NIST Special Publication 800
NIST SP 800-50r1

Building a Cybersecurity and Privacy Learning Program

Marian Merritt
Susan Hansche
Dr. Brenda Ellis
Kevin Sanchez-Cherry
Julie Nethery Snyder
Donald Walden

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-50r1

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication 800
NIST SP 800-50r1

Building a Cybersecurity and Privacy Learning Program

Marian Merritt
Applied Cybersecurity Division
Information Technology Laboratory

Susan Hansche
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security

Dr. Brenda Ellis
National Aeronautics and Space Administration

Kevin Sanchez-Cherry
Office of the Chief Information Officer
Department of Transportation

Julie Nethery Snyder
MITRE

Donald Walden
Internal Revenue Service

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-50r1

September 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2024-08-09
Supersedes NIST SP 800-50 (October 2003) https://doi.org/10.6028/NIST.SP.800-50; Supersedes NIST SP 800-16 (April 1998) https://doi.org/10.6028/NIST.SP.800-16

How to Cite this NIST Technical Series Publication:

Merritt M, Hansche S, Ellis B, Sanchez-Cherry K, Snyder JN, Walden D (2024) Building a Cybersecurity and Privacy Learning Program. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-50r1. https://doi.org/10.6028/NIST.SP.800-50r1

Author ORCID iDs

Marian Merritt: 0000-0002-2116-8959

Contact Information

sp800-50-comments@nist.gov
National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/50/r1/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

This publication provides guidance for federal agencies and organizations to develop and manage a life cycle approach to building a Cybersecurity and Privacy Learning Program (CPLP). The approach is intended to address the needs of large and small organizations as well as those building an entirely new program. The information leverages broadly accepted standards, regulations, legislation, and best practices. The recommendations are customizable and may be implemented as part of an organization-wide process that manages awareness, training, and education programs for a diverse set of federal employee audiences. The program should encourage behavior change as part of risk management and lead to developing a privacy and security culture in the organization. The guidance also includes suggested metrics and evaluation methods to regularly improve and update the program as needs evolve.

Keywords

awareness; behavior change; cybersecurity; education; learning program; privacy; privacy culture; role-based; security culture; training.

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective cybersecurity and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

Table of Contents

List of Tables

List of Figures

Acknowledgments

This publication was developed through the efforts of a dedicated team of volunteer authors. We express our thanks to Jessica Dickson, National Institute of Standards and Technology (NIST); Susanne Furman, NIST; Julie Haney, NIST; Dan Jacobs, Office of Personnel Management; Jody Jacobs, NIST; Eric Gray, Department of Education; Sarah Moffatt, National Institutes of Health; Dylan Gilbert, NIST; Naomi Lefkovitz, NIST; Jeremy Licata, NIST; Rodney Petersen, NIST; Eduardo Takamura, NIST; and Victoria Yan Pillitteri, NIST.

Executive Summary

Ensuring that a federal organization's workforce is aware of and prepared to respond appropriately and effectively to cybersecurity and privacy risks is an important effort that requires a strategic approach based on thoughtful planning, resource considerations, and leadership-driven decision-making. This long-awaited update to the 2003 NIST Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program,* provides guidance to create and manage a program that includes cybersecurity and privacy awareness campaigns, role-based training, and other workforce education programs. These programs combine to create an overall Cybersecurity and Privacy Learning Program (CPLP) that is part of a larger organizational effort to reduce cybersecurity and privacy risks. The resulting CPLP supports federal requirements and incorporates industry-recognized best practices for risk management.

In addition to meeting statutory responsibilities under the Federal Information Security Management Act (FISMA) [2], this Special Publication supports the National Defense Authorization Act of 2021 (NDAA) [1] to "publish standards and guidelines for improving cybersecurity awareness of employees and contractors of Federal agencies."[1] Including privacy as a foundational element in the CPLP reflects the guidance found in the 2016 update to the Office of Management and Budget (OMB) Circular A-130:

> …it also emphasizes the role of both privacy and security in the federal information life cycle. Importantly, the inclusion of privacy represents a shift from viewing security and privacy requirements as merely compliance exercises to understanding security and privacy as crucial and related elements of a comprehensive, strategic, and continuous risk-based program at federal agencies. [3]

Additionally, this update includes elements previously found in SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* [4], which identified federal agency and organizational work roles that required specialized role-based training for cybersecurity tasks and skills. The relevant content from SP 800-16 has been incorporated into this publication or has been included in SP 800-181r1 [5]. As a result, SP 800-16 will be withdrawn upon the release of this publication.

Everyone in an organization plays a role in the success of an effective cybersecurity and privacy program. For those whose information technology, cybersecurity, or cybersecurity-related job responsibilities require additional or specific training, the NICE Workforce Framework for

[1] Section 9402 of FY 21 NDAA, *Development of Standards and Guidelines for Improving Cybersecurity Workforce of Federal Agencies*, amends the NIST Act as follows: "(b): PUBLICATION OF STANDARDS AND GUIDELINES ON CYBERSECURITY AWARENESS. Not later than three years after the date of the enactment of this Act, the Director of the National Institute of Standards and Technology shall publish standards and guidelines for improving cybersecurity awareness of employees and contractors of federal agencies."

Cybersecurity (NICE Framework)[2] [5] identifies the specific knowledge and skills necessary to perform tasks associated with work roles in these areas.[3]

Users of this publication will find guidance on the steps necessary to:

- Build an effective CPLP for all federal organizational personnel, including employees and contractors, that leads to improved norms and behaviors that reduce cybersecurity and privacy risks to the organization while creating a privacy and security culture
- Identify personnel who require advanced training
- Create a methodology for evaluating the program
- Engage in ongoing improvement to the program

Throughout each section, there are recommendations to enable a program to continually evolve and improve, thereby minimizing privacy and security risks to the organization.

This document identifies the phases in the management of a CPLP and is organized as follows:

- Section 1: Introduction
- Section 2: CPLP Plan and Strategy
- Section 3: CPLP Analysis and Design
- Section 4: CPLP Development and Implementation
- Section 5: CPLP Assessment and Improvement

[2] The National Initiative for Cybersecurity Education (NICE) is led by NIST in the U.S. Department of Commerce.
[3] As of the time of development of this publication, NIST is leading a privacy workforce development effort to create a privacy companion to NICE.

1. Introduction

Reducing and managing cybersecurity and privacy risks require continuous attention from everyone in an organization. A key component of organizational cybersecurity and privacy plans is a learning program, which helps to build an understanding of risks and explain everyone's role in identifying, responding to, and managing those risks. While learning programs vary in each federal organization, there are fundamental shared elements that can be utilized to create a Cybersecurity and Privacy Learning Program (CPLP) strategy and establish support for implementation, evaluation, and reporting activities. The CPLP effort sits within a larger federal organizational program to address risks, including efforts to reduce risks from physical privacy and security threats, insider threats, and other related human risk management concerns. Such efforts are outside of the scope of this document.

For ease of use, the remainder of this document will use the term "CPLP" to refer to all elements of cybersecurity and privacy awareness, training, and educational activities to include other programs with titles such as awareness training, practical exercises (e.g., tabletop exercises, role-playing simulations, cyber ranges, or phishing campaigns), topic-based training, role-based training, and educational programs. It is not necessary for organizations to rename their programs as CPLP; this term is applied generically.

The previous version of SP 800-50 defined awareness, training, and education as separate elements in a learning continuum. Research efforts [6][7] conducted with Federal Government training managers have shown that these terms have different meanings and can lead to confusion when describing the broader purpose of building a CPLP. While some managers may refer to programs as "awareness and training" or "awareness training," the terms are applied inconsistently across organizations. Regardless of what an organization calls its program, the overarching goal of a CPLP is to provide opportunities for learning at all levels or stages of one's career. It is about creating programs where learning can take place.

This Special Publication also uses the term "learner" to describe individuals in any of the learning program audience segments. The term "learner" can be found in SP 800-181r1 [5], where it refers to an individual who is acquiring specialized knowledge or developing a skill. This definition is useful here since it describes all participants in a "learning program." This document will refer to the program as a CPLP or CPLPs, as some organizations may require multiple programs to fulfill the learning requirements of the entire workforce.

1.1. Purpose

This document provides guidelines for building and maintaining comprehensive CPLPs for federal organizations and includes awareness activities and campaigns, awareness training, practical exercises, topic-based training, role-based training, and educational programs. The document includes guidance on how an organization can create a strategic program plan and ensure that there are appropriate resources to meet the organization's learning goals.

This publication is intended to serve a diverse audience, including:

- **Workforce and learning professionals**
    - Individuals associated with designing, developing, implementing, assessing, operating, managing, and improving CPLPs for federal agencies and organizations
    - Individuals responsible for overseeing federal human resources, talent management, contractors, and training programs
    - Individuals responsible for federal CPLPs, learning professionals, and managers, such as Chief Learning Officers (CLOs) and curriculum developers
- **Leadership and management**
    - Individuals responsible for meeting staff learning needs, prioritizing the use of learning resources, identifying learning gaps, and evaluating learning effectiveness within the workspace
    - Individuals with information system oversight or governance responsibilities, such as senior leaders, risk executives, authorizing officials, Chief Information Officers (CIOs), Chief Information Security Officers (CISOs), Data Management Officers (DMOs), and Chief Privacy Officers (CPOs)
    - Individuals with cybersecurity and privacy management responsibilities (e.g., managing programs and projects and ensuring that staff members have the appropriate knowledge and skills to perform their work roles), including program and project managers, cybersecurity managers, and security operation managers
- **Cybersecurity and privacy specialists**
    - Workforce members who are responsible for assisting in the identification of CPLP activities as a subject-matter expert (SME), meeting the requirements of the roles or job functions, identifying learning and/or competency gaps and needs within the organization's cybersecurity and privacy program, determining necessary customizations, and developing a compliance baseline for the organization

Key considerations for managers of federal Cybersecurity and Privacy Learning Programs[4]

- Develop, maintain, and implement mandatory organization-wide CPLPs for all members of the workforce that support enterprise cybersecurity and privacy goals and objectives.

[4] This text is adapted from OMB Circular A-130, Appendix I, Section 4.h, and is meant to accommodate the needs of any organization, not just federal agencies and organizations.

- Ensure that the CPLPs align with established rules of behavior and are consistent with applicable policies, standards, and guidelines.
- Inform the workforce of available cybersecurity and privacy resources (internal and external), such as policies, products, techniques, best practices, or expertise.
- Provide both foundational and more advanced levels of cybersecurity and privacy training to the workforce, and ensure that measures are in place to assess the knowledge and skill of participants.
- In consultation with senior leadership, identify cybersecurity and privacy behaviors that impact risk in a data-driven manner.
- Identify those who need specialized cybersecurity and privacy training based on assigned cybersecurity and privacy roles and responsibilities.
- Measure attitudes, behaviors, and workforce sentiment as part of tracking the development of a cybersecurity and privacy culture.

1.2. Scope

This guide describes how a federal organization can design, develop, implement, and maintain a CPLP as part of an enterprise cybersecurity and privacy program. This includes identifying the learning needs of the organization's personnel, including federal full-time or part-time employees, interns, retirees, contractors, external partners, consultants, researchers, and any users who access the enterprise system or data in support of the organizational mission.

CPLPs are inclusive of various other programs, such as awareness programs, social engineering campaigns, new hire training, regular training, technical training, role-based training, and other relevant learning activities conducted within the organization or through external resources (e.g., courses, certificates, and advanced programs). Additionally, CPLPs sit within a larger federal organizational effort to address and reduce risks from physical privacy and security threats, insider threats, and other related human risk management concerns. Those efforts are outside of the scope of this document.

1.3. CPLP Life Cycle

CPLPs must have actively managed plans throughout their life cycles, which requires attention and adjustment over time. CPLP managers should carefully and thoughtfully outline, discuss, review, and document the CPLP's goals and available options. When the owners of the organization's CPLP adopt an effective strategy and develop a proper planning approach with measurement and feedback throughout the year, the entire organization remains connected to

the CPLP's objectives. Figure 1 shows the key phases of building and managing a learning program: Plan and Strategy, Analysis and Design, Development and Implementation, and Assessment and Improvement.

Fig. 1. Cybersecurity and Privacy Learning Program life cycle

These phases can occur in sequence or simultaneously. At any time during the life cycle, CPLP managers and their teams can develop curriculum, evaluate instructor feedback, send out practical exercise email quizzes, design posters for awareness, or develop a presentation for senior leadership. Consider this diagram a reminder of the breadth of work.

In a broad sense, CPLPs are valued elements of the organization's learning culture. To be effective, the CPLPs must be linked to organizational goals and viewed as adaptive, continuous, and evolving. In a learning organization, personnel can expand and enhance their current capabilities to understand and meet new mission requirements. Personnel are respected for their ability to create and inspire others and are active in creating life-long learning achievements. If an organization offers other learning programs (e.g., career development, leadership, and executive development), CPLPs need to be similarly integrated into the enterprise-wide learning structure.

1.4. Developing a Cybersecurity and Privacy Culture

Developing a cybersecurity and privacy culture is an important component of establishing a successful CPLP. The culture of the organization should emphasize, reinforce, and drive its desired behaviors toward cybersecurity and privacy. Risks increase when the dominant culture fails to recognize the value of engaging individuals in the efforts to support cybersecurity and privacy best practices. There are two risk sectors that the CPLP can address:

1. Technical risks — Systems are poorly designed, unpatched, or similarly compromised from the ideal state. This can be addressed with topic-based and role-based training designed for practitioners with significant cybersecurity and/or privacy responsibilities.
2. Human risks — Individuals fail to maintain their cybersecurity and privacy standards, or systems have been poorly configured and allow individuals to expose the organization to undue threats through a variety of human failures.

When a CPLP is valued in the organization's culture, the ability to address both types of risk increases. The organization's leaders establish a CPLP as a significant component of managing risks by supporting, championing, and participating in learning activities, from awareness campaigns to role-based training. CPLP learning managers create rigorous measurement systems to evaluate the workforce's attitudes, engagement, and support for the program. CPLP activities contribute to and help measure the organization's cybersecurity and privacy culture. Human resource leaders reinforce those cultural norms by ensuring that CPLP messaging is part of onboarding and other workplace materials. Together, these efforts set the tone for the entire organization.

People are an organization's greatest asset. A cybersecurity and privacy culture supports an environment in which the entire workforce is well-versed in cybersecurity and privacy risk management needs, expectations, and values. An organization, in turn, supports an effective cybersecurity and privacy culture when it understands the needs of the workforce and provides education and training to help employees and contractors learn expected cybersecurity and privacy behaviors. Any effective learning activity can be incorporated into a CPLP when it is respectful, inclusive, and helps learners understand their roles in the organization. The content should indicate to the learner that they are a valued participant in helping the organization manage risks. The workforce appreciates that they will contribute to the organization's positive cybersecurity and privacy culture with the knowledge and skills they acquire by participating in the CPLP.

Organizations and system owners must develop a CPLP approach that champions every user's responsibility to protect information and assets. New technologies and risks will continue to require an organization-wide approach to managing cybersecurity and privacy risks. The NIST Cybersecurity Framework (CSF) [8], Privacy Framework [9], and Risk Management Framework (RMF) [10] highlight the importance of awareness and training for personnel as well as monitoring and improving risk management practices.

1.5. Relationship Between Cybersecurity and Privacy

While cybersecurity and privacy are independent and separate disciplines, some of their objectives overlap. Cybersecurity programs are responsible for protecting information, information systems, and operational technologies from unauthorized access, use, disclosure, disruption, modification, or destruction (i.e., unauthorized system activity or behavior) in order to provide confidentiality, integrity, availability, and safety. Privacy programs are responsible for managing risks to individuals that are associated with data processing throughout the information life cycle[5] in order to provide predictability, manageability, and disassociability, as well as ensure compliance with applicable privacy requirements. Managing cybersecurity risks contributes to managing privacy risks. However, managing cybersecurity risks alone is not sufficient, as privacy risks can also arise by means unrelated to cybersecurity incidents, as illustrated in Fig. 2 [9].

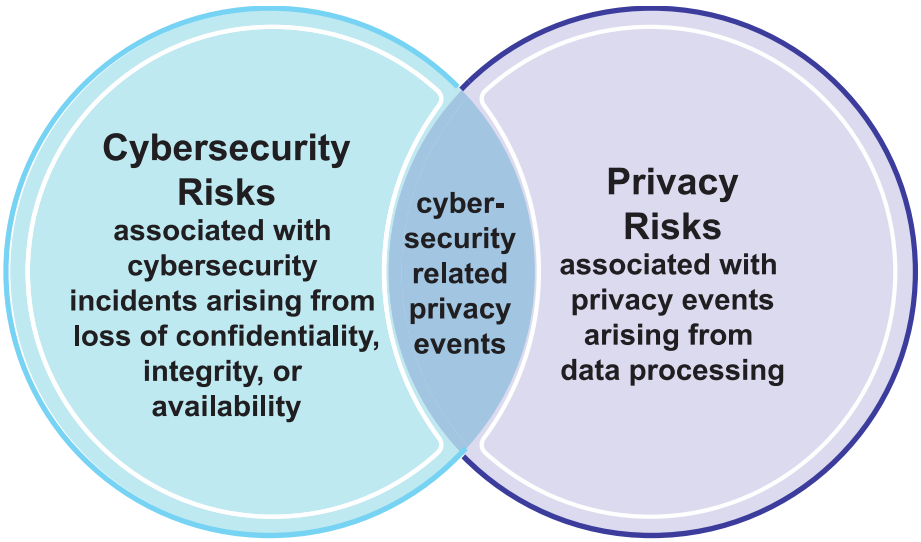

Fig. 2. Cybersecurity and privacy risk relationship

For example, an organization may combine de-identified data with a new data set during data processing, resulting in re-identification. Similarly, a de-identified data set may be publicly released but result in re-identification when combined with other public information. The data processing activities do not include a cybersecurity incident or breach but still introduce privacy risks.

