely hosted in an approved cloud environment, and the number of facilities with Personal Identity Verification (PIV)-based electronic locks.

Q2. Results for the detection of cybersecurity events should relate to the detection processes you report in category 6. These results might include, for example, the number of anomalies detected, investigated, and resolved, and the percentage of planned vulnerability mitigation actions effectively completed.

Q3. Results for your response to cybersecurity events should relate to the response processes you report in category 6. These results might include, for example, incident recovery and response time, number of disaster recovery incidents, and number of reports shared with Information Sharing and Analysis Organizations or other appropriate third parties.

Q4. Results for your recovery from cybersecurity events should relate to the recovery processes you report in category 6. These results might include, for example, the time to restore lost availability, the time to access alternate availability mechanisms and restore services, and results of efforts to restore your organization's reputation.

Q5. Process effectiveness and efficiency results for your cybersecurity operations might include ensuring that security and other requirements are considered at the design phase, avoiding costly mitigation through prevention of vulnerabilities, and reduction of incidents based on effective training of expectations and responsibilities.

Q6. Emergency preparedness results might include the cybersecurity operation's response times for emergency drills or exercises and results for work relocation or contingency exercises.

Q8. Results for cybersecurity supply-network performance might include the percentage of contracts that include cybersecurity monitoring and reporting requirements; supplier and partner audits; and acceptance results for externally provided services and processes, as well as improvements in downstream supplier services to customers.

7.2 Customer Results: What are your customer-focused cybersecurity performance results?

(1) What are your RESULTS for your internal and external CUSTOMERS' satisfaction and dissatisfaction with your CYBERSECURITY policies and operations?

(2) What are your RESULTS for the impact of your organization's CYBERSECURITY policies and operations on CUSTOMER ENGAGEMENT?

(3) What are your RESULTS for your internal and external CUSTOMERS' understanding and fulfillment of their CYBERSECURITY roles and responsibilities?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

7.2. Results for customer satisfaction, dissatisfaction, and engagement should relate to the customer groups you identify in C.1b(2) and to the listening and determination methods you report in item 3.1.

Q1. Results might include, for example, survey results on customer satisfaction and dissatisfaction with cybersecurity and privacy, and the number of complaints about cybersecurity-related issues.

Q2. Results might include, for example, those for the impact of cybersecurity policies and procedures, incidents, and responses to incidents on customer loyalty, retention, and willingness to recommend.

Q3. Results might include, for example, the number of potential incidents reported by external customers, the requirements for service-level agreements regarding recovery of critical customer systems, the percentage of customers who have changed their passwords regularly or within a specified time period, and the number of customer systems applying multifactor (strengthened) authentication.

7.3 Workforce Results: What are your workforce-focused cybersecurity performance results?

(1) What are your CAPABILITY and CAPACITY RESULTS for your CYBERSECURITY WORKFORCE?

(2) What are your RESULTS for the ENGAGEMENT of your WORKFORCE in CYBERSECURITY matters?

(3) What are your RESULTS for WORKFORCE members' fulfillment of their CYBERSECURITY roles and responsibilities?

(4) What are your WORKFORCE and leader development RESULTS related to CYBERSECURITY?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

7.3. Results reported in this item should relate to the processes you report in category 5. Your results should also respond to the key work process needs you report in category 6 and to the action plans you report in item 2.2.

Q1. Results might include, for example, the number of qualified referrals received through employee recommendations, the percentage of cybersecurity vacancies remaining open for a specified number of days, and the percentage of staff members who have achieved necessary qualifications (e.g., Certified Information Security Manager [CISM], Certified Information Systems Security Professional [CISSP]).

Q2. Results should relate to the workforce engagement drivers you describe in C.1a(3) and the methods of assessing engagement you describe in item 5.2.

Q3. Results might include the percentage of employees who follow specific cybersecurity policies and practices, such as those who observe your organization's password practices.

Q4. Results might include, for example, the percentage of employees who complete role-specific cybersecurity training, cybersecurity management training hours per full-time equivalent, the percentage of employees trained on incident handing, the percentage of employees trained to recognize and avoid email scams, the percentage of employees trained on how to secure an email browser, and the number of employees trained on use of guidelines for cell phone and personal device security.

7.4 Leadership and Governance Results: What are your cybersecurity leadership and governance results?

(1) What are your RESULTS for leaders' communication and engagement with your organization's other leaders, your WORKFORCE, and your KEY CUSTOMERS and STAKEHOLDERS regarding CYBERSECURITY?

