proofpoint.

WHITE PAPER

People-Centric Security Framework (PCSF)

Date Published: June 2020

Email questions to: dwatson@proofpoint.com

Acknowledgements

This publication is intended to be the result of a collaborative effort between Proofpoint and organizational and individual stakeholders in the public and private sectors. In developing the People-Centric Security Framework (PCSF), Proofpoint plans to rely upon public workshops, a notification for a request for comment (RFC), webinars and direct interactions with stakeholders. Proofpoint acknowledges and thanks all of those who contribute to this publication.

Those familiar with the National Institute of Standards and Technology (NIST) publications concepts may recognize that this framework seems familiar and is designed with similar constructs. Proofpoint recognizes the significant value of the NIST content and believes that using similar messaging will facilitate easier integration into an organization's existing cybersecurity programs. Reuse of any content is not meant to imply ownership, but rather is intended to remove the inconsistencies that often exist in security frameworks that are meant to be complementary. Well-known frameworks and a great deal of advice exist to help people protect data, privacy and devices, but minimize the implication of human factors due to the historical reliance on protecting the perimeter. The PCSF is intended to address this gap, focusing on people-centric factors. The PCSF complements and does not replace any NIST recommendations, an organization's risk management process or their cybersecurity program.

Table of Contents

Table of Contents

1. People-Centric Security Framework Introduction

The need for people-centric risk assessments to support enterprise risk management

For the last two decades, there has been a dissolution of the security perimeter. The unprecedented evolution of the internet and information technology has evolved how we live and work. The twenty-first century has brought an evolution of the work environment that requires more individuals than ever before to work outside of the office. Employees have always been our last line of defense, yet also the weakest link in our layered, defense-in-depth strategy. Today's employees often work from home, the coffee shop, the airport or the park where our traditional strategy does not apply. With individuals relocating outside of their secured environments, we are forced to reevaluate our principles of protection to support innovation and economic growth.

Using a transparent, consensus-based process, including both private and public stakeholders, to produce this voluntary tool, Proofpoint is publishing this People-Centric Security Framework: A Tool for Improving Security through People-Centric Risk Management (PCSF) to enable better people risk practices and help organizations protect confidentiality, integrity and availability of their environments. PCSF can support organizations by:

- Building customers' trust through identifying relevant threats to their workforce or threats directed through organizations against other organizations
- Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment
- Facilitating communication about people-centric risk practices with individuals, business partners, assessors and regulators.

People are the foundation upon which success is built. This tool for People-Centric Security (PCS) is intended to be widely usable by organizations of all sizes and is agnostic to any technology, vendor, sector, law or jurisdiction. People-centric protection should allow an organization to make risk-based choices, with effective risk mitigations engineered into products and services. It is the intent that this framework will help organizations move one step closer to having people recognized as the new enterprise edge.

1.1 Overview of the people-centric security framework

As shown in Figure 1, the PCSF Framework is composed of three parts: Core, Profiles and Implementation Tiers. Each component reinforces how organizations manage PCS risk through the connection between business or mission drivers, organizational roles and responsibilities and PCS protection activities. As further explained in section 2:

- The **Core** is a set of people-centric security protection activities and outcomes that allows for communicating prioritized PCS protection activities and outcomes across an organization from the executive level to the implementation/operations level. The Core is further divided into key Categories and Subcategories that are discrete outcomes for each Function.
- A **Profile** represents an organization's current people-centric security activities or desired outcomes. To develop a Profile, an organization can review the outcomes and activities in the Core to determine which are most important to focus on based on business or mission drivers, ecosystem role(s), types of business processes and individual needs. An organization can create or add Functions, Categories and Subcategories as needed. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "current" Profile (the "as is" state) with a "target" Profile (the "to be" state). Profiles can be used to conduct self-assessments and to communicate within an organization or between organizations about how PCS risks are being managed.
- **Implementation Tiers** provide a point of reference on how an organization views PCS risk and whether it has adequate processes and resources in place to manage that risk. Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk informed. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices, the degree of integration of PCS risk into its enterprise risk management portfolio, its ecosystem relationships and its workforce composition and training program.

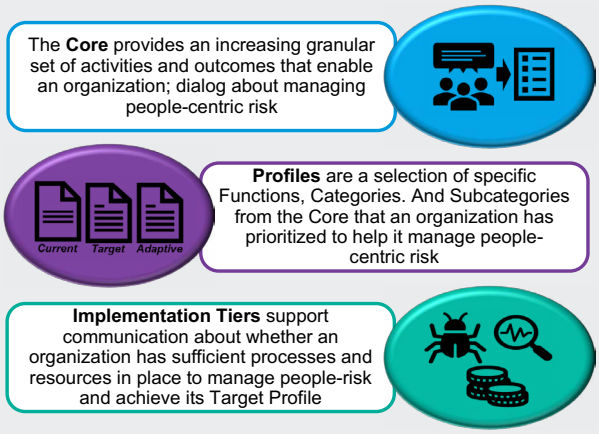

Figure 1: Core, Profiles and Implementation Tiers.

1.2 People-Centric Security Risk Management

While some organizations understand individual PCS risk management factors, a common understanding of many aspects of this topic is still not widely understood. To promote broader understanding, this section covers concepts and considerations that organizations may use to develop, improve or communicate about PCS risk management practices.

1.2.1 Cybersecurity and people-centric risk management

Since its release in 2014, the NIST Cybersecurity Framework[1] has helped organizations to communicate and manage cybersecurity risk. While managing cybersecurity risk contributes to managing PCS risk, it is not enough, as PC risks can also arise by means unrelated to cybersecurity incidents, as illustrated by Figure 2. The human element is considered the last line of defense. Social engineering, malicious insiders and vulnerable insiders can all contribute to a system where that last line of defense fails. Well-known frameworks and a great deal of advice exist to help people protect data, privacy and devices, but minimize the implication of human factors. The PCSF intends to address this gap, focusing on people-centric factors.[2] Having a general understanding of the different origins of cybersecurity and people-centric risks is important for determining the most effective solutions to address the risks.

The PCSF approach to PC risk is to consider PCS events as potential problems that individuals could experience arising from system, product or service operations with actions, whether in digital or non-digital form, through a complete lifecycle, from user activity data collection through disposal.

The PCS framework describes these user actions in the singular as a user action and collectively as user activities. The problems individuals can experience as a result of user activities can be expressed in various ways. NIST describes them as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss or physical harm.

The basis for the problems that individuals may experience can vary. As depicted in Figure 2, problems arise as an adverse effect of user-related activities that organizations perform to meet their mission or business objectives. An example is where accounting payment process are sidelined by social engineering. The ability of attackers to convince users to deviate from standard operating procedures has repeatedly resulted in financial loss and embarrassment. Since 2013, the FBI began tracking business email compromise (BEC), which has affected large and small companies and organizations in every U.S. state and more than 100 countries around the world.[3]

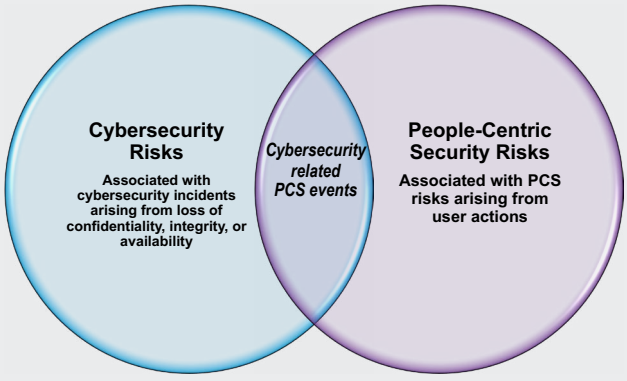

Figure 2: Cybersecurity and PCS Risks Relationship.

In an increasingly connected world, some problems can arise simply from individuals' interactions with systems, products and services, even when following processes that have been in place for many years. For example, vendor communications, such as when and to whom you should remit payments, can be impersonated to alter or influence people's behavior.[4] Figure 2 shows these types of cybersecurity-related PCS events as the overlap between PCS risks and cybersecurity risks.

Once an organization can identify the likelihood of any given problem arising from user activities, which the PCS Framework refers to as a problematic user action, it can assess the impact should the problematic user action occur. This impact assessment is where PCS risk and organizational risk intersect. Individuals, whether singly or in groups (including at a societal level) experience the direct impact of problems. As a result of the problems individuals experience, an organization may experience impacts such as noncompliance costs, revenue loss arising 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 problems that individuals experience to these well-understood organizational impacts, organizations can bring PCS risk into parity with other risks they are managing in their broader portfolio and drive more informed decision-making about resource allocation to strengthen PCS programs. Figure 3 illustrates this relationship between PCS risk and organizational risk.