Teaching the workforce about different cybersecurity and privacy risks enables them to effectively address the risks they encounter in their daily activities. For example, all members of the workforce will need training that helps them understand what a privacy event is and how one might occur within their organization. They should be able to identify and report a privacy event. Incident response professionals will need training that helps them determine when a cybersecurity incident may also be a privacy event, which often requires additional procedures when responding (e.g., determining if an unsecured site resulted in an actual privacy breach).

[5] The information life cycle describes the stages through which information passes, such as its creation or collection, processing, dissemination, use, storage, and disposition, including destruction and deletion [3].

Organizations can benefit from a coordinated and flexible approach to developing CPLPs that effectively meet the organization's needs.[6]

Once an organization understands the relationship between cybersecurity and privacy, it can determine its approach to developing both integrated and cybersecurity- or privacy-specific learning activities based on the relevant topics and workforce roles in its environment. For example, the organization can determine how to effectively:

- Associate learning tracks with work roles (particularly those with data processing activities) and job performance
- Describe its approach to managing cybersecurity and privacy risks in a way that aligns with enterprise risk management capabilities
- Incorporate lessons learned from cybersecurity and privacy risks, audit findings, incidents, events, or changes to governance documents (e.g., laws, regulations, policies, and standards) into general and role-based training
- Institute learning activities that are appropriate for both internal and external members of the workforce, including contractors and third parties
- Identify learning obligations in contracts and agreements
- Identify and track metrics to assess the effectiveness of learning efforts (e.g., determining whether the number of a certain type of incident or event decreases after a targeted awareness campaign)

1.5.1. Privacy Risk Management Concepts to Emphasize

Members of the workforce with roles that can impact privacy must also have a clear understanding of how to identify and address privacy risks that may arise. The NIST Privacy Framework [9] provides a common language for understanding, managing, and communicating about privacy risks. Just as the workforce considers the risks associated with security events, they must also consider *privacy events* — the potential problems that could arise from system, product, or service operations with digital or non-digital data through a complete life cycle, from data collection to disposal. Privacy problems can arise from an individual's direct use of a product. Some problems can also arise simply from individuals' interactions with systems, products, and services, even when the data being processed is not directly linked to identifiable individuals. The problems that individuals can experience as a result of data processing can be expressed in various ways. The NIST Privacy Framework describes them as ranging from dignity-

[6] Role-based privacy training should address the full scope of privacy risks, as depicted in Fig2. For federal agencies, role-based privacy training addresses the types of information that may constitute personally identifiable information (PII) and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process data documented in privacy policies and notices, system of records notices, computer matching agreements and notices, privacy impact assessments, Privacy Act statements, contracts, information sharing agreements, memoranda of understanding, or other documentation.

type effects (e.g., embarrassment or stigmas) to more tangible harms (e.g., discrimination, economic loss, or physical harm) [9].[7]

Individuals may experience privacy problems that arise from data processing, and the organization may in turn experience impacts, such as noncompliance costs, revenue loss from customer abandonment of products and services, or harm to its external brand reputation or internal culture. Organizations commonly manage these types of impacts at the enterprise risk management level. By connecting problematic data actions (i.e., data processing activities that can cause problems) that individuals experience to these well-understood organizational impacts, organizations can bring privacy risks into parity with other risks that they manage in their broader portfolio and drive more informed decision-making about resource allocation to strengthen privacy programs. Figure 3 illustrates the relationship between privacy risks and organizational risks [9].

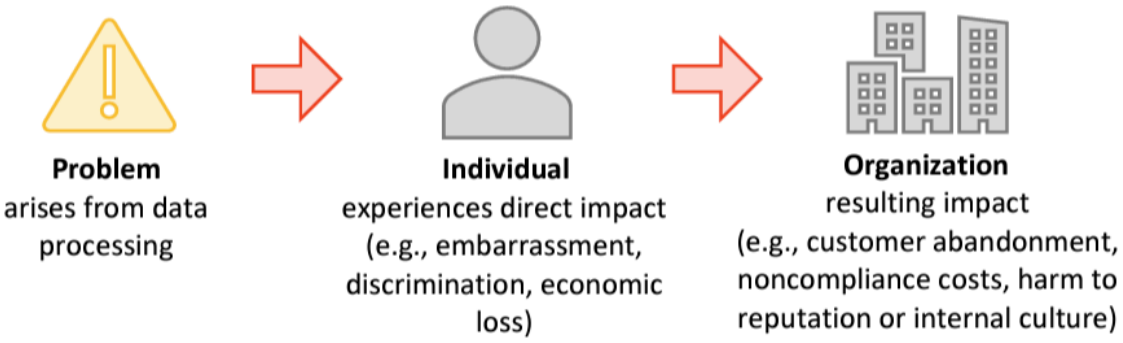

Fig. 3. Relationship between privacy risks and organizational risks

CPLPs are most effective when they help the workforce understand both the direct impacts of privacy events on individuals and the resulting impacts that privacy risks can have on the organization. For example, a CPLP can address the types of impacts that an individual may experience from the secondary use of data (e.g., for marketing purposes) and the resulting consequences to the organization (e.g., costs associated with non-compliance, loss of trust in the organization, or a shift in mission priorities while addressing the impact).

1.5.2. Coordinating Cybersecurity and Privacy Learning Efforts

An organization's CPLP should coordinate with existing cybersecurity and privacy programs. With limited resources, duplicating efforts will negatively affect one or both programs. In cases where there is an integrated cybersecurity and privacy program, this is less likely to be an issue.

1.6. Roles and Responsibilities

While it is important to understand the policies that require agencies to develop and implement CPLPs, it is also crucial for organizations to understand who is responsible for

[7] The NIST Catalog of Problematic Data Actions and Problems provides examples of privacy problems that individuals may face and is available at https://github.com/usnistgov/PrivacyEngCollabSpace/blob/master/tools/risk-assessment/NIST-Privacy-Risk-Assessment-Methodology-PRAM/catalog-PDAP.md.

cybersecurity and privacy education. This section identifies and describes those in an organization who are responsible for ensuring that the workforce has access to and completes their cybersecurity and privacy training.

SP 800-37r2 (Revision 2), *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* [10], identifies the typical roles associated with these programs. Since terminology may vary by organization, it can be useful to refer to the NICE Framework as a complementary tool for identifying those with responsibilities for managing the CPLP and those who require additional training. The NIST Privacy Workforce Public Working Group (PWWG)[8] also has information about the tasks, knowledge, and skills required of privacy professionals in an organization.

The size, maturity, and resources of CPLPs can vary widely, even within the same organization. The roles and responsibilities for key positions in CPLPs should be documented to help ensure the most effective use of resources and enable the programs to mature to their desired state. As such, each organization needs to consider how to assign these roles. Whether there is a single person serving multiple functions or multiple people collaborating across the organization, be mindful of the possibility of overlapping responsibilities.

1.6.1. Head of Organization

The head of the organization is responsible and accountable for information security protections and must prioritize the development of effective CPLPs. This includes implementing a viable cybersecurity and privacy program with a strong learning component. As noted in SP 800-37r2, the head of the organization ensures that "the organization has adequately trained personnel to assist in complying with the security and privacy requirements in legislation, Executive Orders, policies, directives, instructions, standards, and guidelines" [10]. The head of the organization should:

- Designate leadership roles to manage the organization's CPLPs, develop the strategic direction for the learning programs, write performance goals and objectives, and review and manage performance metrics. CPLP managers are responsible for the analysis, design, development, and delivery of CPLPs and should be given adequate resources to meet performance goals and objectives.
- Ensure that an agency- or organization-wide cybersecurity and privacy program is implemented; is well-supported by resources, including personnel and funding; and is effective at reducing and managing risk.
- Ensure that the agency or organization has sufficiently knowledgeable and skilled personnel to support its programs and resources and protect individual privacy.
- Ensure that privacy and cybersecurity behaviors related to organizational risks are identified and measured in a data-driven way.

[8] See the NIST Privacy Workforce Public Working Group website at (PWWG) https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group.

- Support the ongoing measurement of the cybersecurity and privacy culture.

1.6.2. Senior Leadership

FISMA [2], OMB Circular A-130 [3], and various other regulations designate the responsibility for ensuring CPLPs to certain senior official positions. Titles for these positions include Executive Director, Associate Director, Assistant Director, Division Chief, Chief Information Officer, Chief Privacy Officer, Chief Information Security Officer, Chief Data Officer, Chief Artificial Intelligence Officer, Information Owner, System Owner, Mission or Business Owner, Senior Accountable Official for Risk Management, and System Security or Privacy Officer. These roles are tasked with setting strategic direction, identifying and managing risks, ensuring that resources are available, and overseeing personnel with significant responsibilities for cybersecurity and privacy, including the roles found in appropriate program funding and management.

In addition, senior leaders must champion workforce requirements by:

- Leading by example and participating in their own CPLP training, as required
- Identifying who has cybersecurity and privacy responsibilities and documenting them in position descriptions or other relevant work and performance requirement statements
- Identifying relevant learning requirements and documenting them in individual development plans or other career pathway documentation
- Establishing policies and procedures for learning programs and documenting them in the organizational records
- If serving in the role of system owner or data owner, designating staff who have significant cybersecurity and/or privacy responsibilities on their system (e.g., general support systems and major applications) and ensuring that users and support personnel are appropriately trained in how to fulfill their responsibilities before being granted access to system resources

Agencies and organizations should form a Senior Leadership Committee that meets regularly with CPLP managers to discuss strategy and provide resource support. The CPLP managers will provide the Senior Leadership Committee with regular reports on the CPLP's performance throughout the year. If there is an emerging risk or new threat that needs to be addressed in the CPLP, the Senior Leadership Committee can connect the learning team with operational teams and SMEs who can provide learning content and resources. Organizations may also include employee representatives as stakeholders in the Senior Leadership Committee to ensure that they have a voice in decision-making.

1.6.3. CPLP Managers

CPLP managers have tactical-level responsibilities for the CPLP. In this role, the CPLP manager should work with the curriculum development professionals and instruction team, security

operations team, information system security officers and managers, CISOs, human resources (HR), procurement, and risk executive teams to:

- Collaborate with policy SMEs on the interpretation and application of relevant legislation and organizational policies to guide the CPLP program
- Facilitate the development of learning material that is appropriate and timely for the intended audiences
- Develop effective approaches to disseminating learning materials to the intended audience for maximum engagement and impact
- Offer learners and their managers an effective way to provide feedback on the learning material and its presentation
- Oversee periodic reviews, and update the learning material when necessary
- Ensure the efficient use of all available internal and external resources to effectively manage the CPLP
- Assist in establishing a tracking and reporting strategy
- Assist in identifying those with significant cybersecurity and privacy responsibilities
- Provide senior leadership with regular status reports on the CPLP's goals, objectives, and performance metrics

1.6.4. Managers

The term "managers" includes supervisors and those with organizational responsibilities to ensure that the personnel who report to them comply with cybersecurity and privacy learning requirements. Managers should:

- Work with the senior leaders and CPLP managers to fulfill shared responsibilities
- Create individual development plans (IDPs) to assess the knowledge gaps of personnel with significant cybersecurity and privacy roles and responsibilities
- Promote the professional development of personnel with cybersecurity and privacy responsibilities, and encourage them to acquire industry-recognized certifications
- Ensure that personnel understand the specific rules of each system and application that they use
- Ensure that all personnel (including the general workforce) maintain competence in cybersecurity and privacy by participating in the CPLP
- Work to reduce errors and omissions by personnel that might be caused by a lack of awareness or training

1.6.5. System User

The system user is an individual authorized to access information and information systems to perform assigned duties. As noted in SP 800-37r2,

> System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems, using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior. [10]

2. CPLP Plan and Strategy

A CPLP strategic plan provides an organization-wide view of the current state of cybersecurity and privacy learning, where the organization wants or needs to be, and how to address the gap between those two states (e.g., resources, staffing.) The CPLP strategic plan helps CPLP managers ensure that the organization's personnel are ready to meet the challenges of the cybersecurity and privacy risks associated with their work.

OMB Circular A-130 [3] establishes a general policy for the planning, budgeting, governance, acquisition, and management of federal information, personnel, equipment, funds, IT resources, and supporting infrastructure and services. Each federal agency is required to develop, maintain, and implement a comprehensive CPLP to meet its mission needs. To develop a robust program with a variety of materials, including offering learners engaging opportunities to stay current on relevant cybersecurity and privacy risks to their organization, the CPLP must have an effective strategy for development, implementation, and continual improvement.

This section discusses the steps involved in building a CPLP strategic plan that takes the organization's objectives, unique requirements, audience types, and program scope into consideration. The planning stages will also help the organization evaluate its priorities, budget, resources, and communication plans.

2.1. Building the Strategic Plan

The CPLP strategic plan must intersect with the organization's strategic plan for continual workforce development. The owner of the CPLP should understand the structure and mission of the organization to determine where the organization's strategy originates. Some agencies are organized with a top-down approach, where a headquarters owns the mission and provides guidance on the CPLP strategy. Other organizations develop CPLPs in various business functions or combine both approaches. Documenting the CPLP strategy and how it supports the goals of the organization's risk management strategy shows executive leadership why the CPLP is needed.

A well-developed CPLP strategic plan describes how an organization's risk management and cybersecurity and privacy culture enable all personnel to assess risks with their every action and decision. With agencies of varying sizes, a program that works for one will not necessarily work for another. Each agency must develop a program that will work best for them. The CPLP strategy should always be clearly stated and will most likely be reviewed by the Senior Leadership Committee and agreed upon before any funding is approved.

The CPLP strategic plan should address key items, including:

- Vision and mission
- Strategic goals and objectives
- Training approaches and action plans
- Tactics that help pursue the objectives

- Metrics and reporting

The CPLP strategic plan should also:

- Describe how it supports a culture of risk-based decision-making and emphasizes the importance of transformational workforce learning, including the development of knowledge, skills, and capabilities to help workers succeed now and in the future
- Explain how the program will meet knowledge and skills gaps, enhance overall capabilities, and support a culture of personnel engagement in their cybersecurity and privacy roles
- Intersect with the overall mission of the organization (e.g., mission and vision statements, risk tolerance, learning goals, objectives, outcomes, methods, and organizational structure)
- Include information about organizational policies and policy owners, such as how existing rules of behavior, policies, procedures, and guidance will be communicated to personnel
- Include metrics and measurements that help determine whether the current programs are meeting goals and learners are retaining knowledge and skills, changing their behaviors, and developing positive attitudes in support of the cybersecurity and privacy culture
- Include operational tactics, such as the tools, mechanisms, or methods that the program owners will leverage to achieve program objectives
- Identify key stakeholders, leaders, and roles, many of whom will be within the offices of the CIO, CISO, Senior Agency Information Security Officer (SAISO), Senior Agency Official for Privacy (SAOP), CPO, and HR
- Use risk assessment results and existing strategies to inform the alignment between program development, learning materials, and risk management
    - Existing CPLPs may also benefit from a gap analysis or current program assessment to clearly distinguish between the current and target states and enable the program leadership to shape their approach accordingly.
- Identify how the program will meet regulatory and compliance requirements to minimize risks by educating personnel on their roles in the cybersecurity and privacy culture of the organization
- Plan for and support the needs of a diverse workforce, including those with accessibility requirements and those who work remotely or travel frequently
- Include learning methods that are experiential and atomize content (i.e., look at how existing content can be separated into smaller items or repurposed)

2.2. Developing CPLP Policies and Procedures

CPLP policies and procedures work together to express what the organization wants to do and how to do it. Policies are clear and simple statements, rules, or assertions that specify the correct or expected behavior of an entity. They provide the guiding principles for meeting the mission and conducting operations, and they can ensure consistent and effective training and awareness methods. Procedures describe how policies will be implemented or enacted. They are written to include who will do what, the steps or phases of the action, defined criteria or implementation levels, and related documentation.

For both cybersecurity and privacy business operations, policies and procedures identify acceptable practices and expectations, as well as guidance for how to train personnel on those requirements and expectations. CPLP policies and procedures should align with broader organizational policies and clearly describe the expectations of the learning programs.

The benefits of establishing policies and procedures include:

- Clear expectations for the workforce throughout the organization
- Documented executive support for the program
- Auditable management and oversight capabilities
- Identified cybersecurity and privacy assurance strategic goals and objectives
- Clearly identified CPLP information and resources
- A structured approach to training personnel on their cybersecurity and privacy responsibilities
- Documentation of the evolution of a cybersecurity and privacy culture

2.2.1. Examples of Learning Program Policy Statements

The following example policy statements provide context on what is important when establishing, reviewing, or updating CPLP policies.

- The CIO and CISO must establish a cybersecurity training program for users of [organization] information systems.
- The CPO must establish a privacy training program for users of [organization] data.[9]
- All personnel, contractors, or others who work on behalf of [organization] accessing [organization] systems must receive initial training and regular refresher training in cybersecurity and privacy awareness and accepted cybersecurity and privacy practices

[9] OMB Circular A-130 [3] includes responsibilities for protecting federal information resources and managing PII. However, each federal organization may choose other language to refer to the same concept. This document aligns with the NIST Privacy Framework and adopts the term “data” to include information involved in data processing about individuals. Organizations should consult with their legal advisors to determine their preferred language.

- Personnel must complete cybersecurity and privacy awareness training within 24 hours of being granted a user account. If a user fails to meet this training requirement, user access will not be granted or will be suspended.
- All personnel, contractors, or others who work on behalf of [organization] with significant security responsibilities must receive role-based training prior to obtaining access to systems that process sensitive information and will be required to complete refresher training each fiscal year.
- User accounts and access privileges, including access to email, must be disabled for employees who have not completed required refresher training unless a waiver is granted by the CISO, the CISO's delegates, or the information systems security manager (ISSM).
- Privacy managers, the CISO, and ISSMs must prepare and submit required awareness and role-based training plans.
- Privacy managers, the CISO, and ISSMs must prepare and submit reports on workforce behavioral changes, attitudinal measures, and other metrics associated with developing cybersecurity and privacy cultural norms with content, frequency, format, and distribution at the request of the CPO and CIO.
- The CISO or their delegates must regularly review information security awareness and role-based training programs.