(2) What are your RESULTS for GOVERNANCE accountability related to CYBERSECURITY?

(3) What are your legal and regulatory RESULTS related to CYBERSECURITY?

(4) What are your RESULTS for ETHICAL BEHAVIOR related to CYBERSECURITY?

(5) What are your RESULTS for support of the CYBERSECURITY infrastructure of your KEY communities?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

Q1. Responses should include results relating to the communication processes you identify in item 1.1.

Q2. Responses should include results relating to the governance processes you describe in item 1.2. These results might include financial statement issues and risks, important internal and external auditor recommendations, and management's responses to these matters.

Q3. Legal and regulatory results should relate to the processes and measures you describe in item 1.2. Examples might be the percentage of business systems in compliance with legal and regulatory requirements, the number of compliance breaches, and the frequency of warnings/violation notices for cybersecurity infractions.

Q4. Responses should relate to the processes for ensuring ethical behavior that you identify in item 1.2.

Q5. Results for support of the cybersecurity infrastructure of your key communities might include the extent of external participation and collaboration to improve cybersecurity and results showing its effectiveness (e.g., improved detection using shared indicators of compromise).

7.5 Financial and Strategy Results: What are your cybersecurity-related financial and strategy performance results?

(1) What are your financial and budgetary PERFORMANCE RESULTS for your CYBERSECURITY operations?

(2) What are your RESULTS for the impact of CYBERSECURITY costs on your organization's overall financial PERFORMANCE?

(3) What are your RESULTS for the achievement of your CYBERSECURITY strategy and ACTION PLANS?

Terms in SMALL CAPS are defined in the Glossary of Key Terms (pages 28–29).

Notes

7.5. Results should relate to the financial measures you report in item 4.1 and the financial management approaches you report in item 2.2.

Q1. Examples might include cybersecurity spending as a percentage of the IT budget, cost performance to budget, and lowering of costs as a result of increased efficiency.

Q2. Examples might include cost savings or losses avoided (e.g., fines for nonconformance) produced by the information security program or through costs incurred from addressing information security events, cost/schedule variance in information security activities, and the impact of the cost of cybersecurity breaches on your organization's other financial results.

Q3. Results for strategy and action plan achievement should relate to the strategic objectives and goals you report in item 2.1 and the action plan performance measures you report in item 2.2.

Assessing Your Responses

1. **For each item (e.g., 1.1, 1.2) in categories 1–7 of the *Baldrige Cybersecurity Excellence Builder*, use the process and results rubrics on pages 26–27 to assign a descriptor (Reactive, Early, Developing, Mature, Leading, or Exemplary) for each evaluation factor.**

   For processes (categories 1–6), the evaluation factors are approach, deployment, learning, and integration (ADLI):

   - *Approach* consists of the methods used to carry out a process, the degree to which your approach is systematic (i.e., repeatable and based on reliable data and information), the appropriateness of these methods to the item questions and your operating environment, and the effectiveness of your use of the methods.
   - *Deployment* is the extent to which your approach is applied consistently and the extent to which it is used by all appropriate work units.
   - *Learning* is the refinement of your approach through cycles of evaluation and improvement, the encouragement of breakthrough change to your approach through innovation, and the sharing of refinements and innovations with other relevant work units and processes in your organization.
   - *Integration* is the extent to which your approach is aligned with the organizational needs identified in the Organizational Context section and in other process items. Integration also includes the extent to which your measures, information, and improvement systems are complementary across processes and work units; and the extent to which your plans, processes, results, analyses, learning, and actions are harmonized across processes and work units to support organization-wide goals.

   For results (category 7), the evaluation factors are levels, trends, comparisons, and integration (LeTCI; "let's see").

   - *Levels* are your current performance on a meaningful measurement scale.
   - *Trends* are your rate of performance improvement or continuation of good performance in areas of importance (i.e., the slope of data points over time).
   - *Comparisons* are your performance relative to that of other, appropriate organizations, such as competitors or organizations similar to yours, and your performance relative to industry leaders or relevant benchmarks.
   - *Integration* is the extent to which your results address important performance requirements relating to customers, products/services, markets, processes, and action plans identified in the Organizational Context section and in the process items (categories 1–6). It also includes the extent to which your results reflect harmonization across your processes and work units to support organization-wide goals.