1.2.2 People-centric risk assessment

PCS risk management is a cross-organizational set of processes that helps organizations to understand how their systems, products and services may create problems for individuals and how to develop effective solutions to manage such risks. PCS risk assessment is a sub-process for identifying and evaluating specific PCS risks. In general, PCS risk assessments produce the information that can help organizations weigh the benefits of the user action against the risks and to determine the appropriate response—sometimes referred to as proportionality.[4] Organizations may choose to prioritize and respond to PCS risk in different ways, depending on the potential impact to individuals and the resulting impacts to. Response approaches include:[5]

- Mitigating the risk (example: organizations may be able to apply technical and/or policy measures to the systems, products or services that minimize the risk to an acceptable level)
- Transferring or sharing the risk (example: contracts are a means of sharing or transferring risk to other organizations; acceptable use and consent mechanisms are a means of sharing risk with individuals);
- Avoiding the risk (example: organizations may determine that the risks outweigh the benefits and forego or terminate user activities)
- Accepting the risk (example: organizations may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).

Figure 3: Relationship Between PCS Risk and Organizational Risk.

PCS risk assessments are particularly important because, as noted above, PCS is a condition that safeguards multiple principles. The methods for safeguarding these principles may differ, and may conflict with each other. Depending on its objectives, if an organization is trying to achieve PCS by limiting access, this may lead to implementing measures such as distributed architectures or PCS-enhancing cryptographic techniques that hide data even from the organization. If an organization is also trying to enable auditing of user activities, the measures could conflict. For example, if an individual requests access to user activity data when analyzing an event, the organization may not be able to produce the user activity data if the data has been distributed or encrypted in ways the organization cannot access. PCS risk assessments can help an organization understand, in each context, the principles to protect, the methods to employ and how to balance implementation of different types of measures.

Lastly, PCS risk assessments help organizations distinguish between PCS risk and compliance risk. Identifying if user activities could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision making in system, product and service design or deployment. Although there is no objective standard for ethical decision-making, it is grounded in the norms, values and legal expectations of society. This facilitates optimizing beneficial utility of user activities while minimizing adverse consequences for individuals' PCS and society, as well as avoiding losses of trust that damage organizations' reputations, slow adoption or cause abandonment of products and services.

See **Appendix D** for more information on the operational aspects of PCS risk assessment.

1.3 Document overview

The remainder of this document contains the following sections and appendices:

- **Section 2** describes the PCSF components: Core, Profiles and Implementation Tiers.
- **Section 3** presents examples of how the PCSF can be used.
- The **References** section lists the references for the document.
- **Appendix A** presents the PCSF Core in a tabular format: Functions, Categories Subcategories.
- **Appendix B** contains a glossary of selected terms.
- **Appendix C** lists acronyms used in this document.
- **Appendix D** considers key practices that contribute to successful privacy risk management.
- **Appendix E** defines the Implementation Tiers.
- **Appendix F** identifies controls that can be used to measure maturity state

2. People-Centric Security Framework Basics

PCSF provides a common language for understanding, managing and communicating PCS risk with internal and external stakeholders. The PCSF language and construct is modeled on the NIST Privacy Framework[6] concepts:

- It is adaptable to any organization's role(s) in the ecosystem.
- It can be used to help identify and prioritize actions for reducing PCS risk.
- It is a tool for aligning policy, business and technological approaches to managing that risk.

2.1 Core principles

As set forth in Appendix A, the Core provides an increasingly granular set of activities and outcomes that enable a dialogue about managing PCS risk. As depicted in Figure 4, the Core comprises Functions, Categories and Subcategories.

The Core elements work together:

- Functions organize foundational PCS activities at their highest level. They aid an organization with expressing its management of PCS risk by understanding and managing user privileges and user activity flows, enabling risk management decisions, determining how to interact with individuals and improving by learning from previous activities. They are not intended to form a serial path or lead to a static desired end state. Rather, the functions should be performed concurrently and continuously to form or enhance an operational culture that addresses the dynamic nature of PCS risk. While the functions can be viewed as illustrated in Figure 4, the Governance, Risk and Compliance (GRC) function is an overarching concept providing the umbrella for People, Process and Technology, as illustrated in Figure 6 on page 12.
- Categories are the subdivisions of a Function into groups of PCS outcomes closely tied to programmatic needs and activities.
- Subcategories further divide a Category into specific outcomes of technical and/or management activities. They provide a set of results that, while not exhaustive, help support achievement of the outcomes in each Category.

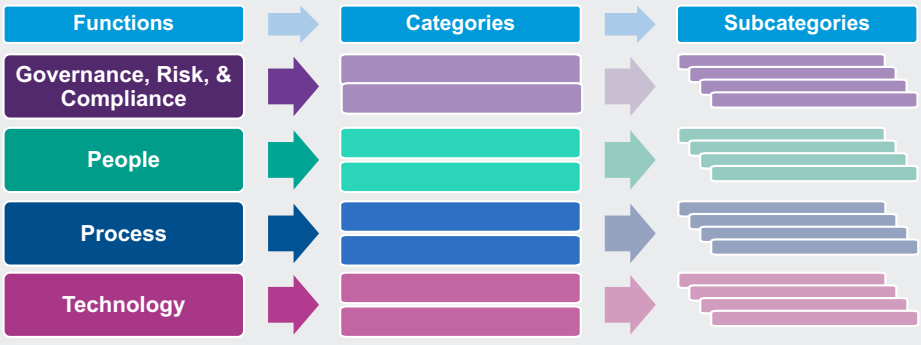

Figure 4: PCSF Core Functions.

The four Functions—GRC, People, Process and Technology—defined below can be used to manage PCS risks arising from user activity. GRC is mainly focused on managing risks associated with cybersecurity-related PCS events, such as data loss. The Cybersecurity Framework, although intended to cover all types of cybersecurity incidents, can be leveraged to further support the management of risks associated with the cybersecurity-related PCS events by using the Detect, Respond and Recover Functions, which are similar to the recommended use of the Privacy Framework. The PCSF is designed to complement the Cybersecurity Framework or the Privacy Framework. Organizations may use all five of the Cybersecurity Framework Functions in conjunction with PCSF Functions of People, Process and Technology to collectively address people-centric and cybersecurity risks. Figure 5 uses the Venn diagram from section 1.2.1 to demonstrate how the Functions from both frameworks can be used in varying combinations to manage different aspects of PCS risks.

The four PCSF Functions are defined as follows:

- **GRC**: Develops the organizational understanding to manage PCS risk for individuals arising from user actions.

  The activities from the GRC Function are foundational for effective use of the PCSF. They include: establishing organizational principles and policies, identifying legal/regulatory requirements, understanding risk tolerance and appetite, inventorying the privilege under which user activity data are processed, understanding the motivations of individuals directly or indirectly served or affected by the organization and conducting risk assessments to enable an organization to understand the business environment in which it is operating and identify and prioritize people-centric risks. Once established, oversight needs to be applied to identify gaps and apply focus for continuous improvement and compliance to legal and regulatory requirements in addition to business goals.

- **People**: Develop and implement organizational communication, culture and security training and awareness activities to enable organizations and individuals to have a reliable understanding and engage in a dialogue about how privileges are managed, how user activity flows and the associated PCS risks.

  The People Function recognizes that both organizations and individuals may need to know how user activity flows and privileges are managed and user activity flows through the organization in order to manage PCS risk effectively, with overlap between people-centric and cybersecurity risk management.

- **Process**: Develop and implement appropriate processes to enable organizations or individuals to manage privileges and controls with enough granularity to manage people-centric risks.

  The Process Function considers privilege and user activity flow management from the standpoint of both organizations and individuals, with overlap between people-centric and cybersecurity risk management.

- **Technology**: Develop and implement appropriate people-centric safeguards.

  The Technology Function covers controls to prevent cybersecurity-related PCS events, with overlap between people-centric and cybersecurity risk management.

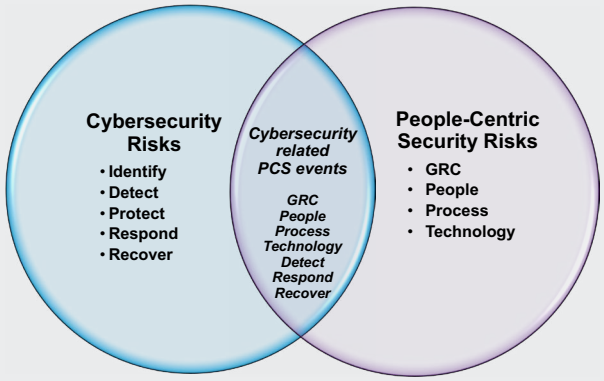

Figure 5: Using Functions to Manage Cybersecurity and PCS Risks.