SP 800-53r5 [11] control AT-1 describes the policies and procedures for cybersecurity and privacy awareness and training (learning) programs.

2.3. Aligning Strategies, Goals, Objectives, and Tactics

Organizations can utilize a variety of techniques to identify and describe the steps needed to implement a program. One method is to begin by identifying the organization's goals, the objectives to meet those goals, and the operational tactics to meet those objectives. Each goal should have objectives that will often include measurable targets, such as identifying who needs role-based training or training a percentage of the organization by a specified date. It is a best practice to choose "SMART" goals: specific, measurable, achievable, relevant, and time-bound. Each program objective will have tactics associated with them. Tactics are tools, methods, or mechanisms that enable the program to pursue the objective identified in the plan's strategy. Ultimately, every individual item in the plan — down to the most detailed tactical level — can be traced back to where it originates in the overall strategy. Every activity should support the overall CPLP strategy. Managing the steps to implement CPLPs and ensure that the program meets organizational learning needs requires discipline on the part of the team.

Table 1 outlines a model for the strategy, including goals, objectives, and tactics.

Table 1. Elements of a CPLP strategy

Element	Description
Strategic Plan	CPLP managers meet to set or reset priorities and develop the CPLP strategic plan.
Strategic Goals	Define distinct elements of the strategic plan around which to organize the program, such as decreasing susceptibility to social engineering attacks, identifying when to apply privacy risk management measures, increasing the adoption of multi-factor authentication, or including scenario-based training activities.
Objectives	Based on the strategic goals, develop objectives that include distinct measurable outcomes, and the types of metrics associated with the program element.
Tactic	Based on the objectives, develop tactics to achieve the program objectives in part or in full, such as a phishing exercise to promote awareness of social engineering attacks, enterprise-wide newsletters or other announcement mediums, webinars on multi-factor authentication basics and procedures, or brainstorming sessions with SMEs on scenario development.

The following two scenarios demonstrate each of the implementation steps.

2.3.1. Scenario 1: Protecting Sensitive Printed Data

A physical security review of an area in the organization where sensitive data is routinely handled by many employees finds that basic steps are not being taken to maintain a "clean desk." The privacy policy requires files that contain sensitive data to be kept in folders in locked cabinets. During the review, printed files that contained sensitive data were located in paper stacks and folders that were loosely placed on top of the desks.

The CPLP manager seeks to improve the handling of printed sensitive data and ensure that personnel follow the protection requirements. They determine that a fresh, eye-catching awareness flier or poster might encourage better employee adherence to the policy and reduce this risk.

An executive offers available funding dedicated to producing printed materials. The CPLP manager can utilize that funding to print "Keep It Clean" stickers to attach to work folders and provide a case of such folders to each member of the workforce in the area that handles sensitive data.

In this example, the CPLP manager continually monitored the workplace and risks, coordinated the budget, planned the printing of the stickers, and worked with management to deliver the materials. Because this is a one-time issue, the planning steps were streamlined under the existing program.

- ***Strategic Plan —*** Meet privacy compliance requirements.
- ***Strategic Goal —*** Support the organization's privacy program.
- ***Objective —*** Ensure that all employees who handle sensitive data are trained and aware of their privacy responsibilities.
- ***Tactic —*** Provide "Keep It Clean" stickers for folders in areas of the organization where sensitive data is processed.

2.3.2. Scenario 2: Developing a New Regulation-Required Training Program

A new regulation requires all cybersecurity professionals to implement a specific procedure in their daily routines.

The CPLP manager works with the cybersecurity policy owners to understand and interpret the regulation. Together, they define a strategy with goals, objectives, and a set of program tactics to provide new training to all members of the workforce and meet the new requirements with specific new procedures. The CPLP manager decides to work with organizational training staff to create an online experience that would also enable remote workers to fully participate.

As the course is being completed, the CPLP manager works with organizational leaders and management to identify expected measures of completion and success and to ensure that all necessary members of the workforce are identified and trained. As an element of continuous monitoring, the CPLP manager works with the learning office and leadership to test the completion and success of the training.

- ***Strategic Plan —*** Enable all cybersecurity professionals to recognize their responsibilities and develop the necessary skills to meet new regulatory requirements.
- ***Strategic Goal —*** Update training for all cybersecurity professionals that complies with the new regulatory requirements.
- ***Objective —*** Launch (or update) an online training program that will enable all cybersecurity professionals to meet the training objectives on the specific procedure in the new regulations, even from remote work locations.
- ***Tactic —*** Work with management to schedule the training and ensure 100 % compliance and develop a continuous monitoring program to test completion rates and provide daily tracking data to managers.

2.4. Determining CPLP Measurements and Metrics

Program measurements and metrics are the key drivers for the Assessment and Improvement phase of the CPLP life cycle (see Sec. 1.3). CPLP measurements enable an organization to describe and quantify the learning program, show the effectiveness and impact of the program, understand where changes are required for success, meet budgetary and resource requirements, and make data-driven decisions. Through the development and monitoring of CPLP measurements, an organization can better address their learning goals and resources.

For CPLP purposes, it is necessary to differentiate between quantitative and qualitative measurements. A quantitative measurement is assessed by assigning a number or category to an object to describe an attribute of that object, such as using a 1-5 scale to assess the effectiveness of learning content. For example, a post-learning program assessment instruction might state: “Rate your knowledge level of social engineering exploits on a scale of 1-5, where 1 is a low level of knowledge and 5 is a high level of knowledge.” Such a measurement enables the learning content to be evaluated with an average or mean score.

A qualitative measurement is based on descriptive data, for example, data collected through observations, interviews, focus groups, or open-ended text fields in surveys.

2.4.1. Measurements

Developing and establishing CPLP measurements requires careful consideration and should be driven by the program's goals and objectives as well as any regulatory requirements. CPLP managers should be prepared to answer some common questions, such as:

- What laws, policies, and regulations apply to our organization?
- How often is reporting required?
- What data is required in the report?
- What data for potential audits are we required to maintain and for what length of time?

The CPLP manager should identify how the measurements will be collected, how frequently, who should have access to the measurements, and how the reports will be documented and shared. While laws, regulations, and policies often set specific measurable requirements, CPLP measurements must go beyond simply achieving compliance. The CPLP's impact on workforce capabilities, attitude, and behavioral changes must also be measured.

The measurements and metrics should be tied directly to the *learning goals*, *objectives*, and *outcomes* of the CPLP program and organization. While these terms are often used interchangeably, they each have a specific meaning with regard to the designation and collection of measurements and metrics. Whether it is at the organizational, course, module, or lesson level, these terms retain their distinct meanings. For clarification, this document provides the following high-level definitions for these terms and describes how they are used in the learning community:

- **Goal:** The goal is a general statement written from the organizational or instructional team perspective that describes the intended competency and desired tasks, knowledge, and/or skills that a participant will learn from the activity.
- **Objective:** The objectives are specific statements written from the organizational or instructional team perspective that describe what the developer wants the participant to do after completing the learning activity. Objectives typically relate to the specific subject or content that the instructional material will cover.
- **Outcome:** Learning outcomes are learner-centered and describe how the learner will be evaluated. The written learning outcomes should be measurable, achievable, and outcome-based. A general formula for writing learning outcomes is:
    - After participating in the learning activity, learners will be able to (*insert measurable verb*) and (*insert learning statement*).

Table 2 shows examples of learning goals, objectives, and outcomes and how their differences impact the generation of measurements for a program.

Table 2. Examples of learning goals, objectives, and outcomes

Learning Term	Perspective	Assessment Method	Measurement	Measurement Technique (quantitative and qualitative)
Goal: Help learners understand the benefits of using approved generative artificial intelligence (AI) tools that are relevant to their work role	Organization, Instructional Design Team, or Instructor	Assessed by the organization or learning team by looking at the learning content	Did the course content provide learners with an understanding of the benefits of using AI?	Presenter and program feedback, open-ended surveys, reports from participants
Objective: Teach learners how to (1) identify approved generative AI tools, (2) select the appropriate generative AI tool that is relevant to their work role, and (3) use the approved generative AI tool to enhance their work duties	Organization, Instructional Design Team, or Instructor	Assessed by the organization or learning team by looking at the learning content	Were generative AI tools covered in the learning material? Were decision criteria presented by work roles? Were benefits per AI tool presented?	Presenter and program feedback, open-ended surveys, reports from participants, observations of learning program participants
Outcome: Teach learners how to access approved generative AI tools and create a generative AI activity relevant to their work role	Learner	Assessed by the organization or learning team to determine the learner's ability to demonstrate their new knowledge or skills	Was the learner able to access AI tools and use the tools to create an AI activity?	Interactive assessments, quizzes, lab-based demonstrations, oral evaluations, and observations of learning program participants

CPLP managers should build programs with efficient data gathering techniques to provide effective reporting information. This will likely include collecting data on employees that may carry a heightened sensitivity due to context (e.g., training records are often part of employment or contract records and can be tied to performance evaluations or result in consequences for failure to take required training). CPLP managers must identify and manage the cybersecurity and privacy risks associated with processing learning data, including risks associated with learning management systems (LMSs) and reporting practices.

2.4.1.1. Quantitative Measurements

Quantitative measurements are expressed in numerical form and are usually referred to as objective data. The combination of quantitative and qualitative measurements provides a holistic understanding of the CPLP.

Some common examples of quantitative learning program data include:

- Training attendance, performance assessments, and completion rates
- Closed-ended employee survey feedback
- Cost of development and delivery per participant
- Usage of online or other digital learning programs, such as the number of logins, time spent online accessing the content, and how often the site or content is accessed
- Tracking the number of participants who attempted and obtained commercial certifications
- Cybersecurity incident data limited to employee-generated incidents or topics that can be mitigated or addressed in the learning programs
- Metrics on incident reporting that demonstrate employee ability to recognize and report potential cybersecurity events
- Phishing or other simulated attack response tracking
- Longitudinal data that depicts program impacts, including employee behavior change, over time (e.g., employee implementation of operating system updates in a timely fashion, increased adoption of multi-factor authentication, adherence to password management rules)
- Employee testing data before the learning program, immediately after the learning program, and three months after attending the course to assess knowledge retention
- Performance data by department, including technical performance measurements
- Frequency of updating the training material to evaluate relevancy
- Extent of cybersecurity or privacy events, such as reduced downtime or outages due to events (these may be indicators for role-based training)
- Ability to recognize and report privacy information disclosures or misuse, as evidenced by employee adoption of reporting tools
- Changes following technical training may also provide measurements, such as reduction of accounts with privileged access, identification of high-value assets, new network segmentation, or additional controls written in acquisition and budget documentation

2.4.1.2. Qualitative Measurements

Qualitative measurements are based on descriptive data, for example, data collected through observations, interviews, focus groups, or open-ended text fields in surveys and can provide insight into the learning experience.

Some common examples of qualitative learning program data include:

- Instructor/presenter observations and feedback

- Attitude surveys related to workforce support for the cybersecurity and privacy culture
- Open-ended feedback or survey fields
- Detailed reports from participants, such as written feedback sent to the program
- Focus group discussions with participants, instructors, or other stakeholders
- Observations of learning program instruction and interactions
- Observations and analyses of instructional case studies
- Interviews with participants, instructors, or other stakeholders
- Suggestion box submissions

2.4.2. From Measurements to Metrics

Developing metrics can be one of the most important yet challenging parts of the CPLP effort. How the organization defines and collects measurements will lead to the definition and analysis of the metrics. An effective set of metrics can help improve content quality and learner engagement, obtain support from the organization, increase funding, reveal impacts on the cybersecurity and privacy risk management program, and demonstrate returns on investment. In recent learning program research efforts by NIST, participants reported [6] that despite best intentions, their organizations often used a limited number of metrics that did not provide a complete view of program effectiveness.

The following examples show how measurements provide the data for metrics:

Course Attendance

- Metric: The percentage of learners who registered and attended the learning course
- Measurements: Registration and attendance records (quantitative)
- Analysis: Identify differences or trends in how many learners registered versus how many attended

Course Completion

- Metric: The percentage and attributes of learners who completed the learning course
- Measurement: The number of learners, their work roles, and their organization, who attended and completed a course (quantitative)
- Analysis: Identify differences or trends in how many learners attended and how many of those in attendance completed the course

Engagement During Courses

- Metric: The level of interaction from participants, such as how many engaged in discussions or completed interactive elements

- Measurement: Number of learners who participated in group activities or lab activities (quantitative), comments and feedback received from learners (qualitative), and how many participants posed questions or participated in chat features (quantitative)
- Analysis: Identify trends based on how many learners participated in engagement activities and whether there was positive or negative feedback from participants about the activity

Course Cost per Participant

- Metric: The cost of the program compared with the number of participants who attended the course
- Measurement: The cost of the course (quantitative) and the number who attended the course (quantitative)
- Analysis: Identify cost effectiveness by reviewing attendance versus costs

Behavior Change per Participant

- Metric: Percentage of participants who changed a behavior in the workplace (e.g., reported a suspected phishing email)
- Measurement: Number of participants who received a phishing test email and reported it appropriately (quantitative)
- Analysis: Identify the impact of training on recognizing phishing emails and how they are reported

CPLP managers rely on CPLP measurements and metrics to assess the effectiveness of their learning programs and ensure that the learning outcomes are achieved. SP 800-55v1 [12] provides guidance on the selection and aggregation of information security measurements and the development of an information security measurement program.

2.5. Learning Program Audience Segments

When considering the organizational personnel whose learning objectives will be addressed with the CPLP, it is recommended to view each individual as belonging to one or more learning program audience segment. Every person who participates in the CPLP is counted in the "all users" group. The second group includes privileged access account holders who have organization-approved access to restricted systems or data that requires special care. These individuals will receive additional cybersecurity and privacy training to minimize risks to systems and data. The third group includes employees and contractors with significant cybersecurity and/or privacy responsibilities who require an individualized program of role-based training to ensure that their knowledge and skills are sufficient to execute the tasks required for their work. There will likely be some overlap between the privileged access account holders and those with significant cybersecurity and/or privacy responsibilities. Figure 4 shows the groups and how they overlap.

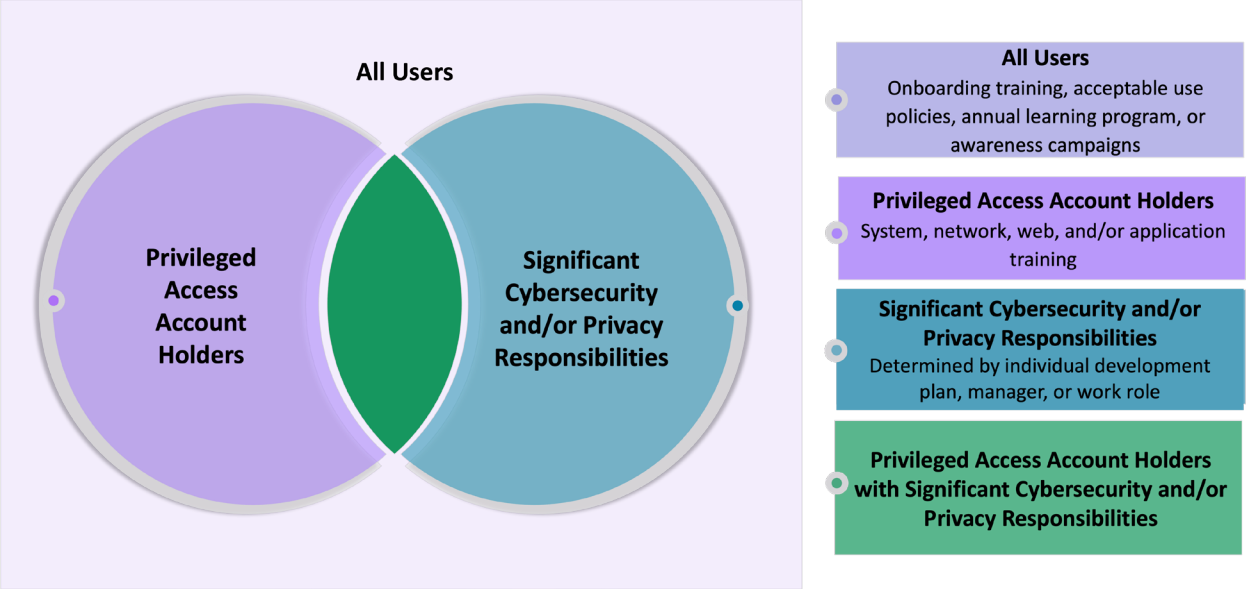

Fig. 4. CPLP learning program audience segments

2.5.1. All Users

In a typical scenario, all of the organization's personnel will participate in the CPLP, agree to abide by the acceptable use policy or standards of behavior, complete the recurring[10] learning program training, and attend, complete, view, and receive the other various ongoing program elements.

SP 800-53r5 [11] control AT-2, Awareness and Training, refers to "all user" training as cybersecurity and privacy "literacy" training. As part of or after completing the recurring training, users will sign a rules of behavior policy that defines the behaviors required to gain and keep system access. SP 800-53r5 also indicates that the training will need to be updated for any system changes or following any organization-defined events:

> Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, Executive Orders, directives, regulations, policies, standards, and guidelines.