2. **Indicate the importance (high, medium, or low) of each item to the successful management of cybersecurity within your organization.**

3. **Prioritize your actions.**

   Celebrate your strengths of your cybersecurity risk management program, and build on them to improve what you do well. Sharing the things you do well with the rest of your organization can speed improvement.

   Prioritize your opportunities for improvement; you cannot do everything at once. Think about what is most important for your organization as a whole at this time, balancing the differing needs and expectations of your stakeholders, and decide what to work on first. Look at the next level in the rubric for how you might improve. Develop an action plan, implement it, and measure your progress.

Assessment Rubric

Process (Categories 1–6)

Maturity Level	Evaluation Factor			
	Approach	Deployment	Learning	Integration
Reactive	CYBERSECURITY-related policies/operations are characterized by activities created to fix problems rather than by PROCESSES.	CYBERSECURITY-related APPROACHES are not used consistently in appropriate organizational units or by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Improvement in CYBERSECURITY-related policies/operations is achieved mainly in reaction to immediate needs or problems.	There is no coordination among CYBERSECURITY-related policies/operations in different parts of your organization or between CYBERSECURITY-related policies/operations and those of the rest of the organization; individual areas or work units operate independently.
Early	CYBERSECURITY-related policies/operations are beginning to be carried out with well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are beginning to be used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	CYBERSECURITY-related policies/operations are in the early stages of a transition from reacting to problems to a general improvement orientation.	CYBERSECURITY-related APPROACHES are ALIGNED with other areas or work units, and with organization-wide APPROACHES, largely through joint problem solving.
Developing	Some elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate, although some are in the early stages of use.	CYBERSECURITY-related policies/operations are beginning to be SYSTEMATICALLY evaluated and improved.	CYBERSECURITY-related APPROACHES are beginning to be ALIGNED among work units and with your organization's basic needs.
Mature	Many elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate, although use may vary in some areas or work units.	CYBERSECURITY-related policies/operations are SYSTEMATICALLY evaluated for improvement, and learnings are shared, with some INNOVATION.	CYBERSECURITY-related APPROACHES are ALIGNED among work units and with your organization's overall needs.
Leading	Most elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in most appropriate organizational units by CUSTOMERS, PARTNERS, and suppliers, as appropriate, with no significant gaps.	CYBERSECURITY-related policies/operations seek and achieve efficiencies through analysis, INNOVATION, and the sharing of information and knowledge.	CYBERSECURITY-related policies/operations in different units work mainly in harmony with each other and with current and future organizational needs defined by your organization.
Exemplary	All elements of CYBERSECURITY-related policies/operations are characterized by EFFECTIVE, well-ordered, repeatable APPROACHES.	KEY CYBERSECURITY-related APPROACHES are used consistently in all appropriate organizational units and by CUSTOMERS, PARTNERS, and suppliers, as appropriate.	Fact-based, SYSTEMATIC evaluation and improvement and organizational LEARNING through INNOVATION are KEY tools; CYBERSECURITY-related policies/operations are characterized by refinement and INNOVATION, backed by ANALYSIS and sharing.	CYBERSECURITY-related policies/operations in different units work in total harmony with each other and with current and future organizational needs defined by your organization.

Results (Category 7)

Maturity Level	Evaluation Factor			
	Levels	**Trends**	**Comparisons**	**Integration**
Reactive	CYBERSECURITY-related RESULTS are frequently missing, poor, or not used.	CYBERSECURITY-related RESULTS are not tracked over time or have not improved.	Available comparative information is not tracked.	CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are not tracked.
Early	A few CYBERSECURITY-related RESULTS are tracked, and they show early good performance LEVELS.	Some TREND data are tracked, and some show improvement over time.	Little or no available comparative information is tracked.	A few CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are tracked.
Developing	Some CYBERSECURITY-related RESULTS are tracked, and they show good performance LEVELS.	Some TREND data are tracked, and most show improvement over time.	Some available comparative information is tracked.	Many CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are tracked.
Mature	Many CYBERSECURITY-related RESULTS are tracked, and they show good PERFORMANCE LEVELS.	CYBERSECURITY-related RESULTS show improvement or sustained high PERFORMANCE over time in some areas of importance to your organization's ongoing success.	Some CYBERSECURITY-related RESULTS show good PERFORMANCE relative to available information on competitors, other relevant organizations, or BENCHMARKS.	Many CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are tracked. RESULTS are beginning to be used in decision making.
Leading	Most CYBERSECURITY-related RESULTS are tracked, and they show good-to-excellent performance LEVELS.	Most CYBERSECURITY-related RESULTS show improvement or sustained high PERFORMANCE over time in most areas of importance to your organization's ongoing success.	Many CYBERSECURITY-related RESULTS show good PERFORMANCE relative to available information on competitors, other relevant organizations, or BENCHMARKS.	Most CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are tracked. The RESULTS are used in decision making.
Exemplary	The full array of CYBERSECURITY-related RESULTS is tracked, indicating top PERFORMANCE.	The full array of CYBERSECURITY-related RESULTS is TRENDED over time, indicating improvement or sustained high PERFORMANCE in all areas of importance to your organization's ongoing success.	CYBERSECURITY-related RESULTS indicate top PERFORMANCE relative to information on other organizations or BENCHMARKS.	Most CYBERSECURITY-related RESULTS that are important to your organization's ongoing success are tracked, including PROJECTIONS of future RESULTS. The RESULTS are used in decision making.