2.2 Profiles

Profiles are a selection of specific Functions, Categories and Subcategories from the Core that an organization has prioritized to help it manage PCS risk. Profiles can be used to describe the current state and the desired target state of specific user activities. A Current Profile indicates PCS outcomes that an organization is currently achieving, while a Target Profile indicates the outcomes needed to achieve the desired PCS risk management goals. The differences between the two Profiles enable an organization to identify gaps, develop an action plan for improvement and gauge the resources that would be needed (examples: staffing, funding) to achieve PCS outcomes. This forms the basis of an organization's plan for reducing PCS risk in a cost-effective, prioritized manner. Profiles also can aid in communicating risk within and between organizations by helping organizations understand and compare the current and desired state of PCS outcomes.

Under the PCSF's risk- based approach, organizations may not need to achieve every outcome or activity reflected in the Core. When developing a Profile, an organization may select or tailor the Functions, Categories and Subcategories to its specific needs. This includes developing its own additional Functions, Categories and Subcategories to account for unique organizational risks. An organization determines these needs by considering its mission or business objectives, PCS principles and risk tolerance; role(s) in the organizational ecosystem or industry sector; legal/regulatory/privacy requirements and industry best practices; risk management priorities and resources; and the needs of individuals who are directly or indirectly served or affected by an organization's systems, products or services.

Adaptive profiles

Adaptive profiles are profiles that have been developed to address specific risk scenarios. Federal Information Processing Standards (FIPS) Publication 199 (FIPS PUB 199) provides guidance on categorizing information and information systems based on their security objectives (confidentiality, integrity and availability) and the potential impact of events jeopardizing them (low, moderate or high). PCSF utilizes the foundational concepts of FIPS PUB 199 to provide guidance on categorizing groups and individuals based on their people-centric security objectives (vulnerabilities, attack techniques, privilege and more) and the potential impact of PC events (strict, stricter, strictest; applied like low, moderate, high).

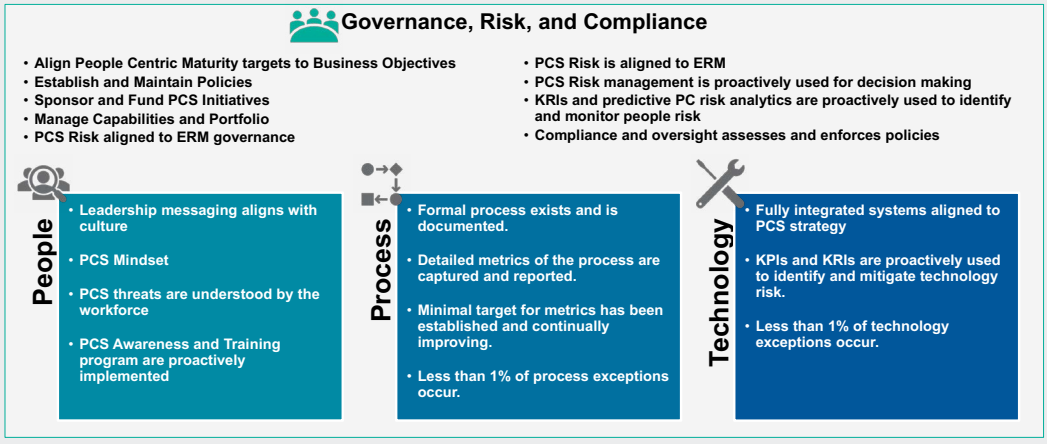

Figure 6: The GRC Function Is Overarching.

As illustrated in Figure 7, there is no specified order of development of Profiles and Adaptive Profiles. An organization may first develop a Target Profile in order to focus on its desired outcomes for PCS Risk and then develop a Current Profile to identify gaps. Alternatively, an organization may begin by identifying its current activities and then consider how to adjust these activities for its Target Profile. An organization may choose to develop Adaptive Profiles for different roles, systems, products or services or categories of individuals (examples: employees, customers) to enable better prioritization of activities and outcomes where there may be differing degrees of PCS risk. Organizations in a certain industry sector or with similar roles in the ecosystem may coordinate to develop common Profiles.

2.3 Implementation tiers

Tiers support organizational decision-making about how to manage PC risk by considering the nature of the PC risks engendered by an organization's systems, products or services and the sufficiency of the processes and resources an organization has in place to manage such risks. When selecting Tiers, an organization should consider its Target Profile(s) and how achievement may be supported or hampered by its current risk management practices; the degree of integration of PCS risk into its enterprise risk management portfolio; its ecosystem relationships; and its workforce composition and training program.

There are five distinct Tiers, Initial (Tier 0), Developing (Tier 1), Defined (Tier 2), Repeatable (Tier 3) and Adaptive (Tier 4). Descriptions are found in Appendix E. The Tiers represent a progression, though not a compulsory one. Although organizations at Tier 0 will likely benefit from moving to Tier 2, not all organizations need to achieve Tiers 3 or 4 (or may only focus on certain areas of these Tiers). Progression to higher Tiers is appropriate when an organization's processes or resources at its current Tier may be insufficient to help it manage its PCS risks.

An organization can use the Tiers to communicate internally about resource allocations necessary to progress to a higher Tier or as general benchmarks to gauge progress in its capability to manage PCS risks. An organization can also use Tiers to understand the scale of resources and processes of other organizations in the ecosystem and how they align with the organization's PCS risk management priorities. Nonetheless, successful implementation of PCSF is based upon achieving the outcomes described in an organization's Target Profile(s) and not upon Tier determination.

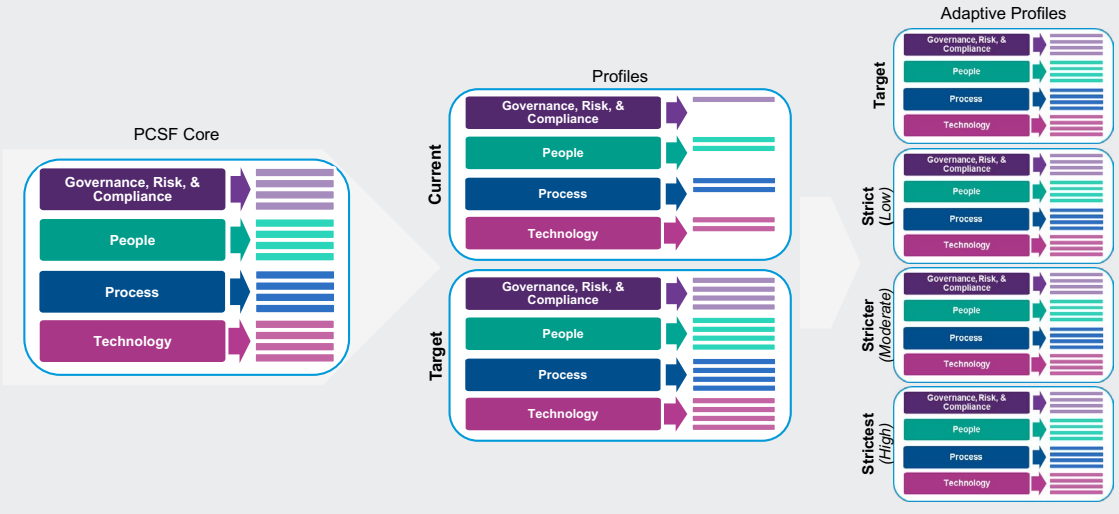

Figure 7: Relationship between Core, Profiles and Adaptive Controls.

3. How to Use the People-Centric Security Framework

When used as a risk management tool, the PCSF can help an organization with its efforts to optimize the development of innovative systems, products and services while minimizing adverse consequences for individuals. PCSF can help organizations answer this fundamental question: "How are we considering the impacts to individuals as we develop our systems, products and services?" To account for the unique needs of an organization, use of PCSF is flexible, although it is designed to complement existing business and system development operations. The decision about how to apply it is left to each organization. For example, an organization may already have robust risk management processes, but may use the Core's four Functions as a streamlined way to analyze and articulate any gaps. Alternatively, an organization seeking to establish a PCS program can use the Core's Categories and Subcategories as a reference. Other organizations may compare Profiles or Tiers to align PCS risk management priorities across different roles in the ecosystem. The variety of ways in which PCSF can be used by organizations should discourage the notion of "compliance with the PCSF" as a uniform or externally referenceable concept. The following subsections present a few options for use of PCSF.

3.1 Mapping to informative references

Organizations often crosswalk multiple frameworks to identify their requirements. Gaps in mappings can also be used to identify where additional or revised standards, guidelines and practices would help an organization to address emerging needs. An organization implementing a given Subcategory or developing a new Subcategory might discover that there is insufficient guidance for a related activity or outcome. To address that need, an organization might collaborate with technology leaders and/or standards bodies to draft, develop and coordinate standards, guidelines or practices.