All users in the workforce (commonly referred to as "system users" and "general users") are critical to reducing unintentional errors and vulnerabilities. The organization's personnel may

[10] Federal agencies and organizations should refer to current FISMA requirements to determine frequency of the All User programs.

include full-time and part-time employees, contractors, consultants, foreign or domestic guest researchers, visitors, guests, other agency personnel, and other collaborators or associates who require access. All users must:

- Understand and comply with the organization's cybersecurity, physical security, and privacy policies and procedures
- Understand and accept the rules of behavior for the systems and applications to which they have access
- Work with management to meet training needs
- Be aware of actions they can take to better protect their organization's information and environment

Examples of topics that the CPLP may address include:

- Understanding how cybersecurity and privacy activities support the organization's mission and business objectives
- Using proper passwords or multi-factor authentication
- Handling data
- Using AI or other enterprise tools
- Learning remote access procedures
- Collecting and protecting PII
- Reporting any suspected incidents or violations of cybersecurity and privacy policies
- Following the rules established to avoid social engineering attacks (e.g., ransomware and phishing) and to deter the spread of spam and malware
- Identifying and addressing privacy risks during information processing
- Knowing where to find the organization's cybersecurity and privacy resources and points of contact

The organization may also be able to identify those who are subject to or who pose greater human risk due to their role, the applications they use, or simply because they have not yet committed to adopting best practices for cybersecurity and privacy. The CPLP manager — in consultation with the individual's manager and the IT department — should develop additional mechanisms for identifying risky behaviors and metrics for evaluating participation in the "all user" learning program and consider ways to incentivize behavioral change in positive, non-punitive ways.

2.5.2. Privileged Access Account Holders

Individuals with privileged access accounts are trusted with additional access or responsibilities to perform functions that ordinary users are not authorized to perform, such as configuring network management and granting system access (e.g., system administration privileges). Due

to their ability to access critical resources, privileged access account holders require additional training to ensure that they understand their account access privileges and do not accidently cause or exploit vulnerabilities or misuse data. For each type of privileged access account, the CPLP manager must coordinate training with the account holder's manager or supervisor, human capital officer, and training managers to ensure that training is delivered and kept current.

2.5.3. Staff With Significant Cybersecurity and/or Privacy Responsibilities

Personnel with significant cybersecurity and/or privacy responsibilities — including some privileged access account holders (e.g., "super users") — have rights or access to sensitive or critical systems and will require additional training. For example, a manager of an HR environment who ensures that the system is properly configured and available or a Chief Human Capital Officer (CHCO) who collaborates on setting policies for the system will have significant cybersecurity and privacy responsibilities. Network and IT administrators who manage the system and network access are privileged access account holders. If their work roles include monitoring for data loss or other privacy and cybersecurity issues, then they also have significant cybersecurity and/or privacy responsibilities that require additional role-based training. This access can be rescinded when a holder's work role changes.

SP 800-53r5 [11] control AT-3, Role-Based Training, provides a definition for the training required:

> Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies.

This training is typically associated with job duties determined by organizational leaders (e.g., the agency's CIO, CPO, or CISO) and the employee's manager or supervisor and is documented in the employee's performance plan. Personnel in these work roles may require professional development to maintain their status or memberships, such as annual certifications or courses. Examples of typical role-based training recipients include the CISO, privacy officers, cybersecurity managers, cybersecurity and privacy analysts, and incident responders. Cybersecurity work roles and competency areas are explored in SP 800-181r1 [5], which describes the knowledge, skills, and tasks associated with cybersecurity-related work.

2.5.4. Determining Who Has Significant Cybersecurity and/or Privacy Responsibilities

FISMA [2] requires personnel with significant cybersecurity and/or privacy responsibilities to receive role-based training. Additional guidance can be found in SP 800-37r2 [10], SP 800-53r5

[11], and SP 800-181r1 [5]. In combination, these documents assist with the identification of roles and functions in the cybersecurity workforce that require role-based training.

Determining who in the organization will participate in role-based training is a multi-step process that begins with defining the significant cybersecurity and privacy work roles in the organization and identifying the staff who are aligned with the designated work roles. Often, the determination begins with senior leadership and direction from the office of the CIO, CISO, or CPO in partnership with HR. CPLP managers should participate closely in this effort to identify those with significant cybersecurity and privacy responsibilities.

These work roles should also be included in position descriptions, hierarchy charts, and responsibilities to show how the work required to achieve a particular objective has been identified. Individuals may assume additional work roles based on their particular skills, organizational policies regarding cross-training, and organizational staffing levels. SP 800-181r1 [5] identifies work roles for cybersecurity and is a detailed lexicon for understanding the related knowledge and skills that are typical for such roles.

2.6. Determining Scope and Complexity

The ultimate goal of a CPLP is to reduce cybersecurity and privacy risks to the organization through cultural and behavioral changes, not simply to achieve compliance.

The complexity of the material must be determined before development begins and be commensurate with the role of the person who will undergo the learning effort. Material should be developed based on two important criteria: 1) the target attendee's role and 2) the cybersecurity and privacy responsibilities required for that role. This will require coordination with HR and CLOs (or equivalent). Individuals who receive training will appreciate the effort made to ensure that they understand the material in a manner appropriate to their learning needs and the nature of the work that they do.

2.7. CPLP Elements

A typical CPLP includes a variety of learning program elements that are delivered to diverse audiences through various platforms and methods. CPLP managers will identify the necessary and most effective types of program elements for each audience type per learning goal and adjust their selections to match their available budget and schedule considerations.

The typical CPLP elements are:

- Awareness activities
- Experiential learning and practical exercises
- Training

Employees may initially believe that the CPLP is the annual or regularly scheduled training course or event delivered to all users, which may include informal department programs, a mandatory presentation delivered in an auditorium, or an online course. Other learning

program elements are targeted for those with significant cybersecurity and/or privacy responsibilities and those who are privileged access account holders. A CPLP program will consist of the mandatory elements (required by policy and learning objectives for all CPLP learning participants) and the many other activities implemented throughout the CPLP life cycle to reinforce these messages.

Regardless of the learning activity, the learning goal for these events is to ensure that personnel are aware of their roles and responsibilities for protecting information and assets and are able to take appropriate action to respond to a variety of cybersecurity and privacy risks.

2.7.1. Awareness Activities

Cybersecurity and privacy awareness learning activities should be conducted on an ongoing basis throughout the year to ensure that employees are aware of their roles within the organization and the appropriate steps they must take to protect information, assets, and individuals' privacy. Activities can be campaign-oriented or ad hoc based on the subject matter, threats, or vulnerabilities or take place during seasonal events.

Examples of awareness activities that are appropriate for all users include:

- Messages on logon screens, organizational screen savers, and email signature blocks
- Employee newsletters with cybersecurity and privacy articles
- Posters (physical or digital) with cybersecurity and privacy tips
- A Cybersecurity Awareness Month (October) or Data Privacy Awareness Week (January) activity fair
- Cybersecurity and privacy reminders and tips on employee materials (e.g., pens, notepads, etc.)
- Periodic or as-needed email messages that provide timely tips or are sent in response to a cybersecurity or privacy event or issue

2.7.2. Experiential Learning

Experiential learning activities or practical exercises are specific learning scenarios that simulate events and incidents. The practical exercises can include social engineering efforts (e.g., phishing, smishing, and vishing) in the form of simulations, learning games, quizzes on identifying and processing data, tabletop exercises, hands-on virtual lab exercises, contingency plan and disaster recovery scenarios, and attack or defend scenarios conducted in cyber ranges.

For example, in an organization-wide all-user phishing exercise, a "tricky" email is sent to users to see whether they can spot a phishing attempt or if they can be tricked into clicking on a link to a malicious website or opening an infected attachment. Phishing exercises can also target learning for those in specific roles, such as leadership or known administrators. Begin by determining the current click rates for a specific group of users or by work roles to understand if there is a need for more targeted training. The NIST Phish Scale can be helpful in identifying

and measuring behaviors for phishing threats.[11] These exercises offer opportunities to collect metrics and measurements, which are usually referred to as "click-through" or reported measurements. These types of measurements indicate whether the user reported the email as a phishing attempt or whether they clicked on a link or opened an attachment. Some organizations include "report phishing" capabilities on their email platform (e.g., a button on the platform's menu) to encourage best practices.

The organization's legal team should be included in the design and review of planned phishing exercises to avoid negative impacts, such as using legitimate brands or naming federal organizations in the phishing "bait," which could result in emails or calls to those entities. In addition, since employees may not like being tricked, it is important to tell employees that the organization is conducting phishing exercises on a random basis and that the results will be used to guide future learning activities. These activities should not be punitive, nor should any employee be called out for their response. When viewed as learning opportunities, the phishing exercises can provide important data on vulnerabilities and which employees may need additional learning support.

Other experiential learning exercises may be better suited for those with significant cybersecurity or privacy responsibilities (e.g., role-based training), such as tabletop exercises and contingency plan scenarios. Additional examples may be found in NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities* [13].

2.7.3. Training Content

Training is a broad term that includes the learning program content designed to increase or improve job-related knowledge and skills. Some of the techniques that an organization can employ include:

- **Synchronous training:** Instructors and learners participate together in a virtual or physical classroom-based learning environment.
- **Asynchronous training:** The learner can access material individually and on demand. This is sometimes called "self-paced" because the learner accesses content based on their schedule.
- **Virtual-led:** Instruction occurs in a virtual or simulated environment and is presented or facilitated by an instructor in real time.
- **Cyber range:** Instruction takes place in a safe, web-based practice environment (i.e., sandbox) and delivers hands-on realistic training, scenarios, challenges, and exercises.
- **Podcasts:** Learning is asynchronous, self-paced, and audio-based.
- **Animations:** Animations can visually represent a process, system, or complex cybersecurity or privacy concept.

[11] The NIST Phish Scale considers employee context in its method for determining the difficulty of a simulated phishing email. See additional information https://doi.org/10.6028/NIST.TN.2276 .

- **Demonstration:** The instructor provides the learner with the step-by-step actions of a process or activity. This can be delivered in-person, recorded, or via other methods.
- **Scenario-based exercise:** The facilitator leads discussions on topical, situation-driven scenarios that may be customized to the organization or a specific department. These are also referred to as "tabletop" exercises.
- **Self-paced online training:** This asynchronous technique is currently popular for distributed environments. Attendees of a web-based session can study independently and learn at their own pace. Testing and accountability features can gauge performance. Web-based training can include video, audio, and interactive techniques, such as drag-and-drop or fill-in-the-blank exam responses.
- **On-site instructor-led training:** This is one of the oldest and most popular techniques for delivering training material to an audience. The biggest advantage of this technique is the interactive nature of the instruction. It can also include peer presentations and mentoring.

Blending various training delivery techniques can be an effective way to present material and hold an audience's attention. For example, showing videos during an instructor-led session allows the audience to focus on a different source of information. The video can also reinforce what the instructor has been presenting.

2.8. Establishing the CPLP Plan Priorities

During the planning phase of the CPLP life cycle, evaluate the organization's critical risk factors to determine the learning priorities. If a phased approach is necessary due to budget constraints or resource availability, some factors to consider are:

- **Role and organizational impact —** It is very common to address priority in terms of organizational roles and risks. Broad-based awareness initiatives that address the enterprise-wide mandate may receive high priority because the rules of good cybersecurity and privacy practices can be delivered to the workforce quickly. It is also common to look at *high-trust/high-impact* positions (see Sec. 1.6) and ensure that they receive high priority in the rollout strategy. These types of positions are typically commensurate with the type of access that these users possess, or the specialized requirements assigned to their roles and job duties. In addition, the protection of high-value or critical assets or the deployment of privacy-sensitive products or services can also drive priorities.
- **State of current compliance —** This involves looking at major gaps in the CPLP (e.g., gap analysis) and targeting deficient areas for attention.
- **Availability of materials and resources —** Determine whether appropriate learning materials and necessary resources are readily available for the program element. Repurpose and utilize existing materials in new ways, when possible.

2.9. Developing the CPLP Plan

The CPLP plan defines sufficiently detailed program elements that support the strategy for each activity or campaign. Many organizations utilize standard program plan templates that provide baselines for organizational expectations. The exact level of detail within the plan will vary, depending on organizational and program requirements and resources. As the program matures, the CPLP manager should conduct recurring reviews (i.e., at least annually) of the plan, along with the stakeholders and individuals who will support and manage the program.

2.10. CPLP Resources

An important element of developing the CPLP strategy is to determine what currently exists within the organization and what resources are dedicated to existing programs. If the learning program does not yet exist or requires significant redesign or updates, refer to the program strategy process (outlined in Sec. 2.1) to review the most important program elements for inclusion. Resources are typically defined as any asset that is required to meet goals and objectives, such as people, materials, equipment, and technology. An important consideration in obtaining resources is establishing a CPLP budget.

2.10.1. Establishing a CPLP Budget

Once the CPLP strategy has been approved by senior leadership (identified in Sec. 1.6.2) and priorities have been established, funding requirements must be added to the plan. A determination must be made regarding the extent of funding support to be allocated based on the strategic goals. Senior leadership should help the CPLP manager understand or establish their budget. While each program will have different funding needs, some typical costs include:

- Training personnel, such as program managers, instructional designers, instructors, graphic artists, web developers, and programmers
- Classroom space and materials, such as whiteboards, markers, erasers, flip charts, note pads, pens, pencils, and name cards
- Printed program materials, handouts, and certificates or electronic distribution that may require web-based platforms
- Online (i.e., virtual) space to distribute materials, including synchronous activities (e.g., webinars) and asynchronous activities (e.g., job aids, recorded sessions, and web-based content)
- LMSs for content delivery, participant registration, and course completion records
- Licenses (per seat) for learning platforms or content
- Awareness materials, such as posters, notepads, and themed items for awareness activities
- Professional services for curriculum design and development and the presentation of content

- Privacy and cybersecurity culture mapping efforts

Organizations with a limited (or even no additional) budget for cybersecurity and privacy initiatives can still establish an effective CPLP by leveraging existing resources, implementing cost-effective monitoring solutions, and prioritizing cybersecurity and privacy as a shared responsibility across the organization. Some materials may be available from other federal agencies, partner organizations, or online vendor resources. Some materials may already exist in-house and should be inventoried and evaluated to determine whether they are current and meet the existing learning goals. The implementation timeline will help indicate when additional funding may be required to support tools, major curriculum and content deliverables, new staffing requirements, and other learning program elements and activities.

The following are example questions that can help guide the development of budget requirements:

- What mission and business needs will be influenced or impacted?
- Are there regulations, legislative requirements, or other internal or external requirements that would influence the decision?
- What shared federal or other external resources can be leveraged?
- What internal resources can be leveraged? This can include existing content and delivery mediums.
- Is it more cost-effective to develop the material in-house versus outsourcing?
- Is the learning requirement specific to the organization or the system? This would include policies, procedures, or rules of behavior.
- When must the learning material be ready? Are there critical schedules that need to be met? Would outsourcing allow for delivery schedules to be met?
- How many people need to be trained?
- How often will the material need to be updated?
- What delivery mediums will be required, and what are the associated costs?
- Are there in-house resources to do the job?
- Does the organization have the subject-matter expertise to provide content for the training?
- Are resources available to effectively manage and monitor contractor activity during acquisitions?
- Does the course sensitivity preclude the use of a contractor?
- What is the cost in staff time, and how can the CPLP achieve the desired results while maximizing its return on investment (ROI)?

CPLP managers must work with senior leadership to advocate for the program against competing priorities, budget constraints, and staff time costs and to develop a strategy to address any shortfall in funding that may impact the organization's ability to meet its learning goals. This may require adjusting the learning strategy to be more in line with the available budget, advocating for additional funding, or reallocating current resources. It may also mean that the program plan needs to be phased in over some predefined time period as funding becomes available.

2.10.2. CPLP Staff and Locations

Those who have managed federal CPLPs report that training the workforce requires a combination of technical knowledge and professional attributes, such as communication, creativity, and interpersonal skills [7]. If the organization does not have the budget for CPLP course developers, research what other agencies or organizations of similar size have done to meet their own needs. Some organizations may have in-house instructional designers, curriculum developers, instructors, web developers, communications experts, and graphic designers. Other organizations may need to include these professional costs in the budget for a new project and identify qualified contractors or external courses.

Different information requires different methods of delivery. Some program elements will be appropriate to deliver via online learning, while others will necessitate both instructors and physical classroom locations. Determining these requirements in the planning stage will allow for appropriate resource allocation (e.g., rooms to be reserved, computers and projectors secured, etc.). Even posters and flyers require space considerations, as they will need to be displayed in a sufficiently prominent area to have a learning impact on personnel.

2.11. Communicating the Strategic Plan and Program Performance

One of the most important aspects of executing the CPLP strategic plan is collaborating with the learning team, key stakeholders, senior leadership, and personnel. Involving stakeholders and employees during the planning process can lead to greater success as the program begins and as each program element is implemented. Determining what to communicate should focus on:

- How the CPLP helps meet organizational and learning goals
- How the CPLP elements will impact personnel
- Engaging with stakeholders to identify concerns or conflicts in advance
- Soliciting feedback to identify gaps or missing elements in the plan
- Supporting ongoing efforts to develop a cybersecurity and privacy culture

Obtaining early and continual support for the strategic plan is important to keep the momentum for the CPLP strong and inspire engagement and satisfaction with the plan. A solid communication strategy will address those needs. Consider whether the organization has a centralized communications department or whether communications decisions will be made at the business unit level. Then develop a communications plan (or incorporate these elements

into an existing communications plan) to share information about the new or updated CPLP. Keep it simple and tailored to internal stakeholders. The CPLP manager may choose to create a custom version of the strategic plan that includes different information for different audiences.

Some important elements to share include information about what the CPLP is and who manages it. Funding issues and gaps may also need to be identified and addressed. For example, agency leaders and managers need to know whether the cost to implement the CPLP activities will be funded by the CIO, CISO, CLO, or another program budget or whether their budgets will be impacted to cover a portion of the expense. In addition, schedules and completion requirements must be communicated.