Glossary of Key Terms

The terms below are those in SMALL CAPS *in the* Baldrige Cybersecurity Excellence Builder *categories and assessment rubric.*

ACTION PLANS. Specific actions that your organization takes to reach its strategic objectives. These plans specify the resources committed to and the time horizons for accomplishing the plans. See also STRATEGIC OBJECTIVES.

ALIGNMENT. A state of consistency among plans, processes, information, resource decisions, workforce capability and capacity, actions, results, and analyses that support key organization-wide goals. See also INTEGRATION.

APPROACH. The methods your organization uses to carry out its processes.

BENCHMARKS. Processes and results that represent the best practices and best performance for similar activities, inside or outside your organization's industry.

COLLABORATORS. Organizations or individuals who cooperate with your organization to support a particular activity or event or who cooperate intermittently when their short-term goals are aligned with or are the same as yours. See also PARTNERS.

CORE COMPETENCIES. Your organization's areas of greatest expertise; those strategically important capabilities that are central to fulfilling your mission or that provide an advantage in your marketplace or service environment.

CUSTOMER. An actual or potential user of your organization's products, programs, or services. See also STAKEHOLDERS.

CUSTOMER ENGAGEMENT. Your customers' investment in or commitment to your brand and product offerings.

CYBERSECURITY. The process of protecting information and assets by preventing, detecting, and responding to attacks.

CYBERSECURITY EVENT. A cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). A cybersecurity incident is an event that has been determined to have such an effect, prompting the need for response and recovery.

DEPLOYMENT. The extent to which your organization applies an approach in relevant work units throughout your organization.

DETECT. Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. Detect is one of the five functions included in the *Cybersecurity Framework* Core. The others are Identify, Protect, Respond, and Recover.

EFFECTIVE. How well a process or a measure addresses its intended purpose.

ETHICAL BEHAVIOR. The actions your organization takes to ensure that all its decisions, actions, and stakeholder interactions conform to its moral and professional principles of conduct. These principles should support all applicable laws and regulations and are the foundation for your organization's culture and values.

GOALS. Future conditions or performance levels that your organization intends or desires to attain. See also PERFORMANCE PROJECTIONS.

GOVERNANCE. The system of management and controls exercised in the stewardship of your organization.

HIGH PERFORMANCE. Ever-higher levels of overall organizational and individual performance, including quality, productivity, innovation rate, and cycle time.

HOW. The systems and processes that your organization uses to achieve its mission requirements.

IDENTIFY. Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. Identify is one of the five functions included in the *Cybersecurity Framework* Core. The others are Protect, Detect, Respond, and Recover.

INNOVATION. Making meaningful change to improve products/services, processes, or organizational effectiveness and create new value for stakeholders. The outcome of innovation is a discontinuous or breakthrough change.

INTEGRATION. The harmonization of plans, processes, information, resource decisions, workforce capability and capacity, actions, results, and analyses to support key organization-wide goals. See also ALIGNMENT.

KEY. Major or most important; critical to achieving your intended outcome.

KNOWLEDGE ASSETS. Your organization's accumulated intellectual resources; the knowledge possessed by your organization and its workforce in the form of information, ideas, learning, understanding, memory, insights, cognitive and technical skills, and capabilities.

LEARNING. New knowledge or skills acquired through evaluation, study, experience, and innovation.

LEVELS. Numerical information that places or positions your organization's results and performance on a meaningful measurement scale.

MEASURES AND INDICATORS. Numerical information that quantifies the input, output, and performance dimensions of processes, products, programs, projects, services, and the overall organization (outcomes).