3.2 Strengthening accountability

Accountability is generally considered a key PCS principle, although conceptually it is not unique to PCS.[7] Accountability occurs throughout an organization, and it can be expressed at varying degrees of abstraction, for example as a cultural value, as governance policies and procedures or as traceability relationships between PCS requirements and controls. PCS risk management can be a means of supporting accountability at all organizational levels as it connects senior executives who can communicate an organization's PCS principles and risk tolerance to those at the business/process manager level, who, in turn, can collaborate on the development and implementation of governance policies and procedures that support organizational PCS principles. These policies and procedures can then be communicated to those at the implementation/operations level, who collaborate on defining the PCS requirements that support the expression of the policies and PCS state, changes in risk, implementation progress and incident management activities procedures in an organization's systems, products and services. Personnel at the implementation/operations level also select, implement and assess controls as the technical and policy measures that meet the PCS requirements and report on progress, gaps and deficiencies, incident management and changing PCS risks so that those at the business/process manager level and the senior executives can better understand and respond appropriately.

Figure 8 provides a graphical representation of this bi-directional collaboration and communication and how elements of PCSF can be incorporated to facilitate the process. In this way, organizations can use PCSF as a tool to support accountability. They can also use PCSF in conjunction with other frameworks and guidance that provide additional practices to achieve accountability within and between organizations.[8]

3.3 Establishing or improving your cybersecurity strategy with the people-centric security framework

Using a simple model of "crawl, walk, run" phases, PCSF can support the creation of a new PCS program or improvement of an existing program like insider threats. As an organization goes through these phases, it may use the PCS Control Requirements to provide guidance on prioritizing or achieving outcomes.

Crawl

Effective PCS risk management requires an organization to understand its mission or business environment; its legal environment; its risk tolerance; the PCS risks engendered by its employees, systems, products or services; and its role(s) in the ecosystem. An organization can use the Governance Functions to prepare by reviewing the Categories and Subcategories and beginning to develop its Current Profile and Target Profile. Activities and outcomes, such as establishing organizational PCS principles and policies, determining and expressing an organizational risk tolerance and conducting PCS risk assessments (see Appendix D for more information on PCS risk assessments) provide a foundation for completing the Profiles in "Walk."

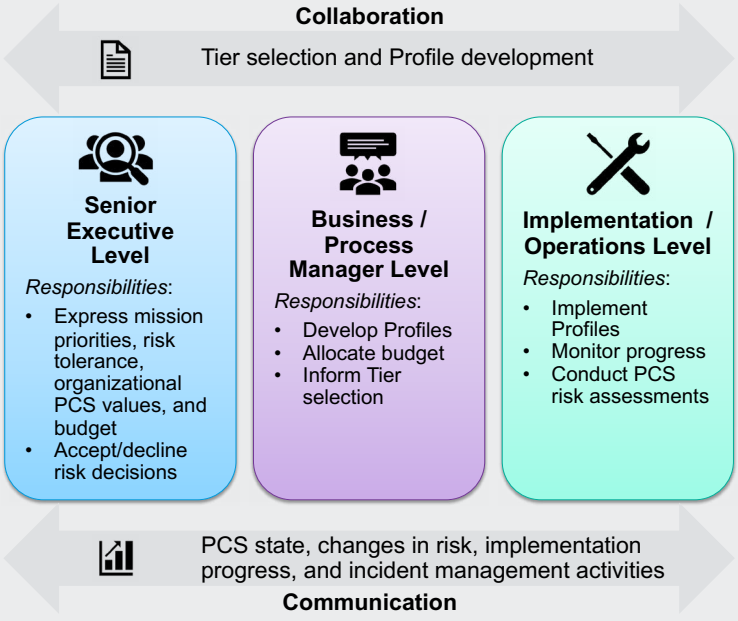

Figure 8: Notional Collaboration and Communication Flows Within an Organization.

Walk

An organization completes its Current Profile by indicating which Category and Subcategory outcomes from the remaining Functions are being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information. Informed by the activities under Governance, such as organizational PCS principles and policies, organizational risk tolerance and PCS risk assessment results, an organization completes its Target Profile focused on the assessment of the Categories and Subcategories describing its desired PCS outcomes. An organization also may develop its own additional Functions, Categories and Subcategories to account for unique organizational risks. It may also consider influences and requirements of external stakeholders, such as business customers and partners when creating a Target Profile. An organization can develop multiple Profiles to support its different business lines, processes or high-risk users, which may have different business needs and associated risk tolerances.

An organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps—reflecting mission drivers, costs and benefits and risks—to achieve the outcomes in the Target Profile. An organization using the Cybersecurity Framework and PCSF together may develop integrated action plans. It then determines resources, including funding and workforce needs, necessary to address the gaps, which can inform the selection of an appropriate Tier. Using Profiles in this manner encourages an organization to make informed decisions about PCS activities, supports risk management and enables an organization to perform cost-effective, targeted improvements.

Run

With the action plan defined, an organization prioritizes which actions to take to address any gaps and then adjusts its current PCS practices in order to achieve the Target Profile.[8]

An organization can go through the phases nonsequentially as needed to continuously assess and improve its PCS state. For instance, an organization may find that more frequent repetition of the activities in the Walk phase improves the quality of PCS risk assessments. Furthermore, an organization may monitor progress through iterative updates to the Current Profile or the Target Profile to adjust to changing risks, subsequently comparing the Current Profile to the Target Profile.

3.4 Applying to the system development lifecycle

The Target Profile can be aligned with the system development life cycle (SDLC) phases of plan, design, build/buy, deploy, operate and decommission to support the achievement of the prioritized PCS outcomes. Beginning with the plan phase, the prioritized PCS outcomes can be transformed into the PCS capabilities and requirements for the system, recognizing that requirements are likely to evolve during the remainder of the life cycle. A key milestone of the design phase is validating that the PCS capabilities and requirements match the needs and risk tolerance of an organization as expressed in the Target Profile. That same Target Profile can serve as an internal list to be assessed when deploying the system to verify that all PCS capabilities and requirements are implemented. The PCS outcomes determined by using PCSF should then serve as a basis for ongoing operation of the system. This includes occasional reassessment and capturing results in a Current Profile to verify that PCS capabilities and requirements are still fulfilled.

PCS risk assessments typically focus on the user activity lifecycle, the stages through which activity passes—often characterized as the data processes of creation or collection, processing, dissemination, use, storage and disposition—to include destruction and deletion. The PCS perspective prioritizes employment and external attacker viewpoints to inform data relationships and evaluate risk and assign controls. Factors to be considered include, but are not limited to, attraction, recruitment, onboarding, development, retention, exit, alumni or PCS building blocks selection, employment, onboarding, task fulfillment, development and discontinuation. Once people factors are identified, they should be aligned to the SDLC. This is performed by identifying and understanding user activity flows in relationship to data process flows during all stages of the SDLC. It helps organizations to better manage PCS risks and inform the selection and implementation of PCS Control Requirements, allowing an organization to reduce risk by meeting PCS requirements.

3.5 Using within the ecosystem

Human factors

Human factors are broken down by demographics, vulnerabilities, liability, medium, assets and context. Figure 9 illustrates one example of mapping human factors.

Organizations need to understand:

- People-based inherited and modified risk or avoid risk before engagement
- Motives, behavior and intentions, linking to risk potentials and capabilities
- People-centric infrastructure risk potentials and risks in within business processes

The human factors have evolved within the last decade, creating a necessity to alter our perimeter-based approach.

Demographics	Personality, Biographical Data, Education Social Role, Cultural Background, Age
Vulnerability	People Risk Vector (Intention, Oversight, Inexperience) Assumptions of the mindset (e.g. values & world view)
Liability	Argumentation Triangle (Motive, Opportunity, Justification) Shapes the stylistic elements (Vulnerability and Liability are expected to be particularly consistent)
Medium	Usage of medium and data drop zones (authorization, access) Examples of medium are files, mail, chats, CRM, ERP, etc.
Assets	Usage of different types of assets, systems and tools for performing user activities Vulnerability and Reliability of the different assets, tools and applications
Context	Usage of different types of assets, systems and tools for performing user activities Vulnerability and Reliability of the different assets, tools and applications