The CPLP communications plan should include:

- An overview of the CPLP strategy and ownership
- Goals, objectives, and assessment processes
- A list of key roles and their respective responsibilities, including:
    - Senior leadership and executives
    - Managers and supervisors
    - HR, Office of the CHCO, and labor relations
    - Office of the Chief Financial Officer (CFO) or budget analyst
    - CLO (agency or organization level)
    - CPLP managers and team members
    - SMEs
- Budget overview
- Key deliverables and high-level schedule
- Measurements and metrics
- Reporting methods and frequency

Everyone involved in the implementation of the program must understand their roles and responsibilities. Most organizations may find it helpful to tailor their messaging based on the audience. A few examples of audiences and their roles include:

- **Senior leadership and executives** (e.g., director, CIO, CISO, SAISO, SAOP, CAIO and CPO) **—** Communications may include a high-level summary of the CPLP strategic plan, including the goals for and phases of the year-long program. Senior leadership must understand the overall program so that they can support the allocation of budget and personnel. Ensure that senior leaders are provided with appropriate messaging so that they can avoid harmful language (e.g., “users are the weakest link”).
- **Managers and supervisors —** Communications should emphasize the benefit of building a positive cybersecurity and privacy culture and help managers and supervisors

recognize their crucial role in supporting that culture. Encourage positive associations with allocating time for employee learning.

- **HR, human capital officers, and labor relations officers —** Those involved in HR or human capital are responsible for any required communications regarding the implementation of CPLP requirements into the onboarding and training of employees and contractors throughout the year. For organizations with union members, labor relations officers will also be key stakeholders in assisting with any updates to the plan and receiving reports on learning outcomes and other metrics for their union-represented personnel. Human capital is also a crucial stakeholder to provide input about personnel disciplinary actions and, if necessary, to initiate labor relations and union negotiations with regard to the mandatory training or learning activities outlined in the agency process.
- **Chief Financial Officer (CFO) —** The Office of the CFO (or the organization or agency equivalent senior financial officer) is responsible for approving the CPLP and dispensing funding to the CPLP manager and must, therefore, be kept informed about program implementation and measurements.
- **Chief Learning Officer (CLO) —** The CLO is responsible for education in the organization and may provide the learning infrastructure, such as the LMS or other distribution platforms.
- **Personnel —** Create a communications strategy that allows for direct email messages to personnel and a distributed system to their managers and supervisors. When creating communications materials about the CPLP for individual contributors (e.g., materials in the new hire orientation packages), focus efforts on enabling individual contributors to see their part in the overall CPLP. This should include a schedule to ensure that users are notified in sufficient time before they are required to complete the learning activity.

3. CPLP Analysis and Design

While there are many theories and models for the design and development of training programs, this document focuses on the ADDIE model[12] — a traditional instructional systems design model with five distinct phases:

1. Analysis
2. Design
3. Development
4. Implementation
5. Evaluation

During the analysis phase, the CPLP manager identifies the organizational and learning needs or gaps to determine which audiences will need training and their existing levels of knowledge and skill. It may be necessary to evaluate various work roles for competency gaps so that relevant learning programs can be customized and created based on the specific learning and skill needs for that work role. During the design phase, these gaps are translated into learning objectives, which are the focus of the learning material. Tying the learning objectives to identified knowledge and skills gaps ensures that the end result is relevant and will succeed in addressing the identified learning needs.

3.1. Analysis Phase

The analysis phase is the process during which the CPLP manager determines the organization's learning and performance needs. In this context, the needs (i.e., gaps) are the difference between the current learning goals (or activities) and the desired state. To determine their learning needs, organizations may conduct a formal or informal needs assessment (also referred to as a needs analysis). The primary benefit of the analysis phase is to identify learning needs for the organization and learning audience. Additional benefits include having information that clearly defines the learning needs, support for and prioritization of resources, and the alignment of learning goals to organizational mission goals.

In the beginning of the analysis phase, it may be helpful to identify the primary members of the analysis team, including several additional constituent groups. This may include:

- **Executive management —** These organizational leaders need to understand the relevant regulations, directives, laws, operational changes, or other requirements that form the basis for the CPLP. It is important for leadership to provide input on organizational learning needs since they set the expectations for the program and learners. A key role for CPLP managers is to continually advocate for the program by explaining why analysis is important and how an effective CPLP is part of effective risk management. Additionally, an effective and well-designed CPLP supports the

[12] A modification to this model adds "Planning" as the first step, making it the PADDIE model. It may be helpful to utilize models that help with change management or that use person-centered or human-centered approaches. All have value and should be utilized when appropriate for a specific environment, organization, and desired learning outcome.

development of an organizational culture focused on cybersecurity and privacy protections.

- **Cybersecurity and privacy personnel —** These individuals act as SMEs and consultants for the organization. They identify and help document the knowledge and skills needed to perform the tasks associated with work roles.
- **System owners and program managers —** These individuals will have information on and responsibilities for the particular system in use by the organization. For example, the owner of a system will recognize the potential impacts of learning activities on the personnel tasked with operating that system.
- **Learning program participants or learners —** Representatives from the employee base and different cybersecurity and privacy work roles can provide input on the requirements gathering and analysis process.

3.1.1. Importance of the Analysis Phase

There are many reasons why the analysis phase is rushed or skipped entirely. For example, organizations may think it will take too much time, personnel may be unavailable, or the necessary funding may be lacking. Most often, organizations believe they already know what they need. However, critical problems can arise by skipping the analysis phase, such as:

- Wasted spending when learning materials are developed that do not meet the required knowledge or skills gaps.
- Misunderstanding the knowledge and skills gaps of the learners, which may require personnel, technology, or other resources to remedy.
- Using training to solve an issue that is not a knowledge or skills gap (e.g., an employee is unable to perform "additional as assigned" duties). Conducting an analysis will help determine whether it is a systematic or structural gap rather than a knowledge or skills gap.
- Providing the right personnel with the wrong information, such as giving privileged access account holders only basic training rather than information specific to their additional rights.
- Providing the wrong personnel with the right information, such as giving privileged access account holder training to general users.
- Providing the right information through an ineffective medium or providing the wrong information through an effective medium.
- Repeating the same learning material even if previous efforts have failed.

It may be tempting to skip the time needed to properly analyze the organization's needs. Even if the only option is to conduct an informal discussion and review with a few individuals, it is still important to have the conversation and document what is needed. The analysis phase establishes a clear vision for the next steps of the CPLP's development.

3.1.2. Steps of the Analysis Phase

While there are many ways that CPLP managers can evaluate the learning needs of the organization, the process for identifying learning program needs from a strategic point of view tends to be a repeatable process, regardless of the specific learning goal or audience. The steps are:

1. Identify learning needs based on the work role activities and tasks
2. Identify the learning program audience
3. Match the identified learning needs to each audience
4. Assess the audience's current knowledge and skill level
5. Determine the learning gaps

3.1.2.1. Identify Learning Needs

The most important step in initiating a new phase in the CPLP is to establish the learning needs. For example, the organization may be prepared to introduce new technology, legislation may have been passed that requires personnel to acquire new knowledge or skills, or a new privacy or cybersecurity risk may have emerged that requires the organization to introduce a new learning module. Identifying and prioritizing learning needs will allow the CPLP managers to focus their attention on the issues of greatest importance to the organization.

The following techniques can help define the learning needs:

- Identify what knowledge or skills are needed in the organization through a learning needs assessment.
- Review existing work or job analysis reports.
- Identify any regulatory or other requirements for learning programs.
- Review relevant cybersecurity or privacy risks for the participant audience. All organizations face operational risks. While the majority of risk considerations focus on responding to incidents that result in a failure to maintain cybersecurity, it is important to include an effective learning plan as a mitigation factor for risks.
- Review lessons learned or after-action reports. After an incident, the CPLP manager may be engaged in an effort to educate personnel on corrective best practices. This is an important opportunity to learn from mistakes. New material should be developed that not only speaks to the specifics of the incident but may be able to strengthen weak areas around it, such as identifying and reporting vulnerabilities.

3.1.2.2. Identify the Learning Program Audience

During the analysis phase, the learning program manager will identify and define the audiences to be trained on the learning goals. It may be helpful for supervisors to coordinate with the

organization's cybersecurity and privacy learning function to determine whether personnel need additional training.

Potential learning audiences for the CPLP include:

- **New employees:** This audience includes contractors, and the focus is usually on the important policies and rules of behavior for the systems that they will access. This training includes what is typically called "new employee orientation" or "onboarding" and can be joint cybersecurity and privacy training. Some organizations may need to require visitors and/or guests to sign acceptable use policies if they allow them any type of system access, including use of wireless network connections.
- **All users:** This is also known as "general workforce training" and includes regularly scheduled (often annual but preferably more frequent) cybersecurity and privacy training for all system users, including personnel without access to the system. An analysis of this audience's training requirements should include reviewing the performance of previous program elements and any new organizational requirements.
- **Privileged access account holders:** These are personnel with additional responsibilities who are trusted to perform cybersecurity- or privacy-relevant functions that ordinary users are not authorized to perform. They will require additional training in order to be provided with privileged access accounts. When identifying privileged access account holders, consider:
    - Whether new systems have been implemented or are planned and the rights and privileges associated with privileged access accounts
    - Whether the list of participants with system owners is complete and whether new rights and privileges are required
    - Whether any of these systems have been moved to the cloud and require new training
- **Staff with significant cybersecurity and/or privacy responsibilities training:** Some positions require role-based training for staff with significantly specialized responsibilities. This type of training includes:
    - Specialized or customized training on specific products, networks, systems, applications, or information
    - Work role tasks and activities, such as incident response procedures, oversight responsibilities, or identity management
    - Reskilling and upskilling programs
    - Learning that helps the employee perform their work tasks

The following examples show how personnel can be assigned to multiple learning programs:

- Wilson is currently a system administrator, and as an employee of a federal agency, she attends the annual CPLP training. She is also in the Information Technology department, so she and her team receive additional training on cybersecurity and privacy. In her role

as a system administrator, she has significant cybersecurity and privacy responsibilities and is therefore required to attend additional training.

- Ng is now part of the organization's web publishing team and has access rights to publish the public-facing webpages of the organization. This carries significant agency branding and communications responsibilities. Ng must take annual training and sign an additional Acceptable Use Policy regarding appropriate publishing activities.

3.1.2.3. Match the Identified Learning Needs to Each Audience

The primary knowledge and skillset for the "all users" learning audience segment is the ability to recognize cybersecurity and privacy risks, take appropriate actions to reduce harm to the organization, and report any incidents or events, when appropriate. All users must be empowered and skilled in adhering to the organization's rules of behavior and acceptable use policies, which include guidance on how to use organization-provided devices and access network resources.

Privileged access account holders must be able to judge risks appropriately and use systems that they have been given access to without introducing additional risks or harm to the organization. The NICE Framework [5] can be a useful resource for identifying the necessary role-based knowledge and skills for those with significant cybersecurity or privacy responsibilities. An organizational job analysis will also be useful in determining the learning objectives for program participants. For those with significant privacy responsibilities, the CPLP manager should consult with managers, SMEs, and the privacy senior leadership of the organization (i.e., CPO or SAOP) for additional guidance on the knowledge and skills required of individuals.[13]

There are existing models for evaluating the tasks necessary for a particular person's role, such as considering the complexity or difficulty of the task, its importance, and how frequently the task is performed. This is sometimes referred to as the "DIF model" for considering the relative difficulty, importance, and frequency of the task. It can be helpful for identifying the knowledge and skills that the CPLP should focus on when training those with significant cybersecurity or privacy responsibilities.

3.1.2.4. Assess the Audience's Current Knowledge and Skill Level

The next step in the analysis phase is to determine what the audience segment already knows about the topic and what skills they possess while keeping the learning goal in mind. The CPLP should focus on providing the learner with the requisite amount of new knowledge and skills

[13] The NIST Privacy Workforce Public Working Group is working to identify and document tasks, knowledge, and skills that are aligned with the NIST Privacy Framework. See https://www.nist.gov/privacy-framework/workforce-advancement/privacy-workforce-public-working-group for more information.

while reinforcing existing knowledge and skills. There are several methods for determining the existing knowledge and skill set:

- Hold guided conversations and interviews with SMEs, managers, system owners, and other organizational personnel with relevant mission or business functions
- Review recent job task analyses
- Analyze events and related responses that may indicate skill levels
- Conduct performance-based assessments to evaluate and validate capabilities
- Conduct training with the existing CPLP program elements to establish baseline metrics

These methods can also identify whether new training is needed for a role or whether existing training needs to be updated or modified.

3.1.2.5. Determine the Learning Gaps

Thus far, the analysis measures personnel's existing knowledge and skills with an overview of each audience segment. The difference between that and the ideal state of knowledge and skills for the learning goal is referred to as "the learning gap." During the design phase, the CPLP manager will use information about each learning gap (per learning goal, learning audience, etc.) to design a program specific enough to address each need.

3.2. Design Phase

At the beginning of the design phase, consider what knowledge and skills the audience needs to learn or develop and what gaps the learning material will close. This will drive the creation of the learning objectives and the process for achieving them. The design process should end with a systematic blueprint of the approach needed for the CPLP to address the identified knowledge and skills gaps.

3.2.1. Steps of the Design Phase

The CPLP manager begins a formal design phase for the CPLP or a new element in an ongoing CPLP by creating a Design Document that outlines the requirements. Then it will be necessary to determine whether they need to build or buy learning materials to satisfy those requirements. The steps in the design phase are:

1. Create a Design Document
2. Conduct a survey of available training, both internal and external
3. Identify learning objectives
4. Summarize CPLP or element requirements

3.2.1.1. Creating a Design Document

The Design Document provides a blueprint for the development and implementation of the learning program elements. It is usually created by the CPLP manager and reviewed by key stakeholders (when necessary for funding and other approvals) before moving to the development phase.

Typical elements of a Design Document include:

- Purpose, goals, and background
- Intended audience
- Learning objectives
- Content and available training survey (e.g., build or buy)
- A course outline, including high-level topics (e.g., number of lessons or modules and their length)
- An instructional strategy that includes media (e.g., audio, video, demonstrations, emulations, simulations), activities, and exercises
- Delivery medium (i.e., the learning environment — online, in a classroom, etc.)
- Types of assessments (e.g., participation, quiz with passing grade, performance-based skill assessment, etc.)
- Required measurements and metrics
- Signature page to document acceptance from the key stakeholders

Based on its resources, the organization will determine whether it can build, have built, or utilize existing government or commercial-off-the-shelf (COTS) learning content, which is discussed further in Sec. 4.

3.2.1.2. Conducting a Survey of Available Training

CPLP managers will need to determine what training materials have previously been used in their organization and are still available and appropriate for use. Additionally, there may be materials and programs available from elsewhere in the organization, agency, or partner agencies. Federal resources may have materials, presentations, and even speakers available to satisfy a variety of learning goals. An important result of the survey effort will be insight into what is currently being done to meet learning requirements in the organization and the gap in needed program materials. The content should be adaptable to fit the learning program participants' needs and the organizational context with reasonable effort or costs.

3.2.1.2.1. External Sources of CPLP Materials

There is a variety of external sources of CPLP materials available. Some possible sources include:

- **Vendors:** If the organization decides to outsource some or all of its CPLP course development, a number of vendors in the private sector offer COTS courses that are suitable for particular audiences or that can be developed for specific audiences. Prior to selecting a vendor, agencies should fully understand their CPLP needs, be able to determine whether a prospective vendor's material meets those needs, and consider who "owns" the material for the purposes of future updates and adaptations. The agency contracting officer will help ensure that organizational guidelines are met.
- **Non-profit organizations and grant-based agreements:** Federal organizations may have agreements with non-profit organizations, grants to universities, or other similar arrangements for the creation of educational materials on cybersecurity or privacy topics. CPLP managers should be aware of any such opportunities and leverage these materials.
- **Other organizations:** Organizations can explore CPLP materials that have been developed by other organizations and edit them to fit their needs rather than creating a completely new course. Care should be taken that the available material is applicable to the intended audience and addresses the learning goals of the organization.
- **Shared events and materials:** Federal agencies may offer cybersecurity and privacy learning events that are open to personnel across the Government. CPLP managers should join federal working groups (e.g. Federal Information Security Educators or FISSEA[14]) to remain informed about events, workshops, and conferences intended for professional development.

Sources of timely material may include:

- Email advisories issued by industry-hosted news groups, academic institutions, or the organization's cybersecurity or privacy office
- Cybersecurity or privacy websites
- Themed events, such as Data Privacy Week[15], Cybersecurity Awareness Month[16], or Cybersecurity Career Week[17]
- Conferences, seminars, webinars, forums, and courses

[14] See https://www.nist.gov/itl/applied-cybersecurity/fissea.
[15] See https://staysafeonline.org/programs/data-privacy-week/.
[16] See https://staysafeonline.org/programs/cybersecurity-awareness-month/.
[17] See https://www.nist.gov/itl/applied-cybersecurity/nice/events/cybersecurity-career-week.

3.2.1.2.2. Internal Sources of CPLP Materials

CPLP managers can build new partnerships or reinforce existing ones with the organization's functional managers who coordinate or conduct their own learning programs. Functional training developed in-house (e.g., financial applications or personnel management) often lacks adequate discussion of related cybersecurity and privacy issues. Through these cross-departmental partnerships, CPLP managers can review existing references to topic areas in the materials, check for completeness and accuracy, and assist the functional manager by developing a learning module for any material that previously had no cybersecurity or privacy component.

3.2.1.3. Identifying Learning Objectives: From Analysis to Design

CPLP managers consolidate what they have found in available materials to identify the learning objectives for the CPLP. Whether the CPLP manager is working on the entire plan, designing a few new elements, or updating existing elements, this stage can be very useful in ensuring that the effort is closely aligned with identified organizational needs.

3.2.1.3.1. Examples of Identifying Learning Objectives

Consider the following examples of identified training gaps and their associated learning objectives.