MISSION. Your organization's overall function.

PARTNERS. Key organizations or individuals who are working in concert with your organization to achieve a common goal or improve performance. Typically, partnerships are formal arrangements. See also COLLABORATORS.

PERFORMANCE. Outputs and their outcomes obtained from processes, products/services, and customers that permit you to evaluate and compare your organization's results to performance projections, standards, past results, goals, and other organizations' results.

PERFORMANCE EXCELLENCE. An integrated approach to organizational performance management that results in (1) delivery of ever-improving value to customers and stakeholders, contributing to ongoing organizational success; (2) improvement of your organization's overall effectiveness and capabilities; and (3) learning for the organization and for people in the workforce.

PERFORMANCE PROJECTIONS. Estimates of your organization's future performance. See also GOALS.

PROCESS. Linked activities with the purpose of producing a product or service for a customer (user) within or outside your organization.

PROTECT. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. Protect is one of the five functions included in the *Cybersecurity Framework* Core. The others are Identify, Detect, Respond, and Recover.

RECOVER. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. Recover is one of the five functions included in the *Cybersecurity Framework* Core. The others are Identify, Protect, Detect, and Respond.

RESPOND. Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. Respond is one of the five functions included in the *Cybersecurity Framework* Core. The others are Identify, Protect, Detect, and Recover.

RESULTS. Outputs and outcomes achieved by your organization.

SEGMENT. One part of your organization's customer, market, product offering, or workforce base.

SENIOR LEADERS. Your organization's senior management group or team.

STAKEHOLDERS. All groups that are or might be affected by your organization's actions and success. See also CUSTOMER.

STRATEGIC ADVANTAGES. Those marketplace benefits that exert a decisive influence on your organization's likelihood of future success. These advantages are frequently sources of current and future competitive success relative to other providers of similar products/services.

STRATEGIC CHALLENGES. Those pressures that exert a decisive influence on your organization's likelihood of future success. These challenges are frequently driven by your organization's anticipated competitive position in the future relative to other providers of similar products/services.

STRATEGIC OBJECTIVES. The aims or responses that your organization articulates to address major change or improvement, competitiveness or social issues, and business advantages. See also ACTION PLANS.

SYSTEMATIC. Well-ordered, repeatable, and exhibiting the use of data and information so that learning is possible.

TRENDS. Numerical information that shows the direction and rate of change of your organization's results or the consistency of its performance over time.

VALUE. The perceived worth of a product, process, asset, or function relative to its cost and possible alternatives.

VALUES. The guiding principles and behaviors that embody how your organization and its people are expected to operate.

VISION. Your organization's desired future state.

VOICE OF THE CUSTOMER. Your process for capturing customer-related information.

WORK PROCESSES. Your organization's most important internal value-creation processes.

WORKFORCE. All people actively supervised by your organization and involved in accomplishing your organization's work, including paid employees (e.g., permanent, part-time, temporary, and telecommuting employees, as well as contract employees supervised by your organization) and volunteers, as appropriate.

WORKFORCE CAPABILITY. Your organization's ability to accomplish its work processes through its people's knowledge, skills, abilities, and competencies.

WORKFORCE CAPACITY. Your organization's ability to ensure sufficient staffing levels to accomplish its work processes and deliver your products/services to customers, including the ability to meet seasonal or varying demand levels.

WORKFORCE ENGAGEMENT. The extent of workforce members' emotional and intellectual commitment to accomplishing your organization's work, mission, and vision.

Benefits of Using the *Baldrige Cybersecurity Excellence Builder*, by Organizational Role