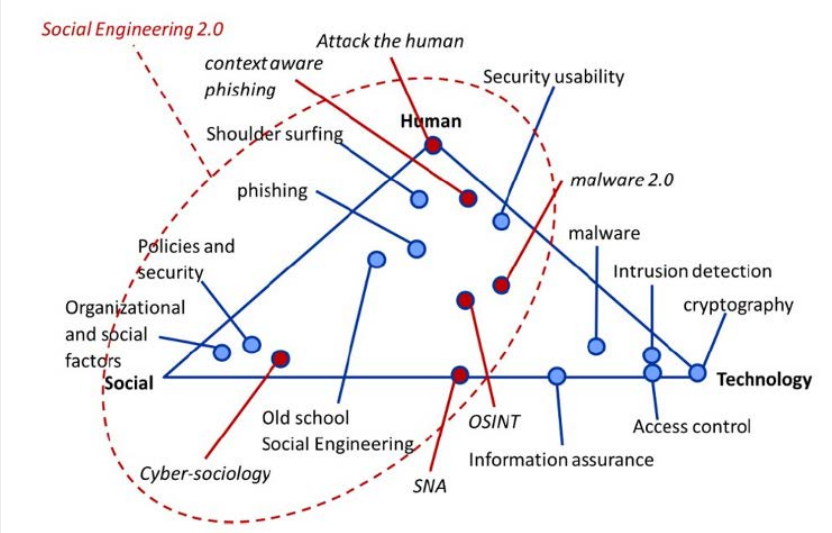

Figure 9: Human attack surface includes social and technical aspects.
Ref: https://www.dogana-project.eu

Ecosystem factors

A key factor in the management of PCS risk is an entity's role(s) in the ecosystem, which can affect not only its legal obligations, but also the measures it may take to manage PCS risk. As depicted in Figure 10, the organizational ecosystem encompasses a range of entities and roles that may have complex, multi-directional relationships with each other and individuals. Complexity can increase when entities are supported by a chain of sub-entities. For example, service providers may be supported by a series of service providers, or manufacturers may have multiple component suppliers. Figure 10 displays entities as having distinct roles, but some may have multiple roles, such as an organization providing services to other organizations and providing retail products to consumers. The roles in Figure 10 are intended to be notional classifications. In practice, an entity's role(s) may be legally codified—for example, some laws classify organizations as data controllers or data processors—or classifications may be derived from industry sector designations.

By developing one or more Profiles relevant to its role(s), an entity can use PCSF to consider how to manage PCS risk not only with regard to its own priorities, but also in relation to how the measures it may take affect other organizational ecosystem entities' management of PCS risk. For example:

- An organization that makes decisions about how to collect and use user activity data about individuals may use a Profile(s) to express PCS requirements to an external service provider (example: a cloud provider to which it is exporting data). The external service provider that processes the user activity data may use its Profile(s) to demonstrate the measures it has adopted to process user activity data in line with contractual obligations.
- An organization may express its PCS posture through a Current Profile to report results or to compare with acquisition requirements.

Figure 10: Organizational Ecosystem Relationships.

- An industry sector may establish common a Profile(s) that can be used by its members to customize their own Profiles.
- A manufacturer may use a Target Profile to determine the capabilities to build into its products so that its business customers can meet the PCS needs of their end users.
- A developer may use a Target Profile to consider how to design an application that enables PCS protections when used within other organizations' system environments.

PCSF provides a common language to communicate PCS requirements with entities within the organizational ecosystem. The need for this communication can be particularly notable when the organizational ecosystem crosses national boundaries, such as with international data transfers. Organizational practices that support communication may include:

- Determining PCS requirements
- Enacting PCS requirements through formal agreement (example: contracts, multi-party frameworks)
- Communicating how those PCS requirements will be verified and validated
- Verifying that PCS requirements are met through a variety of assessment methodologies
- Governing and managing the above activities

3.6 Informing buying decisions

Since either a Current or Target Profile can be used to generate a prioritized list of PCS requirements, these Profiles can also be used to inform decisions about buying products and services. By first selecting outcomes that are relevant to its PCS goals, an organization can then evaluate their partners' systems, products or services against this outcome. For example, if a device is being purchased for environmental monitoring of a forest, manageability may be important to support capabilities for auditing the processing of user activity data about people using the forest and should drive a manufacturer evaluation against applicable Subcategories in the Core to ensure PCS capabilities are included.

In circumstances where it may not be possible to impose a set of PCS requirements on the supplier, the objective should be to make the best buying decision among multiple suppliers, given a carefully determined list of PCS requirements. Often this means some degree of trade-off, comparing multiple products or services with known gaps to the Profile. If the system, product or service purchased did not meet all the objectives described in the Profile, an organization could address the residual risk through mitigation measures or other management actions.

References

1. Cyber Security Framework Version 1.1. *National Institute of Standards and Technology (NIST).* [Online] 2018. https://csrc.nist.gov/publications/detail/white-paper/2018/04/16/cybersecurity-framework-v11/final.

2. The Human Element of Cybersecurity. *Harvard Business Review.* [Online] 2017. https://hbr.org/insight-center/the-human-element-of-cybersecurity

3. Federal Bureau of Investigation (FBI). Business E-Mail Compromise | Federal Bureau of Investigation. *FBI Info.* [Online] https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise.

4. Necessity and Proportionality. *European Data Protection Supervisor.* [Online] 2019. http://edps.europa.edu/data-protection/our-work/subjects/necissity-proportionality_en.

5. NIST Special Publication (SP) 800-39, Managing Information Security Risk: Organization, Mission, and System Vlew. *National Institute of Standards and Technology (NIST).* [Online] 2011. https://doi.org/10.6028/NIST.SP.800-39.

6. Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0. *National Institute of Standards and Technology Technology (NIST).* [Online] 2020. https://doi.org/10.6028/NIST.CSWP.01162020.

7. Definitions. *Title 44 U.S. Code, Sec. 3542.* [Online] 2011. https://www.govinfo.gov/app/details/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapIII-sec3542.

8. NIST Special Publication (SP) 800-37, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. *National Institute of Standards and Technology.* [Online] 2018. https://doi.org/10.6028/NIST.SP.800-37r2.

9. NIST PRAM. *National Institute of Standards and Technoloy (NIST*). [Online] https://www.nist.gov/privacy-framework/nist-pram.

10. Initiative, Joint Task Force Transformation. NIST Special Publication (SP), Guide for Conducting Risk Assessments. *National Institute of Standards and Technology (NIST).* [Online] 2012. https://doi.org/10.6028/NIST.SP.800-30r1.

11. Joint Task Force Transformation Initiative. NIST Special Publication (SP) 800-53, Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations. *National Institute of Standards and Technology (NIST).* [Online] 2013. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft.20

Appendix A: People-Centric Framework Core

This appendix presents the Core: a table of Functions, Categories and Subcategories that describe specific activities and outcomes that can support managing people-centric security risks when systems, products and services are processing user activity data.

Note to users

Risk-based approach:

- *The Core is not a checklist of actions to perform. An organization selects Subcategories consistent with its risk strategy to integrate into the existing cybersecurity controls, as noted in Category statements.* An organization may not need to achieve every outcome reflected in the Core. It is expected that an organization will use Profiles to select and prioritize the Functions, Categories and Subcategories that best meet its specific needs by considering its goals, role in the organizational ecosystem or industry sector, legal/regulatory requirements and industry best practices, risk management priorities and the needs of the individuals who are serviced or affected by an organization's systems, products or services.
- It is not obligatory to achieve an outcome in its entirety. An organization may use its Profiles to express partial achievement of an outcome, as not all aspects of an outcome may be relevant for it to manage PCS risk, or an organization may use a Target Profile to express an aspect of an outcome that it does not currently have the capability to achieve.
- It may be necessary to consider multiple outcomes in combination to appropriately manage PCS risk.

Implementation:

The tabular format of the Core is not intended to suggest a specific implementation order or imply a degree of importance between the Functions, Categories and Subcategories. Implementation may be nonsequential, simultaneous or iterative, depending on the SDLC stage, status of the people-centric security integration into the cybersecurity program, scale of the workforce or role(s) of an organization in the organizational ecosystem. In addition, the Core is not exhaustive. It is extensible, allowing organizations, sectors and other entities to adapt or add additional Functions, Categories and Subcategories to their Profiles.

Roles:

- **Ecosystem Roles:** The Core is intended to be usable by any organization or entity, regardless of its role(s) in the organizational ecosystem. Although PCSF does not classify ecosystem roles, an organization should review the Core from its standpoint in the ecosystem. An organization's role(s) may be legally codified. For example, some laws classify organizations as data controllers or data processors, or classifications may be derived from industry designations. Since Core elements are not assigned by ecosystem role, an organization can use its Profiles to select Functions, Categories and Subcategories that are relevant to its role(s).
- **Organizational Roles:** Different parts of an organization's workforce may take responsibility for different Categories or Subcategories. For example, the legal department may be responsible for carrying out activities under "Compliance Policies, Processes and Procedures," while the IT department is working on "Inventory and Mapping." Ideally, the Core encourages cross-organizational collaboration to develop Profiles and achieve outcomes.
- **Scalability:** Certain aspects of outcomes may be ambiguously worded. For example, outcomes may include terms like "communicated" or "disclosed" without stating to whom the communications or disclosures are being made. The ambiguity is intentional to allow for a wide range of organizations with different use cases to determine what is appropriate or required in each context.