Scenario 1: A recent analysis indicated that on-site, remote, and teleworking employees — including employees with privileged access accounts — are using single-factor authentication (i.e., a password). The CIO has approved the implementation of a multi-factor authentication token system starting with privileged access accounts in the first quarter and all other accounts in the second quarter. The CPLP manager has been tasked with helping employees understand their roles in utilizing this new multi-factor authentication system.

Analysis Phase: Identify Knowledge and Skills Gaps

Since this is a new authentication method, the "all users" and privileged access account holders learning audience segments need information and training on the new policies, processes, and procedures for accessing the system. In addition, they need to know why this effort is important or how it protects the information and assets on enterprise systems. Privileged access account holders will also need additional information focused on the specific privileges they will have once authenticated to the system.

Design Phase: Create Learning Objectives Based on Knowledge and Skills Gaps

The learning goals and objectives for the program must then be established. In this example, the goals and objectives for the learning program involve enabling employees to:

- Understand the vulnerabilities associated with using single-factor authentication (e.g., user ID and password)

- Understand why the organization is adopting a multi-factor authentication token method
- Identify their role in using multi-factor authentication
- Install the authentication application and verify that the token is received
- Utilize the token 100 % of the time for authentication to the system

Scenario 2: A recent external audit of the organization's system privacy policies and practices found that the financial office employees were not adequately protecting the privacy of employee bank information when processing the employees' travel costs.

Analysis Phase: Identify Knowledge and Skills Gaps

During the analysis phase, the learning program manager determined that financial office employees are designated as employees with significant cybersecurity and privacy responsibilities and receive an annual one-hour self-paced training course. Based on the analysis, it was determined that the financial office employees lacked a basic understanding of the policies and procedures for protecting sensitive and privacy-related information. Since this could have immediate and damaging consequences, this lack of knowledge will be addressed with a customized training solution delivered immediately and by including the topic in updates to the annual one-hour self-paced training course.

Design Phase: Create Learning Objectives Based on Knowledge and Skills Gaps

A webinar was scheduled with the financial office employees to provide immediate direction on corrective actions for the protection of sensitive employee bank information. The learning goals and objectives are:

- To be able to describe what is considered sensitive or personally identifiable information, including bank information
- To be able to describe the policies and procedures for protecting sensitive and personally identifiable information
- To be able to adequately protect information while in use and while it is stored on the system when given an online form that contains privacy-related information

3.2.1.4. Summarizing CPLP or Element Requirements

Before moving to the development phase, the CPLP manager must consolidate the requirements for development using the results of the analysis and design phases. It should be possible to fully articulate the competency gaps being targeted by the learning program participant segment and the related learning objectives.

The following CPLP requirements are also important to consider:

- Material should accommodate all learning styles (e.g., online, in-person, repeatable, recorded) and work for different audience types and sizes.
- Program elements should meet accessibility standards.
- Content should be updated and maintained to stay current.
- The diversity of the workforce should be recognized and supported.
- Learning objectives should be provided for any learning element or learning material.
- Learning objectives should be established in accordance with the organizational mission.
- A separate section should be dedicated to each learning objective, and individual lessons for each of the learning objectives should be created.
- Visual elements (e.g., graphics, videos, tables, and other visual tools) should be integrated to reinforce important concepts.
- Interactions should engage the audience and promote their ability to transfer content from the training environment to the workplace.
- Managers and supervisors should be able to check progress, run reports, and access the LMS.
- Required reporting needs for executive leadership should be supported.
- The IT and help desk staff should receive training to support the CPLP.
- If using outsourced courses, vendors should be supported and be able to update the reporting and LMS platforms.

4. CPLP Development and Implementation

In the development phase, each audience's requirements are evaluated, budgeted, and provided for separately. The previously identified audience requirements and learning objectives are the guiding factors for developing the content. Some organizations may have existing and mature awareness, training, and education programs that can provide content or influence the development and implementation phases. Established best practices and lessons learned should be considered when developing the learning content.

The development process will involve various personnel, including:

- **Management:** All levels of management will be responsible for their staff learning needs, the prioritization of training resources, the identification of training gaps, and evaluation of the training's effectiveness.
- **Cybersecurity and privacy specialists and SMEs:** Specialists and SMEs help determine the task, knowledge, and skill requirements of the roles or job functions; identify training gaps and needs within the organization; and guide the development and review of learning materials.
- **Training professionals:** Training professionals acquire, customize, develop, present, and evaluate the training content and training programs. Whether the training team and cybersecurity and privacy teams are in the same department or not, the groups will work closely with other SMEs to ensure that the material and programs are relevant and accurate.
- **Acquisitions and budget:** These departments will be engaged when circumstances and needs require the development or acquisition of externally sourced services or content.

Once the baseline requirements of the program have been solidified, a feedback strategy can be designed and implemented to ensure that materials continue to support the CPLP strategy and address identified training needs.

4.1. Developing CPLP Materials

After the CPLP managers complete their analysis and design reviews, they will have a comprehensive set of design documents to guide the development of new materials. These documents are useful when allocating budgets and personnel for the creation of new materials or program elements. However, additional information will be needed to guide the content creators in their work.

4.1.1. General Guidelines for Developing or Acquiring New CPLP Materials

The CPLP manager will need to create a requirements document if it is necessary to create or source new CPLP content, curricula, or other program elements. The requirements document incorporates the information from the design document as well as any additional and necessary information to provide to the training and curricula developers, editors, and designers, whether

they are in-house or vendors. The requirements document will also be useful for the organization's acquisition and budget functions.

The requirements document generally provides detailed and specific criteria related to the content needed to meet the learning objectives. Typical prompts or questions to review when creating the requirements document for any new CPLP material include:

- For which learning program audience segments is the new element intended for?[18]
- What specific cybersecurity or privacy risks and behaviors does the organization seek to address?
- What knowledge or skills should the learner acquire or improve as a result of the CPLP element?
- Does the material contribute to a positive cybersecurity and privacy culture that reinforces the role of all users in reducing organizational risk?
- Will the material engage personnel?
- What are the budget requirements, restrictions, and timing?
- Who in the organization will review content development and approvals?
- What sort of user testing will be conducted to ensure that the content is appropriate for the learning program participant segment, meets their needs, and is appropriate for their skill level?
- Have the measurements and metrics been included to ensure that the learning program will provide the needed data to improve the next version of the content?

The learning program criteria for the requirements document may include the following considerations:

- Content is topical, relevant, and not quickly dated.
- Content is delivered in formats that support on-site and remote employees, contractors, and guests.
- Content is delivered in appropriate formats for those using adaptive technology (e.g., screen readers).
- Learning material includes qualitative and quantitative assessments and evaluations to measure the learning objectives and outcomes and is aligned to the defined measurements and metrics.
- Learning material is specific to the learning program participant (i.e., audience) segments for which it is intended.

[18] See Sec. 2.5 to review who is in the "all user," privileged access account holders, and significant cybersecurity and/or privacy responsibilities learning program audience segments.

4.1.2. Developing New Materials for the "All User" Learning Program

The "all user" learning program elements (see Sec. 2.5.1) are delivered throughout the year. However, there may be necessary updates to, and iterations of the content based on events and organizational requirements. Ensure that the budget is allocated to update the content or amend the materials with other delivery methods (e.g., to video training) if making actual content changes is cost prohibitive.

Developing a dynamic and effective "all user" learning program — and particularly, the cybersecurity and privacy presentation — is challenging, especially when learners arrive with an expectation that they only need to do the bare minimum to fulfill their training requirement. However, given the ever-changing nature of cybersecurity and privacy risks, there will almost always be new and crucial content for them to understand.

Consider how key messages will be reinforced throughout the "all user" learning program. When necessary, refresher messages may be sent to reinforce a change in behaviors. For example, if the results of a phishing campaign show higher than usual click-through rates, it may be necessary to repeat the campaign using different mediums to ensure that the audience is aware of expected behaviors on the system. Repeated messages become retained messages. Use the awareness program materials to keep the "all user" learning program topical without becoming monotonous or intrusive. This is a tricky balance to achieve and requires a variety of delivery formats and messages. Consider varying the awareness program techniques, such as sending out cybersecurity or privacy topic emails on a monthly basis, adding a campaign message to everyone's official organization signature block for Cybersecurity Awareness Month in October or Data Privacy Week in January, or place posters in the agency's lunchroom all year round.

Choosing techniques for disseminating cybersecurity and privacy awareness messages throughout an organization depends on available resources and the complexity of the messages. Some techniques that are appropriate for a single message include posters, screensavers, warning banners, organization-wide emails, brown bag seminars, and awards programs. Techniques that can more easily include several messages or themes include "do and don't" lists, email newsletters, web-based sessions, teleconferencing sessions, in-person instructor-led sessions, and email signature messaging. Examples of awareness material can be viewed on the Federal Information Security Educators (FISSEA) website[19] under "FISSEA Security Awareness and Training Contest."

Additional considerations when developing the "all user" learning program include:

- What does the organization want all personnel to be aware of regarding cybersecurity and privacy? Starting points may include a review of the latest top risks to the organization, as reported by the cybersecurity or privacy office; common risks reported by cybersecurity and privacy organizations; and new mission goals with cybersecurity or privacy implications. Evaluating organizational policies, program reviews, internal audits,

[19] See https://www.nist.gov/itl/applied-cybersecurity/fissea.

self-assessments, and spot-checks can also help learning program managers identify additional topics to address.

- Were constraints found in the analysis phase? For example, does the organization have particular issues with delivering a learning program to personnel? Will personnel be able to access or attend training by a particular required date to achieve completion? Are some personnel working remotely, traveling, located overseas, or in need of reasonable accommodations? Consider what additional steps will be needed to ensure that all personnel can participate in the "all user" learning program and fulfill their learning program obligations.
- Popular topics for learning programs for this participant segment may include: social engineering exploits (e.g., phishing, spear phishing, vishing, smishing); password policy and management; multi-factor authentication; changing default passwords (e.g., on routers and IOT devices); remote and work-from-home cybersecurity and privacy considerations; cybersecurity when traveling; email security; malware, including ransomware and how to respond; shoulder surfing and insider threat considerations; back-up policy and management; cloud services; and computer, phone, and data disposal policies.

4.1.3. Developing New Materials for the Privileged Access Account Holders Learning Program

Developing new materials or elements for privileged access account holders is similar to developing them for the "all users" segment. Create a requirements document that aligns learning goals for this audience segment with available funding and organizational requirements.

Additional considerations for developing new material for the privileged access account holders learning program include:

- What should privileged access account holders be aware of regarding cybersecurity and privacy?
- What procedures do personnel need to follow to protect their privileged access accounts?

Some starting points include: understanding the rights and privileges allotted to this learning program audience segment; reviewing the risks related to privileged access accounts or the systems or applications associated with privileged access; reviewing these issues with the offices of the CIO, CISO, and/or CPO; and aligning learning goals for these risks to the available budget for impacted personnel and departments. Evaluating organizational policies, program reviews, internal audits, self-assessments, and spot-checks can also help CPLP managers identify additional topics to address.

4.1.4. Developing New Materials for Those With Significant Cybersecurity and/or Privacy Responsibilities

The customized and individualized nature of ongoing skills development and training for personnel with significant cybersecurity and/or privacy responsibilities requires a more detailed and nuanced learning program approach. For example, multiple requirements documents may be needed to develop new learning program elements and identify training that will satisfy learning objectives. The CPLP manager should partner and coordinate these efforts with the organization's human capital office, CLO, training and curriculum developers, and the individual managers and supervisors for the personnel in this learning program audience segment.

CPLP managers should ensure that the complexity of the training is commensurate with the role and needs of the people who will undergo the learning effort. Cybersecurity and privacy role-based training materials can be developed at a beginning level for a person who is just learning a discipline. Materials can be developed at an intermediate level for someone who has more experience and, therefore, more responsibility in their workplace. Advanced materials can be developed for agency SMEs whose jobs incorporate the highest level of trust and an accompanying high level of cybersecurity or privacy responsibilities.

4.1.5. Acquiring Learning Materials From External Sources

CPLP managers should evaluate available materials from a variety of external sources, including federal programs and repositories, industry vendors, and academic institutions. Some of these courses or learning elements may be low cost or even free.

Where budget permits, CPLP managers may choose to acquire (or license) a vendor-provided library of courses and align, curate, and recommend a set of those courses for the learning program audiences or certain work roles. Acquisitions of CPLP materials should be guided by the same learning criteria identified for the creation of new elements (see Sec. 3.3.1). CPLP managers should also consult with their organization's agency contracting office.

4.1.6. Conducting Learner Testing on New CPLP Elements

Include a learner testing ("user testing") phase for all new CPLP elements prior to implementation. Content should be assessed for each learning program audience segment to ensure that it meets their needs and is appropriate for their skill level. Additional learner testing might include evaluating the intended element's delivery method, the appropriateness of the language, the value to the learner, and overall acceptance of the new element. Feedback from learner testing should be iterative and incorporated at every step of the design effort, not just in the form of evaluations after implementation.

4.2. Implementing New CPLP Elements

Implementation refers to the actual distribution and delivery of the CPLP materials. This phase focuses on the connection between the learner and the content. Once the plan for

implementing the CPLP has been communicated to and accepted by management (see Sec. 2.11), the implementation phase can begin. Use a life cycle process when implementing the program to avoid a "one and done" scenario, and periodically review the program for updates and corrections.

4.2.1. Steps for Implementing a New CPLP Element

CPLP managers should implement a new learning program or a single element with the same repeatable steps. It is of the utmost importance that all of those involved in the implementation phase be included in a well-designed communications effort. This ensures that personnel and their managers or supervisors are well-informed about any upcoming CPLP opportunities that are relevant to their required learning plans. The implementation phase is also the time to confirm that the required reporting and metrics can be satisfied in later program phases. Steps to consider before initiating the implementation phase include:

1. Communicating the CPLP implementation
2. Measuring success by establishing measurement, metric, and reporting requirements
3. Building a CPLP schedule
4. Planning to evaluate program success by reviewing post-implementation feedback, measurements, and metrics

4.3. Communicating the CPLP Implementation

Communication is a large part of developing an organization's shared culture of supporting the learning program efforts. CPLP managers should develop a communications plan for each phase of the program element implementation and include the organization's communications team. CPLP managers should also determine the appropriate timing to inform managers, supervisors, and possibly the personnel involved about upcoming and required learning program elements, as well as the frequency with which to send out reminders and other forms of communication that encourage cooperation from the organization.

Each individual CPLP element (e.g., presentation, course, or tabletop exercise) requires a separate and more detailed form of communication to inform learners and their managers of important details regarding the learning event. This includes items such as:

- Titles, descriptions, purpose of the training or learning activity (including prerequisites), learning goals, objectives, and learner outcomes
- Participating learning program audience segments (if not all users)
- Tracking method (and completion tracking), including consequences of not completing the learning, especially for self-paced content (by deadline or at all)
- Delivery method (e.g., in person, virtual delivery, self-directed online learning, etc.)
- Required, recommended, or requested accommodations

- Schedule considerations, such as registration timelines, availability dates, or due dates
- Verification of learners with significant cybersecurity or privacy responsibilities

The communications plan should include a clear explanation of why the learning program is mandated (if applicable) and the benefits of attending (i.e., the learner outcomes). Applicable federal legislation, regulations, and agency or organizational policies should be referenced.

Each learner audience must be specified for the training assigned. For example, if the organization's policy states that all system users must complete a particular training to gain or maintain access to enterprise systems, the communications plan must include this notice. For those with significant cybersecurity or privacy responsibilities, identify which training is assigned to a specific work role, individual, or department.

Employees must know the consequences of failing to complete the learning activity according to the organization's policy. This should be explained in the learning program communications plan and noted in the course description in the learning plan within the LMS.

Other considerations for CPLP communications include:

- Course titles and numbers should be unique, differentiated, and include information on the access method (e.g., online or in-person), availability, course dates, and deadlines.
- All learners, their managers or supervisors, and human capital departments should be informed of any required training and associated due dates. Communication should include reminder messages, references and links to the organization's official policy statements for employee information systems, and the consequences of failing to complete the learning activity.

4.4. Establishing Measurements, Metrics, and Reporting

As noted in Sec. 2.4, CPLP managers should strive to ensure that the implementation of all new CPLP elements (e.g., courses, training, posters, practical exercises, etc.) will allow for performance metrics and measurements to be established and collected. Review these requirements during the developmental phase to ensure that the measurements still meet expectations, such as regulatory and annual reporting requirements, learning objectives, and learner outcomes. The goal is not simply to meet compliance requirements but to enable an ongoing development effort for the CPLP. As previously mentioned in Sec. 3.2.2, the measurements and metrics are included in the design plan requirements used by curriculum and content developers.

Some considerations for reporting measurements and metrics include:

- LMS integration: Any automated LMS used should provide the capabilities to track all necessary measures, such as training registration, attendance, and completion.
- Non-LMS integrated elements: Consider how the participation and performance of each learner will be tracked and recorded if the training is face-to-face, virtual, or hybrid (e.g., manual or paper tracking).

- Consider metrics for how the CPLP element contributes to a positive cybersecurity and privacy culture and improves behavior.

As a final step, the CPLP manager will meet with the Senior Leadership Committee to review the performance of the program, address new organizational risks or concerns to include in the training program content, and identify any areas for significant improvement. Section 5 provides more information on how measurements and metrics help to ensure that the CPLP life cycle is an ongoing and continual effort.

4.5. Building a CPLP Schedule

Establish a primary calendar for CPLP activities, which may be automated using an LMS. Enable organization-wide access so that personnel can find elements that are applicable to each audience segment (e.g., by date, learning objective, etc.). Align this calendar with organizational availability, such as observed holidays, planned events, major IT releases, and other considerations that might cause learner conflicts with the CPLP schedule. As part of the communications plan, send out reminders to ensure that instructors and materials are identified and allocated well in advance.