Role/Function	Benefit of/Reason for Using the *Baldrige Cybersecurity Excellence Builder*
Board and Executive Management	• Understand how internal and external cybersecurity should support organizational (business) objectives, including support for customers • Understand current and planned workforce engagement processes and their success • Understand opportunities to improve cybersecurity in alignment with organizational objectives • Understand the potential exposure of the organization's assets to various risks • Align cybersecurity policy and practices with the organization's mission, vision, and values
Chief Information Officer (CIO)	• Understand how cybersecurity affects organizational information management practices and culture • Improve communication and engagement with organizational leaders and the cybersecurity workforce • Understand how cybersecurity affects the organization's culture and environment
Chief Information Security Officer (CISO)	• Support the organization's commitment to legal and ethical behavior • Create and apply cybersecurity policy and practices to support the organization's mission, vision, and values • Respond to rapid or unexpected organizational or external changes • Support continuous improvement through periodic use of the self-assessment tool • Support organizational understanding of compliance with various contractual and/or regulatory requirements • Understand the effectiveness of workforce communication, learning, and engagement, as well as operational considerations for cybersecurity
IT Process Management	• Improve understanding of business requirements and mission objectives and their priorities • Determine the effectiveness of IT processes and potential improvements • Understand how aspects of cybersecurity are integrated with organizational change management processes
Risk Management	• Discern the impact of cybersecurity on internal/external customers, partners, and workforce • Improve understanding of how workforce engagement in cybersecurity and communication to the workforce about cybersecurity impact the organization's overall risk posture • Improve management of and communication about risk related to external suppliers and partners
Legal/ Compliance Roles	• Understand legal/ethical behavior on the part of the workforce, as well as the overall cultural environment • Understand how the organization applies cybersecurity-related policies and operations to ensure responsible governance, including legal, regulatory, and community concerns • Understand how the organization integrates external suppliers and partners into cybersecurity risk management, including contractual obligations for partners' cybersecurity protection and reporting
Employees (Workforce)	• Understand leaders' expectations • Be better prepared for changes in cybersecurity capability and capacity needs • Benefit from a workplace culture and environment characterized by open communication, high performance, and engagement in cybersecurity matters • Learn to fulfill their cybersecurity roles and responsibilities

Examples of Key Linkages in the *Baldrige Cybersecurity Excellence Builder*

The questions in the Organizational Context, the process categories (1–6), and the results category (7) are closely linked. These linkages help you manage your cybersecurity risk policies and operations as a system by aligning your processes and results with your organization's unique characteristics and situation. Some examples of these linkages follow.

To accomplish this …	… define these elements …	… have these systematic processes in place …	… and track these results.
Create and carry out an effective cybersecurity strategy	**C.2b: Strategic Context** Many other sections in C.1 and C.2	**2.1:** How you include cybersecurity in your organizational strategy **2.2:** How you implement cybersecurity-related elements of your strategy **4.1:** How you measure, analyze, and improve cybersecurity performance	**7.5, Q3:** Your results for achievement of your cybersecurity strategy and action plans
Engage your overall workforce in cybersecurity	**C.1a(3):** Your overall workforce profile	**1.1, Q4:** How leaders communicate with and engage the workforce regarding cybersecurity **5.2:** How you engage your overall workforce in support of cybersecurity policies and operations	**7.3, Q2:** Your results for workforce engagement
Ensure an effective, efficient cybersecurity supply network	**C.1b(3):** Your suppliers for your cybersecurity operations	**1.1, Q1:** How leaders deploy the mission, vision, and values to suppliers **2.1, Q5:** How you decide which key cybersecurity processes to accomplish internally and externally **4.2, Q4:** How you share cybersecurity best practices **6.2b: Supply-Network Management**	**7.1, Q7:** Your results for suppliers' understanding and fulfillment of their cybersecurity roles and responsibilities **7.1, Q8:** Your results for management of your cybersecurity supply network
Protect your assets and systems	**C.1a(2): Product Offerings** **C.1a(4):** Your organization's major physical and virtual assets, and your priorities for protecting them **C.1b: Organizational Relationships**	**6.1(b):** How you protect your assets and systems **2.1:** Your cybersecurity strategy	**7.1, Q1:** Your results for the protection of assets and systems
Detect cybersecurity events	**C.1a(4):** Your organization's major physical and virtual assets, and your priorities for protecting them	**6.1(c):** How you detect cybersecurity events	**7.1, Q2:** Your results for the detection of cybersecurity events **7.1, Q5:** Effectiveness and efficiency results for your cybersecurity operations
Recover from cybersecurity events	**C.1a(4):** Your organization's major physical and virtual assets, and your priorities for protecting them **C.1b: Organizational Relationships**	**6.1(e):** How you recover from cybersecurity events	**7.1, Q4:** Your results for recovering from cybersecurity events

Crosswalk: *Baldrige Cybersecurity Excellence Builder* and *Cybersecurity Framework*