Cybersecurity framework alignment:

- As noted in section 2.1, organizations can use the four PCS Framework Functions—Governance, People, Process and Technology—to manage PCS risks arising from user activities. Process and Technology are focused on managing risks associated with security-related PCS events. To further support the management of risks associated with security-related PCS events, organizations may choose to use Detect, Respond and Recover Functions from the Cybersecurity Framework. For this reason, these Functions are included in Table 1, but are greyed out. Alternatively, organizations may use all five of the Cybersecurity Framework Functions in conjunction with Governance, People, Process and Technology to collectively address PCS and security risks. See Figure 5 for an illustrated example of how the Functions from both frameworks can be used in varying combinations to manage different aspects of PCS and cybersecurity risks.

  Certain Functions, Categories, Subcategories or concepts may be identical to or have been adapted from the Cybersecurity Framework or Privacy Framework.

- **Core Identifiers:** For ease of use, each component of the Core is given a unique identifier. Functions and Categories each have a unique alphabetic identifier, as shown in Table 1. Subcategories within each Category have a number added to the alphabetic identifier. The unique identifier for each Subcategory is included in Table 2.

Table 1: PCS Framework Function and Category Unique Identifiers

FUNCTION UNIQUE IDENTIFIER	FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
GR	Governance, Risk and Compliance	GR.BE	Business Environment
		GR.CO	Compliance and Oversight
		GR.GP	Governance Policies
		GR.IM	Inventory and Mapping
		GR.OE	Organizational Ecosystem Risk
		GR.RA	Risk Assessment
		GR.RM	Risk Management Strategy
PL	People	PL.AT	Awareness and Training
		PL.RR	Roles and Responsibilities
PR	Process	PR.GP	Governance Processes and Procedures
		PR.AC	Identity Management, Authentication and Access Control
		PR.AP	Associated Processing
		PR.DS	User Activity Data Security
		PR.MA	Maintenance
IT	Technology	IT.PM	PCS Management
		IT.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 2: People-Centric Security Framework Core

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
Governance, Risk and Compliance: Develop the organizational understanding to manage and oversee PCS risk for individuals arising from user activities.	Business Environment (GR.BE): The organization's mission, objectives, stakeholders and activities are understood and prioritized. This information is used to inform PCS roles, responsibilities and risk management decisions.	GR.BE-1: The organization's role(s) in the organizational ecosystem are identified and communicated.
		GR.BE-2: Priorities for organizational mission, objectives and activities are established and communicated.
		GR.BE-3: Systems/products/services that support organizational priorities are identified and key requirements communicated.
		GR.BE-4: Dependencies and critical functions for delivery of critical services are established and included in the user activity inventory
		GR.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (example: under duress/attack, during recovery or normal operations).
	Compliance and Oversight (GR.CO)	GR.CO-1: Legal, regulatory and contractual requirements regarding PCS are understood and managed.
		GR.CO-2: PCS risk is re-evaluated on an ongoing basis and as key factors, including the organization's business environment (example: introduction of new technologies), governance (examples: legal obligations, risk tolerance), user activities and systems/products/services change.
		GR.CO-3: PCS principles, policies and training are reviewed and communicated.
		GR.CO-4: Policies, processes and procedures for assessing compliance with legal requirements and PCS policies are established and in place.
		GR.CO-5: Policies, processes and procedures for communicating progress on managing PCS risks are established and in place.
		GR.CO-6: Policies, processes and procedures are established and in place to receive, analyze and respond to problematic user activities disclosed to the organization from internal and external sources (examples: internal discovery, researchers professional events).
		GR.CO7: Policies, processes and procedures incorporate lessons learned from problematic user activities.
		GR.CO-8: Policies, processes and procedures for receiving, tracking and responding to complaints, concerns and questions from individuals about organizational PCS practices are established and in place.
	Governance Policies (GR.GP): The policies to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and inform the management of PCS risk.	GR.PO-1: Organizational PCS principles and policies are established and communicated.
		GR.PO-2: Governance and risk management policies, processes and procedures address PCS risks.
		GR.PO-3: Policies, processes and procedures for authorizing user activities (examples: organizational decisions, individual consent), revoking authorizations and maintaining authorizations are established and in place.
		GR.PO-4: Policies, processes and procedures for enabling user activities are established and in place.
		GR.PO-5: Policies, processes and procedures for enabling individuals' user activities and requests are established and in place.
		GR.PO-6: A user activity lifecycle to manage user roles/profiles is aligned and implemented with the system development lifecycle to manage systems.
		GR.PO-7: Transparency policies, processes and procedures for communicating PCS purposes, practices and associated PCS risks are established and in place.

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
Governance, Risk and Compliance: Develop the organizational understanding to manage and oversee PCS risk for individuals arising from user activities.	Inventory and Mapping (GR.IM): User actions by systems, products or services is understood and informs the management of PCS Risk	GR.IM-1: Systems, products and services that users interact with are inventoried.
		GR.IM-2: Ecosystem Owners or operators (example: the organization or third parties, such as service providers, partners, customers and developers) and their roles with respect to the systems/products/services and components (example: internal or external) that users interact with are inventoried.
		GR.IM-3: Categories of individuals (examples: customers, employees or prospective employees, consumers) whose interact with the organization are inventoried.
		GR.IM-4: User activities of the systems, products and services are inventoried.
		GR.IM-5: The purposes for the user activities are inventoried.
		GR.IM-6: Action elements within the user activities are inventoried.
		GR.IM-7: The user environment is identified (examples: geographic location, internal, cloud, third parties).
		GR.IM-8: User activities flows are mapped, illustrating the user actions and associated activity elements for systems, products and services, including components, roles of the component owners/operators and interactions of individuals or third parties with the systems, products services.
	Organizational Ecosystem Risk (GR.OE): The organization's priorities, constraints, risk tolerance and assumptions are established and used to support risk decisions associated with managing PCS risk and third parties within the organizational ecosystem. The organization has established and implemented the processes to identify, assess and manage PCS risks within the organizational ecosystem.	GR.OE-1: Organizational ecosystem risk management policies, processes and procedures are identified, established, assessed, managed and agreed to by organizational stakeholders.
		GR.OE-2: Organizational ecosystem parties (examples: service providers, customers, partners, product manufacturers, application developers) are identified, prioritized and assessed using a PCS risk assessment process
		GR.OE-3: Contracts with organizational ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's PCS program.
		GR.OE-4: Interoperability frameworks or similar multi-party approaches are used to manage organizational ecosystem PCS risks.
		GR.OE-5: Organizational ecosystem parties are routinely assessed using audits, test results or other forms of evaluations to confirm they are meeting their contractual, interoperability framework or other obligations.
	Risk Assessment (GR.RA): The organization understands the PCS risks to individuals and how such PCS risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (examples: compliance, financial), reputation, workforce and culture.	GR.RA-1: Contextual factors related to the systems/products/services and the user actions are identified (examples: individuals' vulnerabilities, attack demographics, privilege and visibility of user activities to individuals and third parties).
		GR.RA-2: User behavior analytic inputs and outputs are identified and evaluated for bias.
		GR.RA-3: Potential problematic user activities and associated problems are identified.
		GR.RA-4: Problematic user activities, likelihoods and impacts are used to determine and prioritize risk.
		GR.RA-5: Risk responses are identified, prioritized and implemented.
	Risk Management Strategy (GR.RM): The organization's priorities, constraints, risk tolerances and assumptions are established and used to support operational risk decisions.	GR.RM-1: Risk management processes are established, managed and agreed to by organizational stakeholders.
		GR.RM-2: Organizational risk tolerance is determined and clearly expressed.
		GR.RM-3: The organization's determination of risk tolerance is informed by its role(s) in the organizational ecosystem.