4.6. Planning to Evaluate Program Success

Once any CPLP element has been delivered or implemented, the CPLP manager should initiate post-implementation activities that fuel assessment and improvements.[20] Some awareness elements, such as measuring learning program participant engagement, may be difficult, especially for passive items like posters or email signatures. Nevertheless, it is possible to measure impact. One method could include surveying a sample of learners to discuss their familiarity with the messaging or whether they have practiced any of the tips.

Some key items to consider during the implementation phase are:

- Sending post-training feedback surveys
- Conducting instructor feedback surveys
- Determining attendance and completion rates by learner or department
- Other mandated or organizational reporting
- Budget reconciliation
- Consolidating all CPLP feedback surveys, metrics, and other reports to prepare materials for assessment and improvement

[20] Section 5 discusses how to evaluate program success by disseminating, collecting, reviewing, and reporting on the CPLP's performance using all available post-implementation feedback, measurements, and metrics (see Sec. 2.4) and learning program elements (see Sec. 4.4).

5. CPLP Assessment and Improvement

An effective CPLP meets the needs of learners and the organization by measuring and evaluating program performance on a continual basis. This process requires up-to-date knowledge, awareness, and understanding of the legal and regulatory compliance requirements for the organization and cybersecurity and privacy risks. CPLP managers work with organizational leaders, training staff, and learners to share performance reporting and decision-making throughout all phases of the CPLP. Analyzing organizational risks (e.g., decrease in the number and frequency of common issues that the learning program has targeted over time) and reviewing the efficacy of materials (e.g., learner feedback responses to courses) are important in the continual improvement of a CPLP in an evolving threat landscape. Remember to choose measurements that can be quantified, such as SMART goals (i.e., specific, measurable, achievable, relevant, and time-bound).

5.1 Steps for Assessing and Improving the CPLP

The process for assessing and improving the CPLP may vary by organization and available resources. Consider the following steps as part of evaluating the CPLP's performance, whether for the entire CPLP, for each audience segment, or for a single CPLP element.

- Create a CPLP assessment report:
  - Analyze measurements and metrics.
  - Review regulatory compliance and reporting.
  - Evaluate CPLP effectiveness through feedback.
- Review the CPLP assessment report with senior leadership:
  - Agree on the changes needed for the CPLP.
  - Evaluate budget requirements for program improvement.
- Make CPLP improvement efforts:
  - Review and update the CPLP strategic and operational plans.
  - Implement changes into the next revisions of the program elements and schedule.

5.2 Creating a CPLP Assessment Report

At the end of a campaign and regularly throughout the year as agreed upon with the Senior Leadership Committee, CPLP managers should create a summary document to review with senior leadership. This report will provide an analysis of attendance, feedback, measurements, and other metrics and help to identify action items, areas of improvement, and next steps. It should be tailored for senior leadership using appropriate language and framing (e.g., avoid using technical jargon without explanation).

A CPLP assessment report includes:

- Measurements and metrics (Sec. 5.2.1)
- Regulatory compliance information (Sec. 5.2.2)
- Evaluation of CPLP effectiveness (Sec. 5.2.3)
    - Instructor evaluation (Sec. 5.2.3.1)
    - Content evaluation (Sec. 5.2.3.2)
    - Learner, supervisor, and organizational feedback (Sec. 5.2.3.3)

5.2.1 Measurements and Metrics

Measurements and metrics are the key drivers for the assessment and improvement phase of the CPLP life cycle. The process of developing and establishing CPLP measurements requires careful consideration and should be driven by the program goals and objectives, as well as any regulatory requirements.

How the organization defines and collects its measurements will lead to the definition and analysis of its metrics. Metrics monitor the accomplishment of the program goals and objectives by quantifying the level of implementation, effectiveness, and efficiency of the program while identifying possible improvements. An effective set of metrics can help improve content quality and learner engagement, obtain support from the organization, increase funding, reveal impacts on the cybersecurity and privacy risk management program, and demonstrate returns on investment. Include results from both quantitative and qualitative measurement instruments.

5.2.2 Regulatory Compliance Reporting

CPLP managers should be aware of and prepared to participate in all CPLP-related compliance regulations for the organization, including reporting requirements. In some organizations, compliance reporting may be handled by an assigned single individual or group. For those organizations in which the duties are separated, it is critical to maintain collaborative communication to ensure that the program meets compliance.

A fully developed and integrated CPLP may become a useful tool for supporting enterprise risk management, although many are initially developed to address compliance requirements in laws, regulations, policies, or standards. Meeting these compliance obligations is often the primary focus of higher level leadership but should only be the starting point for a robust CPLP program. Examples of common quantifiable metrics to demonstrate CPLP compliance include training a certain percentage of the workforce and the results of practical exercises. Organizations should determine which compliance measurements they must achieve and consider those inputs when developing the CPLP.

CPLP managers should work with policy owners to determine the methods that the CPLP will use to meet reporting needs and ensure that the results of the learning efforts satisfy compliance requirements. Examples of questions to ask to help identify those needs include:

- Which personnel received (or participated in) the learning element?
- How well does the participation level match the goal of learning program participant segment coverage?
- How far should the CPLP go in pursuit of expected coverage?
- Have individuals in compliance-identified roles met their learning requirements?

5.2.3 Evaluating CPLP Effectiveness

CPLP managers should periodically evaluate the overall effectiveness of the CPLP and report the results to leadership to encourage continued support for the program. At this step of the program life cycle, the application of metrics and measurements (see Sec. 2.4) should be documented.

In addition to ensuring compliance with regulatory requirements, the program itself needs to be able to meet its own goals. Two major components of the program to measure and assess are the instructors and the content. CPLP managers should review the performance of instructors to ensure that the material is delivered effectively. The success of the content can then be determined by incorporating feedback from instructors, students, and leadership. The following subsections describe measurements and metrics needs for assessment and evaluation.

5.2.3.1. Instructor Evaluation

The instructor is responsible for creating an environment in which learning can take place by facilitating discussions, providing knowledge and expertise, and motivating and inspiring the participants to learn new skills. An instructor evaluation includes both an assessment of the instructor and feedback from what the instructor observed or experienced.

CPLP managers and the Senior Leadership Committee work together to find the right instructors for their personnel and their CPLP's learning objectives by determining whether organizational resources can support a dedicated in-house team of instructors or external resources are needed to implement instructor-led learning content. In some organizations, the cybersecurity learning program manager is also the privacy learning program manager and the lead instructor.

Since instructors are a key factor in creating a supportive and effective learning environment, it is important to monitor the performance of instructors via observation and other forms of feedback. Some effective instructor qualities include how well the instructor communicates the material and key concepts for the audience level, engages with learners in a positive and respectful manner, encourages active participation, uses interactive teaching methods, and responds to learner questions and concerns.

Instructor feedback can be obtained via the learner's course feedback, as well as from direct annual observations of the instructor. Some tips for providing learner feedback are:

- Allow learners to submit anonymous feedback to encourage constructive reviews.
- Ask learners specific questions about the instructor's teaching methods, knowledge of the subject, and classroom management.
- Provide the feedback to the instructor in summary form so that individuals are not inadvertently identified.

Some tips for instructor observations are:

- Include direct observations of the instructors using experienced instructional designers or supervisors who can provide insights into teaching styles, class management, and engagement with learners.
- Include peer observations from other instructors as an informal feedback mechanism.
- Tell instructors when observers will be there and allow them to be prepared.

It is important to create a fair and supportive instructor evaluation process to ensure that learning goals are achieved and there is continuous improvement. Combining multiple evaluation methods and a transparent process provides a solid foundation for constructive evaluation. Most importantly, instructors will know that they are appreciated for their important role in the learning program.

5.2.3.2. Content Evaluation

Instructors also provide important feedback on the learning material and how it was received by the learners. CPLP managers should work with instructors to review their comments and observations and, when necessary, support the adjustment of material for greater effectiveness. Instructors can provide feedback on:

- Perceived accuracy
- Ease of instruction and learner understanding
- Adequacy of materials to support content
- Relevance and timeliness of materials

5.2.3.3. Learner, Supervisor, and Organizational Evaluation and Feedback

Considering multiple types of feedback can help CPLP managers develop a thorough understanding of what is working and where improvement is needed in a CPLP. Feedback mechanisms can be used to evaluate learners' reactions, learnings, behaviors, and results — the four levels of learner impact in the Kirkpatrick Model [15], as shown in Table 3.

Table 3. Four levels of the Kirkpatrick Model for training evaluation

Level	Impact	Description
Level 1	Reaction	Seek participant feedback on the learning program's usefulness, engagement, and environment (e.g., conducive to learning, etc.) during and at the end of the learning element.
Level 2	Learning	Assess participants to determine whether the intended knowledge or skills have been acquired during and at the end of the learning element.
Level 3	Behavior	Obtain feedback from learners, peers, and/or supervisors to determine whether learners have applied the learning content and acquired skills in the performance of their work role.
Level 4	Results	Obtain feedback from senior leaders to determine whether learning outcomes are meeting organizational goals.

Level 1 is sometimes referred to as the "smile sheet" because a simple questionnaire with visual prompts for ratings can be used to ask the learner for their immediate thoughts on the learning program. The results from Level 1 reactions can be used to assess the immediate impact of the learning program element.

Level 1 reaction measurements are influenced by:

- Overall perceived level of engagement and effectiveness of the training program
- Use of interactive mechanisms throughout the training, such as poll questions, interactive discussions, and individual or small group activities
- Use of end-of-course survey questions or other types of debrief sessions to assess learner satisfaction and their perceptions of the learning element and the learning program. Examples of questions to ask at the conclusion of the learning program element are:
    - Was the learning program element relevant to your work role?
    - How satisfied are you with the content, delivery mechanism (e.g., online platform, facility, or instructor), level of engagement, length of time, and depth of the material?
    - Was the learning program element worth your time?
    - What are the three most important things you learned from the learning program element?
    - What additional information or other topics would be helpful to you?
    - What is your overall impression of the learning program?

Level 2 evaluates how well the participant absorbed the learning content and acquired new knowledge based on the learner outcomes, which are written in a format that is measurable, achievable, and outcome-based. One of the most common techniques for measuring learner performance is an end-of-course assessment, though there are other innovative and engaging techniques that should be considered and utilized.

Level 2 learning best practices include:

- Written questions or practical activities developed at a level commensurate with both the complexity of the material and the level of understanding expected of the learner
- Clear learning objectives and learner outcomes as well as assessments that align with the learning objectives and content
- Practical assessments that allow for the demonstration of knowledge and skill development and that mimic what will be experienced in the work role
- Use of various assessment methods, such as case studies, interactive virtual cyber labs, demonstrations, and scenario-based exercises

Level 3 considers whether the learner was able to apply new knowledge or skills to their work responsibilities and duties. Obtaining feedback depends largely on asking questions of learners, their peers, or their supervisor.

Level 3 behavior best practices include:

- Questions that help identify gaps in the learning program materials and may indicate the need to reinforce those materials
- Questions that help identify gaps in the organizational structure that limit the learner's ability to apply the new knowledge and skills
- Examples of questions for learners may include:
    - How have you utilized the knowledge gained from the learning program in the workplace? How has your approach to [job activity] changed after attending the learning program? Describe a situation at work in which you were able to apply your new knowledge or skills.
    - What additional learning content support or reinforcement or job aid would help you utilize new knowledge and skills in the workplace?
    - Was the cybersecurity lab activity on troubleshooting rogue IP addresses adequate to help you do this activity on the job? In what ways, if any, was the small group activity on identifying roles and responsibilities helpful for your workplace?
- Examples of questions for peers or supervisors may include:
    - In what ways, if any, have you observed or noticed changes in the learner's [job activity] since they attended the learning program. Have you observed the learner sharing their new knowledge or skills with others?
    - What new processes or procedures need to be included in the learning materials, if any? What new focus areas or changes in the workplace, if any, need to be included in the learning materials?
    - How could job aids, awareness materials, or learning support help reinforce the new knowledge or skills?

- Follow-up questions are usually asked three to six months after the learning activity so that enough time has passed for the learner to integrate the learning material into their work responsibilities and duties.

Level 4 feedback determines the impact that the learning program had on the organization, sometimes referred to as a return on investment (ROI). CPLP managers analyze the results of the activity from an enterprise-wide perspective. For example, the organization may decide to implement a new technology, such as artificial intelligence (AI), in its business processes. Training provides the policies and procedures for how the learner can use AI technologies in their work role. The program requires learners to attend the training but also requires supervisor approval and justification for its use. The organization must then determine whether the training on policies and procedures or supervisory control produced the results. To utilize this assessment method correctly, the requirements, objectives, overall outcomes, and metrics must be clearly defined.

Learning objectives and learner outcomes should be aligned with the organization's strategic and business objectives and goals during the design process. An organizational goal aligned to learning objectives should be quantifiable and detailed (e.g., "SMART" goals). An example of aligning an organizational goal, learning goals, learner outcomes, and organizational results is:

- **Organizational goal:** When notified, staff will be able to mitigate all known exploited vulnerabilities within 48 hours following organizational processes.
    - A metric to determine whether the organizational goal is achieved is a trend analysis of time needed by staff to mitigate known exploited vulnerabilities. Establish a baseline before the learning program, and track changes following the learning program.
- **Learning goals:** Participants can track known exploited vulnerabilities, discover impacts to the organization, analyze and document indicators of compromise, notify stakeholders, and implement and document mitigation strategies.
- **Learning outcomes:** When presented with a known exploited vulnerability, learners will be able to analyze impacts to the organization, find and document indicators of compromise, and implement and document mitigation activities within a 48-hour time frame.
- **Organizational results:** The CPLP manager shares the trend analysis results from mitigation activities for known exploited vulnerabilities, which indicate that the organization processes were followed and completed within 48 hours of notification.

Level 4 results best practices include:

- Before the learning program begins, establish baseline metrics that can be used as a starting point for evaluating change. For example, before the learning program, the vulnerability mitigation time was 72 hours; after the learning program, the vulnerability mitigation time was 48 hours.

- Utilize both quantitative and qualitative measurements to ensure a holistic view of the learning program's impact.
- Acknowledge and communicate to senior leadership that it takes time to see the full impact of a learning program on organizational results.
- Implement measurements and metrics on how to attribute changes to the organization through the learning program. A learning program combined with other organizational changes (e.g., change in resources, additional support, or new procedures) will have the greatest impact on organizational changes.

5.2.4. Reviewing the CPLP Assessment Report with Senior Leadership

As a final step, CPLP managers meet with their Senior Leadership Committee to review the performance of the program, address new organizational risks or concerns to include in the learning program content, and identify any areas for significant improvement. The review will leverage the established measurements and requirements (see Sec. 4.4) to ensure that the life cycle approach of the CPLP (see Fig. 1) is an ongoing and continual effort.

During the meeting with the Senior Leadership Committee, discuss specific outcomes and considerations that may impact resource requirements. Some organizations may require documentation, such as a project proposal that outlines the issue (i.e., why it is necessary), solution (i.e., what will solve the problem), scope of the work (i.e., summary of the learning work), benefit (i.e., how the learning effort will benefit the employees and the organization), and an initial estimate of the resources needed (i.e., people and financial costs) for the work.

5.3 CPLP Improvement Efforts

A CPLP provides a robust learning program that is designed to develop the knowledge and skills of personnel to reduce and/or manage privacy and cybersecurity risks. CPLP managers and their teams must analyze the accuracy, quality, and appropriateness of the materials in the context of the desired outcomes and follow up after element implementation to determine whether the materials met the goals as intended.

The NIST CSF [8], Privacy Framework, and SP 800-53r5 [11] offer guidance a CPLP can adapt to facilitating continuous monitoring and improvements. In the CSF, Improvement Category under the IDENTIFY Function acknowledges the importance of "improvements to organizational cybersecurity risk management processes, procedures and activities," and the Continuous Monitoring Category in PROTECT addresses monitoring for "anomalies, indicators of compromise, and other potentially adverse events" (in this case ineffective materials or processes in the CPLP, for example). The Monitoring and Review Category of the GOVERN-P Function in the Privacy Framework discusses the need for ongoing review and informing risk management practices based on those insights. SP 800-53r5 [11], Sec. 1.3, includes the organizational responsibility of "[c]ontinuous monitoring of information systems and organizations to determine the ongoing effectiveness of controls, changes in information systems and environments of operation, and the state of security and privacy organization

wide." In this context, continuous monitoring and improvement refer to the iterative nature of reviewing, updating, and maintaining the program in alignment with requirements and best practices. The process can happen during any phase of the CPLP and acknowledges the constantly shifting needs of an organization to manage resources and risks. Based on the CPLP assessment report and any new requirements (e.g., legislative, organizational, system changes, risk-related, etc.), CPLP managers will be able to identify opportunities for improvement.

6. Summary

Ultimately, the goal of the CPLP is to enable the organization to withstand cybersecurity and privacy-related risks to the organization's information and assets. The organization's workforce is a crucial part of creating the positive cultural norms that will both support the aims of the CPLP and contribute to greater success in changing behaviors. Avoid efforts to penalize those who do not adapt to the culture as well as others. Rather, shine a light on individuals, teams, and departments that improve performance, establish best practices, and help build a positive CPLP culture. Find ways to celebrate personnel who are building the organization's CPLP culture and share information about the CPLP's performance when appropriate. If feedback indicates that a change is required to the learning program because something is not working, ensure that the program is nimble enough for that adjustment to be implemented. Do not wait for the end of the year or another arbitrary time period.

The goals of continual improvement do not need to be built on the ashes of past failures but should be seen as an opportunity to grow and strengthen a critical program. A positive cybersecurity and privacy culture celebrates successes while acknowledging the ever-present risks to the organization.