Baldrige Cybersecurity Excellence Builder Categories and Items	Related Sections in the *Cybersecurity Framework*	
	2.4, Figure 2: Notional Information and Decision Flows	Appendix A: Framework Core Functions and Categories[1]
C Organizational Context		
C.1 Organizational Description	Executive Level	ID-AM, ID-BE, ID-SC
C.2 Organizational Situation	Executive Level; Changes in Current and Future Risk	ID-BE, ID-RM
1 Leadership		
1.1 Leading for Cybersecurity	Executive Level	ID-BE, RC-CO
1.2 Governance and Societal Responsibilities	Executive Level	ID-GV, RS-CO
2 Strategy		
2.1 Strategy Development	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	ID-BE, ID-GV, ID-RA, ID-RM, ID-SC
2.2 Strategy Implementation	Business/Process Level; Mission Priority and Risk Appetite and Budget; Changes in Current and Future Risk	ID-BE, ID-GV, ID-RA, ID-RM
3 Customers		
3.1 Customer Expectations	Business/Process Management; Implementation/Operations Level	ID-BE
3.2 Customer Engagement	Business/Process Management; Implementation/Operations Level	ID-AM, PR-AT, RS-CO, RC-CO
4 Measurement, Analysis, and Knowledge Management		
4.1 Measurement, Analysis, and Improvement of Performance	Implementation Progress	DE-AE, DE-DP, RS-IM, RC-IM
4.2 Knowledge Management	Business/Process Management; Implementation/Operations Level	ID-RA, DE-AE, RS-CO
5 Workforce		
5.1 Workforce Environment	Business/Process Management; Implementation/Operations Level	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO
5.2 Workforce Engagement	Business/Process Management; Implementation/Operations Level	PR-AT, PR-IP, RS-CO
6 Operations		
6.1 Work Processes	Implementation/Operations Level	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
6.2 Operational Effectiveness	Implementation/Operations Level	ID-AM, ID-BE, ID-SC, PR-AT, PR-IP

[1]The *Cybersecurity Framework* functions are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). For definitions of these functions, see the glossary. For a detailed explanation of the categories within these functions, see the *Cybersecurity Framework* (www.nist.gov/cyberframework).

(Continued on the next page)

Crosswalk (*continued*)

Baldrige Cybersecurity Excellence Builder Categories and Items	Related Sections in the *Cybersecurity Framework*	
	2.4, Figure 2: Notional Information and Decision Flows	**Appendix A: Framework Core Functions and Categories[1]**
7 Results		
7.1 Cybersecurity Process Results	Implementation Progress	PR-AC, PR-DS, PR-IP, PR-MA, DE-AE, DE-CM, DE-DP, RS-RP, RS-AN, RS-IM, RS-MI, RC-RP, RC-IM
7.2 Customer Results	Implementation Progress	ID-BE, ID-AM, PR-AT, RS-CO, RC-CO
7.3 Workforce Results	Implementation Progress	ID-AM, ID-GV, PR-IP, DE-DP, RS-CO, PR-AT, PR-IP, RS-CO
7.4 Leadership and Governance Results	Implementation Progress	ID-BE, ID-GV, ID-RA, ID-RM, RC-CO
7.5 Financial and Strategy Results	Implementation Progress	ID-BE

Self-Analysis Worksheet

For a spreadsheet version of this worksheet, see www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative.

Process (Categories 1–6)	Reactive, Early, Developing, Mature, Leading, or Exemplary?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
1 Leadership					
1.1 Leading for Cybersecurity: How do your senior and cybersecurity leaders lead your cybersecurity policies and operations?					
1.2 Governance and Societal Responsibilities: How do you govern your cybersecurity policies and operations and make cybersecurity-related societal contributions?					
2 Strategy					
2.1 Strategy Development: How do you include cybersecurity considerations in your strategy development?					
2.2 Strategy Implementation: How do you implement the cybersecurity-related elements of your strategy?					
3 Customers					
3.1 Customer Expectations: How do you listen to your customers and determine their cybersecurity-related satisfaction?					
3.2 Customer Engagement: How do you build relationships with internal and external customers around cybersecurity?					
4 Measurement, Analysis, and Knowledge Management					
4.1 Measurement, Analysis, and Improvement of Performance: How do you measure, analyze, and then improve cybersecurity-related performance?					
4.2 Knowledge Management: How do you manage your organization's cybersecurity-related knowledge assets?					
5 Workforce					
5.1 Workforce Environment: How do you build an effective and supportive environment for your cybersecurity workforce?					
5.2 Workforce Engagement: How do you engage your workforce for high performance in support of cybersecurity policies and operations?					