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
People	Awareness and Training (PL.AT)	PL.AT-1: The workforce is informed and trained on its roles and responsibilities.
		PL.AT-2: Senior executives understand their roles and responsibilities.
		PL.AT-3: PCS personnel understand their roles and responsibilities.
		PL.AT-4: Third parties (examples: service providers, customers and partners) understand their roles and responsibilities.
		PL.AT-5: Roles and responsibilities (example: public relations) for communicating PCS purposes, practices and associated PCS risks are established.
		PL.AT-6: Mechanisms (examples: notices, internal or public reports) for communicating PCS purposes, practices, associated PCS risks and options for enabling individuals' user roles and requests are established and in place.
		PL.AT-7: Mechanisms for obtaining feedback from individuals (examples: surveys or focus groups) about PCS and associated PCS risks are established and in place.
		PL.AT-8: System, product and service design enables user activity flow visibility.
		PL.AT-9: Records of PCS events, disclosure and sharing are maintained and can be accessed for review or transmission or disclosure.
		PL.AT-10: User activity flow corrections or deletions can be communicated to individuals or organizations in the ecosystem.
		PL.AT-11: User activity provenance and lineage are maintained and can be accessed for review or transmission or disclosure.
		PL.AT-12: Impacted individuals and organizations are notified about a PCS related breach or event.
		PL.AT-13: Individuals are provided with mitigation mechanisms (examples: user data alteration or deletion) to address impacts of problematic user activities.
		PL.AT-14: Physical and cybersecurity personnel understand their roles and responsibilities.
	Roles and Responsibilities (PL.RR)	PL.RR-1: Roles and responsibilities for the workforce are established with respect to PCS.
		PL.RR-2: PCS roles and responsibilities are coordinated and aligned with third-party stakeholders (examples: service providers,

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
Process (PR): The processes and procedures to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and address appropriate user activity safeguards.	Governance Processes and Procedures (PR.GP): PCS processes and procedures are maintained and used to manage the protection of user activities.	PR.GP-1: Processes to instill organizational PCS principles within system, product and service development and operations are established and in place.
		PR.GP-2: A baseline configuration of information technology is created and maintained incorporating security principles (example: concept of least privilege).
		PR.GP-3: Configuration change control processes are established and in place.
		PR.GP-4: Backups of user activity information are conducted, maintained and tested.
		PR.GP-5: Policy and regulations regarding the physical operating environment for organizational assets are met.
		PR.GP-6: Protection processes are improved.
		PR.GP-7: Effectiveness of protection technologies is shared.
		PR.GP-8: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place and managed.
		PR.GP-9: Response and recovery plans are tested.
		PR.GP-10: PCS specific procedures are included in human resources practices (examples: deprovisioning, personnel screening).
		PR.GP-11: A vulnerability management plan is developed and implemented.
	Identity Management, Authentication and Access Control (PR.AC): Access to data and devices is limited to authorized individuals, processes and devices and is managed consistent with the assessed risk of unauthorized access.	PR.AC-1: Identities and credentials are issued, managed, verified, revoked and audited for authorized individuals, processes and devices.
		PR.AC-2: Physical access to data and devices is managed.
		PR.AC-3: Remote access is managed.
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.
		PR.AC-5: Network integrity is protected (examples: network segregation, network segmentation).
		PR.AC-6: Individuals and devices are proofed and bound to credentials and authenticated commensurate with the risk of the transaction (examples: individuals' PCS risks and other organizational risks).
		PR.AC-7: Cybersecurity is included in human resources practices (examples: deprovisioning, personnel screening).
	Disassociated Processing (PR.AP): User activity data processing solutions increase disassociability consistent with the organization's risk strategy to protect individuals' activities and enable implementation of PCS principles (examples: user activity data minimization).	PR.AP-1: User activity data are processed to decrease observability and linkability while adhering to organizational PCS requirements.
		PR.AP-2: Data are processed to limit the identification of individuals (examples: de-identification privacy techniques, tokenization).
		PR.AP-3: User activity data are processed to limit the formulation of inferences about individuals' behavior or activities.
		PR.AP-4: System or device configurations permit selective collection or disclosure of user activity data elements.
		PR.AP-5: Attribute references are substituted for attribute values. (example: when data is aggregated)

FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
Process (PR): The processes and procedures to manage and monitor the organization's regulatory, legal, risk, environmental and operational requirements are understood and address appropriate user activity safeguards.	User Activity Data Security (PR.DS): User activity data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity and availability.	PR.DS-1: Data-at-rest is protected.
		PR.DS-2: Data-in-transit is protected.
		PR.DS-3: Systems, products and services and associated data are formally managed throughout removal, transfers and disposition.
		PR.DS-4: Adequate capacity to ensure availability is maintained.
		PR.DS-5: Protections against data leaks are implemented.
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware and information integrity.
		PR.DS-7: The development and testing environment(s) are separate from the production environment.
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.
	Maintenance (PR.MA): System maintenance and repairs are performed consistent with policies, processes and procedures.	PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.
		PR.MA-2: Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.
Technology (IT)	PCS Management (IT.PM): User Profiles are managed consistent with the organization's risk strategy to protect individuals' liability, increase manageability and enable the implementation of PCS principles (examples: individual participation, user activity quality, user data minimization).	IT.PM-1: User activity elements can be accessed for review.
		IT.PM-2: User activity elements can be accessed for transmission or disclosure.
		IT.PM-3: User activity elements can be accessed for alteration.
		IT.PM-4: User activity elements can be accessed for deletion.
		IT.PM-5: User activity data are destroyed according to policy.
		IT.PM-6: Data are transmitted using standardized formats.
		IT.PM-7: Mechanisms for transmitting user privileges and related values with user activities are established and in place.
		IT.PM-8: Audit/log records are determined, documented, implemented and reviewed in accordance with policy and incorporating the principle of user data minimization.
		IT.PM-9: Technical measures implemented to manage data processing are tested and assessed.
		IT.PM-10: Stakeholder PCS preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.
	Protective Technology (IT.PT): Technical security solutions are managed to ensure the security and resilience of systems, products, services and associated data consistent with related policies, processes, procedures and agreements.	IP.PT-1: Removable media is protected, and its use restricted according to policy.
		IP.PT-2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
		IP.PT-3: Communications and control networks are protected.
		IP.PT-4: Mechanisms (examples: failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

Appendix B: Glossary

This appendix defines selected terms used for the purposes of this publication.

Attribute Reference (NIST SP 800-63-3)	A statement asserting a property of a subscriber without necessarily containing identity information, independent of format. For example, for the attribute "birthday," a reference could be "older than 18" or "born in December."
Attribute Value (NIST SP 800-63-3)	A complete statement asserting a property of a subscriber, independent of format. For example, for the attribute "birthday," a value could be "12/1/1980" or "December 1, 1980."
Availability (44 U.S.C.)	Ensuring timely and reliable access to and use of information.
Category	The subdivision of a Function into groups of people-centric security outcomes closely tied to programmatic needs and activities.
Confidentiality (44 U.S.C.)	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Core	A set of PCS protection activities and outcomes. The Framework Core comprises three elements: Functions, Categories and Subcategories.
Function	A component of the Core that provides the highest level of structure for organizing basic people-centric security activities into Categories and Subcategories.
Implementation Tier	Provides a point of reference on how an organization views PCS risk and whether it has enough processes and resources in place to manage that risk.
Individual	A single person or a group of persons, including at a societal level.
Integrity (44 U.S.C.)	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
People-Centric Security Risk	The likelihood that individuals will experience problems resulting from an individual action, and the impact should they occur.
People-Centric Security Risk Assessment	A people-centric security risk management sub-process for identifying and evaluating specific PCS risks.
Profile	A selection of specific Functions, Categories and Subcategories from the Core that an organization has prioritized to help it manage people-centric risk.
Risk (NIST SP 800-30)	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence.

Appendix C: Acronyms

This appendix defines selected acronyms used in the publication.

GRC	Governance, Risk and Compliance
IT	Information Technology
KPI	Key Performance Indicator
KRI	Key Risk Indicator
PCS	People-Centric Security
PCSF	People-Centric Security Framework
SDLC	System Development Lifecycle

Appendix D: People-Centric Risk Management Practices

Section 1.2 introduces multiple considerations around PCS risk management, including the relationship between cybersecurity and PCS risk and the role of PCS risk assessment. This appendix considers some of the key practices that contribute to successful PCS risk management, including organizing preparatory resources, determining PCS capabilities, defining PCS requirements, conducting PCS risk assessments, creating PCS requirements traceability and monitoring for changing PCS risks. Category and Subcategory references are included to facilitate use of the Core to support these practices; these references appear in parentheticals.

Organizing preparatory resources

The appropriate resources facilitate informed decision-making about PCS risks at all levels of an organization. As a practical matter, the responsibility for the development of various resources may belong to different components of an organization. Therefore, a component of an organization, depending on certain resources, may find that they either do not exist or may not sufficiently address PCS. In these circumstances, the dependent component can consider the purpose of the resource and either seek the information through other sources or make the best decision it can with the available information. In short, good resources are helpful, but any deficiencies should not prevent organizational components from making the best risk decisions they can within their capabilities.

The following resources, while not exhaustive, build a foundation for better decision-making.

Risk management role assignments (PL.RR)

Establishing and enabling cross-organizational understanding of who is accountable and who has responsibility for PCS risk management as well as other risk management tasks in an organization supports better coordination and accountability for decision-making. In addition, a broad range of perspectives can improve the process of identifying, assessing and responding to PCS risks. A diverse and cross-functional team can help identify a more comprehensive range of risks to individuals' activities and select a wider set of mitigations. Determining which roles to include in the risk management discussions depends on organizational context and makeup, although collaboration between an organization's PCS and cybersecurity programs will be important. If one individual is being assigned to multiple roles, managing potential conflicts of interest should be considered.