References

[1] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Public Law 116-283. Available at https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf

[2] Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073. Available at https://www.govinfo.gov/app/details/PLAW-113publ283

[3] Office of Management and Budget (2016) Managing Information as a Strategic Resource. (The White House, Washington, DC), OMB Circular A-130, July 28, 2016. Available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

[4] deZafra DE, Pitcher SI, Tressler JD, Ippolito JB (1998) Information Technology Security Training Requirements: a Role- and Performance-Based Model. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-16. https://doi.org/10.6028/NIST.SP.800-16

[5] Petersen R, Santos D, Wetzel K, Smith M, Witte G (2020) Workforce Framework for Cybersecurity (NICE Framework). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-181, Rev. 1. https://doi.org/10.6028/NIST.SP.800-181r1

[6] Haney J, Jacobs J, Furman S, Barrientos F (2022) Approaches and Challenges of Federal Cybersecurity Awareness Programs. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 8420A. https://doi.org/10.6028/NIST.IR.8420A

[7] Haney J, Jacobs J, Furman S, Barrientos F (2022) The Federal Cybersecurity Awareness Workforce Professional Background Knowledge, Skills, and Development Activities. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Internal Report (IR) NIST Interagency or Internal Report 8420B. Available at https://doi.org/10.6028/NIST.IR.8420B

[8] National Institute of Standards and Technology (2024) Cybersecurity Framework, Version 2.0. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.29

[9] National Institute of Standards and Technology (2020) NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Cybersecurity White Paper (CSWP) NIST CSWP 10. https://doi.org/10.6028/NIST.CSWP.10

[10] Joint Task Force (2018) Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-37, Rev. 2. https://doi.org/10.6028/NIST.SP.800-37r2

[11] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[12] Schroeder K, Trinh H, Pillitteri V (2024) Measurement Guide for Information Security: Volume 1 — Identifying and Selecting Measures. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-55v1 ipd. https://doi.org/10.6028/NIST.SP.800-55v1.ipd

[13] Grance T, Nolan T, Burke K, Dudley R, White G, Good T (2006) Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, 1.0. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-84. Available at https://doi.org/10.6028/NIST.SP.800-84

[14] FY2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v1.1 (2021). Available at https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Metrics%20Final%20v1.1%202020-05-12.pdf

[15] Kirkpatrick DL (1994) Evaluating Training Programs—The Four Levels (Berret-Koehler Publishers, Inc, San Francisco, CA).

[16] National Institute of Standards and Technology (2024) Glossary. Available at https://csrc.nist.gov/glossary

[17] Information Technology Reform Act of 1996, 40 USC 11101; Sec. 5002: Definitions. Available at https://www.govinfo.gov/content/pkg/USCODE-2021-title40/pdf/USCODE-2021-title40-subtitleIII-chap111-sec11101.pdf

[18] U.S. Office of Personnel Management (OPM) (2024) Competencies. Available at https://www.opm.gov/policy-data-oversight/assessment-and-selection/competencies/

Appendix A. Examples of Cybersecurity and Privacy Learning Program Maturity Levels

The following example is adapted from the FY21 Inspector General FISMA Metrics for Security Training [14] and provides one method for assessing the maturity of a learning program. Similar to other business or quality maturity models, this example can help measure progress and set strategic goals for optimizing a learning program. A fully "mature" program is an integrated operational element of the system and processes and is continually monitored and improved.

Table 3. Examples of CPLP maturity levels

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
The extent to which the roles and responsibilities of the learning program have been defined, communicated, implemented, and appropriately resourced	Roles and responsibilities have not been defined, communicated, or implemented across the organization nor appropriately resourced.	Roles and responsibilities have been defined, communicated, and implemented across the organization, and resource requirements have been established.	Individuals are performing the roles and responsibilities that have been defined across the organization.	Resources are allocated in a risk-based manner for stakeholders to consistently implement, and stakeholders are held accountable for carrying out their roles and responsibilities effectively.	
The extent to which the organization utilizes an assessment of the skills, knowledge, and abilities of its workforce to provide tailored and specialized learning content	The organization has not defined its processes for assessing the knowledge, skills, and abilities of its workforce.	The organization has defined its processes for assessing the knowledge, skills, and abilities of its workforce to determine its learning needs. It periodically updates its assessment to account for a changing risk environment.	The organization has assessed the knowledge, skills, and abilities of its workforce; tailored its learning content; and identified its skills gaps. It periodically updates its assessment to account for a changing risk environment. In addition, the assessment serves as a key input to updating the organization's learning strategy and plans.	The organization has addressed its identified knowledge, skill, and ability gaps through training or talent acquisition.	The organization's personnel collectively possess a training level such that the organization can demonstrate that security incidents resulting from personnel actions or inactions are being reduced over time.

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
The extent to which the organization utilizes a learning strategy and plan that leverage skills assessment and are adapted to the organization's mission and risk environment	The organization has not defined its security learning strategy or plan for developing, implementing, and maintaining a learning program that is tailored to its mission and risk environment.	The organization has defined its learning strategy and plan for developing, implementing, and maintaining a learning program that is tailored to its mission and risk environment.	The organization has consistently implemented its organization-wide learning strategy and plan.	The organization monitors and analyzes qualitative and quantitative performance measurements on the effectiveness of its learning strategies and plans. The organization ensures that data-supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization's learning program activities are integrated across other security-related domains. For example, common risks, control weaknesses, and other outputs of the agency's risk management and continual monitoring activities inform any updates that need to be made to the learning program.
The extent to which the organization ensures that the learning program is provided to all personnel and is tailored based on its mission, risk environment, and types of information systems	The organization has not defined its learning policies, procedures, or related materials based on its mission, risk environment, or the types of information systems that its learners have access to. The organization has not defined its processes for ensuring that all personnel are provided with training upon initial access to the system and periodically thereafter. The organization has not defined its processes for evaluating or obtaining feedback on its learning program to make continual improvements.	The organization has defined and tailored its learning policies, procedures, related materials, and delivery methods based on identified requirements and the types of information systems that its learners have access to. The organization has defined its processes for ensuring that all personnel, including contractors, are provided with training upon initial access to the system and periodically thereafter. The organization has defined its processes for evaluating and obtaining feedback on its learning program and uses that information to make continual improvements.	The organization ensures that its learning policies and procedures are consistently implemented. The organization ensures that all appropriate learners complete the organization's training upon initial access to the system and periodically thereafter and maintains completion records. The organization obtains feedback on its learning program and uses that information to make improvements.	The organization measures the effectiveness of its learning program by, for example, conducting practical exercises and following up with additional awareness, training, or disciplinary action, as appropriate. The organization monitors and analyzes qualitative and quantitative performance measurements on the effectiveness of its learning policies, procedures, and practices. The organization ensures that data-supporting metrics are obtained accurately, consistently, and in a reproducible format.	The organization has institutionalized a process of continual improvement that incorporates advanced learning practices and technologies. On a near real-time basis, the organization actively adapts its learning policies, procedures, and processes to a changing cybersecurity and privacy landscape and provides learning content on evolving and sophisticated threats and problematic data actions, as appropriate.

Question	Ad Hoc	Defined	Consistently Implemented	Managed and Measurable	Optimized
The extent to which the organization ensures that specialized learning is provided to individuals with significant security or privacy responsibilities	The organization has not defined its security or privacy learning policies, procedures, or related materials based on its mission, risk environment, or the types of roles with significant security or privacy responsibilities. The organization has not defined its processes for ensuring that personnel with significant security or privacy roles and responsibilities are provided with specialized learning content and does not offer additional learning opportunities.	The organization has defined its security and privacy learning policies, procedures, and related materials based on its requirements, mission, risk environment, and types of roles with significant security and privacy responsibilities. The organization has defined its processes for ensuring that personnel with assigned security and privacy roles and responsibilities are provided with specialized security learning materials and periodically given additional learning opportunities.	The organization ensures that its security and privacy learning policies and procedures are consistently implemented. The organization ensures that individuals with significant security and privacy responsibilities complete the organization's defined specialized learning and are provided with periodic enhancements or additional relevant learning opportunities. The organization maintains completion records for specialized learning taken by individuals with significant security and privacy responsibilities. The organization obtains feedback on its security and privacy learning program and uses that information to make improvements.	The organization ensures that its security and privacy learning policies and procedures are consistently implemented. The organization ensures that individuals with significant security and privacy responsibilities complete the organization's specialized security and privacy learning and provides periodic enhancements and additional relevant learning opportunities. The organization maintains completion records for specialized learning taken by individuals with significant security and privacy responsibilities. The organization obtains feedback on its security and privacy learning program and uses that information to make improvements.	The organization has institutionalized a process of continual improvement that incorporates advanced security and privacy learning practices and technologies. On a near real-time basis, the organization actively adapts its security and privacy learning policies, procedures, and processes to a changing cybersecurity and privacy landscape and provides learning materials on evolving and sophisticated threats and problematic data actions, as appropriate.

Appendix B. Glossary

The following terms are used in this Special Publication, and some definitions are adapted from their original sources. Additional terms that are not defined below may be found in the NIST Glossary [16].

awareness
The ability of the user to recognize and avoid behaviors that could compromise cybersecurity and to act wisely and cautiously to increase cybersecurity.

awareness content
Content that is designed and implemented to help employees understand how their actions may impact or influence vulnerabilities and threats. Organizations provide various types of awareness materials (e.g., posters, newsletters, websites) so that employees can realize their roles in protecting cyber assets.

awareness training
The foundational cybersecurity or privacy training program for all personnel. It is designed to help learners understand the roles that they play in protecting information, cybersecurity, and privacy-related assets. It often consists of instructor-led and online courses, exercises, or other methods that inform learners of the acceptable uses of and risks to the organization's systems.

> *Note:* This is referred to as "literacy" training in the SP 800-53r5 [11] Awareness and Training (AT) control family.
>
> Also see *training*.

certification
A designation earned to ensure qualifications to perform a job or task. Often issued by a professional organization, industry vendor, or employer to signify an achievement following a course of study.

Chief Artificial Intelligence Officer
A senior executive responsible for coordinating their agency's use of artificial intelligence (AI), promoting AI innovation in their agency, and managing risks from their agency's use of AI.

Chief Data Officer
A senior executive responsible for the utilization and governance of data across the agency or organization.

Chief Financial Officer
A senior member responsible for managing the financial actions of an agency or organization.

Chief Learning Officer
A senior-level executive who oversees all learning and employee development programs within an agency or organization.

Chief Privacy Officer
A senior official designated by the head of each agency to have agency-wide responsibilities for privacy, including the implementation of privacy protections; compliance with federal laws, regulations, and policies related to privacy; the management of privacy risks at the agency; and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

competency
An individual's ability to complete a task or tasks within the context of a work role.

> From OPM: "A *competency* is a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully.

Competencies specify the "how" of performing job tasks, or what the person needs to do the job successfully." [18]

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

CPLP (Cybersecurity and/or Privacy Learning Program) manager(s)
The person or people in the organization responsible for the development, procurement, integration, modification, operation, maintenance, or final disposition of the elements of the cybersecurity and/or privacy (CPLP) learning programs. In some organizations, there will be multiple iterations of learning programs in which cybersecurity and privacy are managed separately.

cyber range
This technique provides a safe environment (i.e., "sandbox") to deliver hands-on realistic training, scenarios, challenges, and exercises in an easy-to-access web-based environment.

cybersecurity
The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.

data privacy
A condition that safeguards human autonomy and dignity through various means, including confidentiality, predictability, manageability, and disassociability.

Data Management Officer
An official responsible for overviewing and carrying out the data management tasks of research projects. Main duties and responsibilities include data collection or the formulation, implementation, and enforcement of proper data collection policies and procedures. Trains reporting agencies on data collection tools and equipment.

disassociability
Enabling the processing of data or events without association to individuals or devices beyond the operational requirements of the system.

gap analysis
The process of comparing current learning program or activity performance with the desired, expected performance.

information technology
Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use (i) of that equipment or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. Includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources. Does not include any equipment acquired by a federal contractor incidental to a federal contract.

integrity
Guarding against improper information modification or destruction and ensuring information non-repudiation and authenticity.

learning objectives
Identifies the outcomes that the learning program sub-component or module should strive to meet for each of the participants and their associated roles in reducing, managing, and mitigating risks.

learning program
Consists of numerous elements led by the learning program managers, who develop a strategic plan to deliver a right-sized program to reduce organizational cybersecurity and privacy risks via workforce education and training. Operates throughout the year and incorporates plans for ongoing improvements that are based on rigorous assessments and metrics that support compliance and other mandated reporting.

learning program plan
A formal document that provides an overview of an agency's cybersecurity and privacy learning program, including a description of its structure, the resources dedicated to it, the roles of senior agency officials and staff, and the strategic goals and objectives of the learning program to meet applicable privacy requirements and manage privacy risks.

literacy
An individual's familiarity with a basic set of knowledge.

manageability
Providing the capability for the granular administration of data, including alteration, deletion, and selective disclosure.

needs assessment
The process of identifying gaps in learning and the needs of learning activities.

predictability
Enabling reliable assumptions by individuals, owners, and operators about data and their processing by a system, product, or service.

privacy event
The occurrence or potential occurrence of problematic data actions.

privileged network account
A network account with elevated privileges that is typically allocated to system administrators, network administrators, DBAs, and others who are responsible for system/application control, monitoring, or administration functions.

privileged access account holder
A user who is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform (e.g., special access to software applications or web publishing), requires additional training, and must sign an acceptable use policy. A user with a privileged access account.

problematic data action
A data action that could cause an adverse effect for individuals.

program metrics
Tools designed to facilitate decision-making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data.

role-based training
A multi-step process in the learning program that begins with defining the significant cybersecurity or privacy work roles in the organization and identifying the personnel aligned to those designated work roles. Learning materials are then assigned, acquired, or developed based on the tasks necessary to perform the work role. (See the NICE Framework [3] for "work role.")

NOTE: In addition, SP 800-53r5 [11] control AT-3 provides the following definition for Role-Based Training: "Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the cybersecurity and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational cybersecurity and privacy programs. Role-based training also applies to contractors who provide services to federal agencies."

Senior Agency Official for Privacy
The senior official designated by the head of each agency who has agency-wide responsibility for privacy, including implementing privacy protections; ensuring compliance with federal laws, regulations, and policies related to privacy; managing privacy risks at the agency; and filling a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.

significant cybersecurity or privacy responsibilities
The preferred terminology herein for identifying those whose roles in the organization necessitate ongoing role-based training. These individuals have work-related responsibilities beyond those of all users and will need to participate in both general and specialized learning program activities.

NOTE: From FISMA FY2014 CIO Metrics [14]: "Those with significant cybersecurity responsibilities include all users who have one or more privileged network user account and all other users who have managerial or operational responsibilities that allow them to increase or decrease cybersecurity."

synchronous training
Training in which instructors and learners are scheduled to participate together in a virtual or physical classroom-based learning environment.

tabletop materials
Materials designed for a discussion-based exercise in which personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to discuss their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on that scenario.

NOTE: In SP 800-84 [13], tabletop exercises typically include the following documentation:

- A briefing for the participants that includes an agenda and logistics information.
- A facilitator guide that includes:
  - The purpose for conducting the exercise
  - The exercise's scope and objectives
  - The exercise's scenario, which is a sequential, narrative account of a hypothetical incident that provides the catalyst for the exercise and is intended to introduce situations that will inspire responses and allow for demonstration of the exercise objectives
  - A list of questions regarding the scenario that address the exercise objectives
  - A copy of the IT plan being exercised

  The types of questions documented in the facilitator guide should be tailored to the participants. For example, if senior-level personnel are the participants, the questions should be of a more general, high-level nature and focus on decision-making and oversight, which are consistent with their roles and responsibilities within the plan. If operational personnel are the participants, the questions should typically focus on the specific procedures and processes for carrying out roles and responsibilities.

- A participant guide that includes the same information as the facilitator guide with a modified, shorter list of questions to orient participants to the types of issues that may be discussed during the exercise.
- An after action report

training
Instruction or learning activity to enhance the employee's capacity to perform specific job functions and tasks by focusing on skills, concepts, knowledge, and attitudes related to performing a job. It is designed to change what employees know and how they work.

> *NOTE:* References to training in US law: See U.S. Code § 4101 – Definitions [15]: (4) "training" means the process of providing for and making available to an employee, and placing or enrolling the employee in, a planned, prepared, and coordinated program, course, curriculum, subject, system, or routine of instruction or education, in scientific, professional, technical, mechanical, trade, clerical, fiscal, administrative, or other fields which will improve individual and organizational performance and assist in achieving the agency's mission and performance goals.

virtual-led
When instruction occurs in a virtual or simulated environment and is presented or facilitated by an instructor in real time.

warning banner
The opening screen that informs users of the implications of accessing a computer resource (e.g., consent to monitor). A security banner. System use notification.

web-based training
An internet-based session that allows learners to study independently and at their own pace with video, audio, and/or interactive techniques (e.g., drag-and-drop or fill in the blank). Built-in testing and accountability features can gauge performance.

work role
A grouping of work for which someone is responsible or accountable. Not synonymous with a job title or occupation, though they may coincide, depending on the organization. For example, the work role of "software developer" may apply to those with varying job titles, such as software engineers, coders, and application developers. Conversely, multiple roles could be combined to create a particular job. This additive approach supports improved modularity and illustrates the fact that all learners in the workforce perform numerous tasks in various roles, regardless of their job titles.

Appendix C. Change Log

In September 2024, the following changes were made to the report:

- Additional information was included to address requirements from OMB Circular A-130.
- This guidance leverages other relevant NIST publications that were released in the last 20 years, such as the NIST Cybersecurity Framework, NIST Risk Management Framework, NIST Privacy Framework.
- The terminology has been adapted to the standardized language found in the NICE Workforce Framework for Cybersecurity. The participants in the program are referred to as “learners,” and the overall program is now a “learning program.”
- This publication addresses issues that were identified in NIST research efforts with federal cybersecurity and privacy learning professionals (e.g., guidance for designing impactful metrics and measurements).