(Continued on the next page)

Self-Analysis Worksheet *(continued)*

Process (Categories 1–6)	Reactive, Early, Developing, Mature, Leading, or Exemplary?				High, Medium, or Low?
	Approach	Deployment	Learning	Integration	Importance
6 Operations					
6.1 Work Processes: How do you design, manage, and improve your key cybersecurity work processes?					
6.2 Operational Effectiveness: How do you ensure effective management of your cybersecurity operations?					

Results (Category 7)	Reactive, Early, Developing, Mature, Leading, or Exemplary?				High, Medium, or Low?
	Levels	Trends	Comparisons	Integration	Importance
7.1 Cybersecurity Process Results: What are your cybersecurity performance and process effectiveness results?					
7.2 Customer Results: What are your customer-focused cybersecurity performance results?					
7.3 Workforce Results: What are your workforce-focused cybersecurity performance results?					
7.4 Leadership and Governance Results: What are your cybersecurity leadership and governance results?					
7.5 Financial and Strategy Results: What are your cybersecurity-related financial and strategy results?					

You've used the Baldrige Cybersecurity Excellence Builder to assess your organization's cybersecurity program.

WHAT'S NEXT?

Tell Us about Your Experience

Submit feedback on the *Baldrige Cybersecurity Excellence Builder* at **www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative**.

Learn More about the Baldrige Cybersecurity Initiative

See **www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative** to learn more about this initiative.

Learn More about the Cybersecurity Framework

The *Framework for Improving Critical Infrastructure Cybersecurity* (**www.nist.gov/cyberframework**) is voluntary guidance, based on existing standards, guidelines, and practices, for organizations to better manage and reduce cybersecurity risk.

Download the Baldrige Excellence Builder

The *Baldrige Excellence Builder* (**www.nist.gov/baldrige/products-services/baldrige-excellence-builder**) includes key questions for improving your organization's overall performance. It is based on the Baldrige Excellence Framework's Criteria for Performance Excellence.

Purchase the Baldrige Excellence Framework Booklet

The Baldrige Excellence Framework (Business/Nonprofit, Education, or Health Care; **www.nist.gov/baldrige/products-services/baldrige-excellence-framework**) is a comprehensive guide to organizational performance excellence.

Attend the Quest for Excellence© Conference

At Quest (**www.nist.gov/baldrige/qe**) and other Baldrige conferences, you will learn best performance management practices from Baldrige Award recipients.

Contact the Baldrige Program

We'll answer your questions on these and other products and services.

www.nist.gov/baldrige | 301.975.2036 | baldrige@nist.gov

#BaldrigeCyber
www.nist.gov/baldrige

National Institute of Standards and Technology (NIST)

The mission of NIST, an agency of the U.S. Department of Commerce, is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

Baldrige Performance Excellence Program

Created by Congress in 1987, the Baldrige Program is a unique public-private partnership that is dedicated to helping organizations improve their performance and succeed in the global marketplace. The program administers the Presidential Malcolm Baldrige National Quality Award. In collaboration with the greater Baldrige community, we address critical national needs through

- a systems approach to achieving organizational excellence;
- organizational self-assessment tools and analysis of organizational strengths and opportunities for improvement by a team of trained experts;
- training, executive education, conferences, and workshops on proven best management practices and on using the Baldrige Excellence Framework to improve;
- Baldrige-based approaches to cybersecurity risk management and community excellence; and
- support for and partnership with the Alliance for Performance Excellence (www.baldrigealliance.org), a national network of Baldrige-based programs.

Applied Cybersecurity Division, Information Technology Laboratory

As one of the major research components of NIST, the Information Technology Laboratory has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. The Applied Cybersecurity Division (www.nist.gov/itl/applied-cybersecurity) implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities. The Division:

- develops cybersecurity standards and guidelines in an open, transparent, and collaborative way;
- does cybersecurity testing and measurement—from developing test suites and methods to validating cryptographic modules; and
- advances applied cybersecurity—applications of NIST's research, standards, and testing and measurement work.

Foundation for the Malcolm Baldrige National Quality Award

The mission of the Baldrige Foundation (www.baldrigefoundation.org) is to ensure the long-term financial growth and viability of the Baldrige Performance Excellence Program and to support organizational performance excellence in the United States and throughout the world.

For more information:

www.nist.gov/baldrige | 301.975.2036 | baldrige@nist.gov

CONNECT WITH BALDRIGE

@BaldrigeProgram #Baldrige

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

MIX
Paper from responsible sources
FSC® C101537

03/2019

T1554