Enterprise risk management strategy (GR.RM)

An organization's enterprise risk management strategy helps to align an organization's mission and values with organizational risk tolerance, assumptions, constraints and priorities. Limitations on resources to achieve mission or business objectives and to manage a broad portfolio of risks will likely require trade-offs. Enabling personnel involved in the PCS risk management process to better understand an organization's risk tolerance should help to guide decisions about how to allocate resources and improve decisions around risk response.

Key stakeholders (PL.RR-2, GR.OE-3)

PCS stakeholders are those who have an interest or concern in the PCS outcomes of the system, product or service. For example, legal concerns likely focus on whether the system, product or service is operating in a way that would cause an organization to be out of compliance with privacy laws or regulations or its business agreements. Business owners that want to maximize usage may be concerned about loss of trust in the system, product or service due to poor privacy. Individuals whose data are being processed or who are interacting with the system, product or service will be interested in not experiencing problems or adverse consequences. Understanding the stakeholders and the types of PCS outcomes they are interested in will facilitate system/product/service design that appropriately addresses stakeholders' needs.

Organizational-level PC requirements (GR.PO)

Organizational-level PCS requirements are a means of expressing the legal obligations, PCS principles and PCS policies to which an organization intends to adhere. Understanding these requirements is key to ensuring that the system/product/service design complies with its obligations. Organizational-level PCS requirements may be derived from a variety of sources, including:

- Legal environment (examples: laws, regulations, contracts)
- Organizational policies or cultural values
- Relevant standards
- PCS principles

System/product/service design artifacts (GR.BE-3)

Design artifacts may take many forms, such as system design architectures or user activity flow diagrams. These artifacts help an organization determine how its systems, products and services will operate. Therefore, they can help PCS programs understand how systems, products and services need to function so that controls or measures that help to mitigate PCS risk can be selected and implemented in ways that maintain functionality while protecting PCS.

User Activity Data maps (GR.IM)

User activity data maps illustrate individuals' interactions with systems, products and services. A user activity map shows the organizational environment and includes the components through which activities are being processed or with which individuals are interacting, the ecosystem owners or operators of the components and discrete user actions and the specific activity elements being processed. User activity data maps can be illustrated in different ways, and the level of detail may vary based on an organization's needs. A user activity data map can be overlaid on existing system/product/service design artifacts for convenience and ease of communication between organizational components. As discussed below, a user activity data map is an important artifact in PCS risk assessment.

Determining PCS capabilities

PCS capabilities can be used to describe the system, product, or service property or feature that achieves the desired PCS outcome (example: "the service enables user activity auditing"). The security objectives confidentiality, integrity and availability along with security requirements are used to inform the security capabilities for a system, product or service. As set forth in Table 3, an additional set of PCS engineering objectives can support the determination of PCS capabilities. An organization may also use the PCS engineering objectives as a high-level prioritization tool. Systems, products services that are low in predictability, manageability or associability may be a signal of increased PCS risk and may, therefore, merit a more comprehensive PCS risk assessment.

In determining PCS capabilities, an organization may consider which of the PCS engineering and security objectives are most important with respect to its mission or business needs, risk tolerance and organizational-level PCS requirements (see Organizing Preparatory Resources above). Not all the objectives may be equally important—or trade-offs may be necessary among them. Although the PCS capabilities inform the PCS risk assessment by supporting risk prioritization decisions, the PCS capabilities may also be informed by the risk assessment and adjusted to support the management of specific PCS risks or address changes in the environment, including design changes to the system, product or service.

Table 3: PCS Engineering and Security Objectives

OBJECTIVE	DEFINITION	PRINCIPAL RELATED FUNCTIONS FROM THE PCS FRAMEWORK CORE
PCS Engineering Objectives		
Predictability	Enabling reliable assumptions by individuals, owners and operators about user activity data and their processing by a system	GRC, People, Process, Technology
Manageability	Providing the capability for granular administration of user activity data, including collection, alteration, deletionand selective disclosure	GRC, Process, Technology
Associability	Enabling the processing of user activity data or events with association to individuals or devices to support the operational requirements of the system	GRC, Process
Secondary Objectives		
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information	GRC, Technology
Integrity	Guarding against improper information modification or destruction; includes ensuring information non-repudiation and authenticity	GRC, Process, Technology
Availability	Ensuring timely and reliable access to and use of information	GRC, Process, Technology

Defining PCS requirements

PCS requirements specify the way a system, product service needs to function to meet stakeholders' desired PCS outcomes (example: "the application is configured to allow users to transfer certain data"). To define PCS requirements, consider organizational-level PCS requirements (see Organizing Preparatory Resources above) and the outputs of a PCS risk assessment. This process helps an organization to answer two questions: 1) What can a system, product or service do with user activities and interactions with individuals? 2) What should it do? Then an organization can allocate resources to design a system, product or service in a way that achieves the defined requirements. Ultimately, defining PCS requirements can lead to the development of systems, products and services that are more mindful of individuals' actions, and are based on informed risk decisions.

Conducting PCS risk assessments

Conducting a PCS risk assessment helps an organization to identify PCS risks engendered by the system, product or service and prioritize them to be able to make informed decisions about how to respond to the risks (GR.RA, GR.RM). Methodologies for conducting PCS risk assessments may vary, but organizations should consider the following characteristics:

Risk model (GR.RA, GV.CO-2)

Risk models define the risk factors to be assessed and the relationships among those factors. (9)If an organization is not using a predefined risk model, an organization should clearly define which risk factors it will be assessing and the relationships among these factors. Although cybersecurity has a widely used risk model based on the risk factors of threats, vulnerabilities, likelihood and impact, there is not one commonly accepted PCS risk model. Proofpoint has developed a PCS risk model to calculate risk based on the likelihood of a problematic user action multiplied by the impact of a problematic user action. Each of the three risk factors are explained below.

- A problematic user action is any action an individual or system takes to process actions that could result in a problem for individuals. Organizations consider the type of problems that are relevant to the population of individuals. Problems can take any form and may consider the experience of individuals.
- Likelihood is defined as a contextual analysis that a user action is likely to create a problem for a representative set of individuals. Context can include organizational factors (examples: geographic location, the public perception about participating organizations with respect to PCS), asset/system factors (examples: the nature and history of individuals' interactions with the system or visibility of sensitive data to individuals and third parties) or individual factors (examples: individuals' demographics, interests or perceptions or data sensitivity). A user activity data map can help with this contextual analysis (see Organizing Preparatory Resources).
- Impact is an analysis of the costs should the problem occur. As noted in section 1.2, organizations may not experience these problems directly. Moreover, individuals' experiences may be subjective. Thus, impact may be difficult to assess accurately. Organizations should consider the best means of internalizing impact to individuals in order to appropriately prioritize and respond to PCS risks.[9]

Assessment approach (GR.RA-4)

The assessment approach is the mechanism by which identified risks are prioritized. Assessment approaches can be categorized as quantitative, semi-quantitative or qualitative.[10, 9]

Prioritizing risks (GR.RA-4)

Given the applicable limits of an organization's resources, organizations prioritize the risks to facilitate communication about how to respond. (9)

Responding to risks (GR-RA-5)

As described in section 1.2.2, response approaches include mitigation, transfer/sharing, avoidance or acceptance. (9)

Creating privacy requirements traceability

Once an organization has determined which risks to mitigate, it can refine the PCS requirements and then select and implement controls (examples: technical, physical and/or policy safeguards) to meet the requirements.[8] An organization may use a variety of sources to select controls, such as NIST SP 800-53 Rev.5.[11] After implementation, an organization iteratively assesses the controls for their effectiveness in meeting the PCS requirements and managing PCS risk. In this way, an organization creates traceability between the controls and the PCS requirements and demonstrates accountability between its systems, products and services and its organizational PCS goals.

Monitoring change

PCS risk management is not a static process. An organization monitors how changes in its business environment—including new laws and regulations and emerging technologies—and corresponding changes to its systems, products and services may be affecting PCS risk, and iteratively uses the practices in this appendix to adjust accordingly. (GR.CO-2)

Appendix E: Implementation Tiers Definitions

The five Tiers summarized below are each defined with four elements:

Tier 0: Initial

- **GRC:** PCS Risk practices are undefined, and the organization has no visibility to the risk posed by people-centric threats. Policy or standard statements requiring use of PCS Risk practices do not exist, does not cover all requirements or is not formally approved by management. Funding for PCS Risk is ad hoc. The organization implements PCS risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources. There is limited understanding of an organization's role(s) in the larger ecosystem with respect to other entities (examples: buyers, suppliers, service providers, business associates, partners).
- **People:** There is limited awareness of PCS risk at the organizational level. Some personnel may have a limited understanding of PCS risks or PCS risk management processes but have no specific PCS responsibilities. If available, PCS training is ad hoc and the content is not kept current with best practices.
- **Process:** The organization may not have processes that enable the sharing of information about PCS risks within the organization. The organization does not have processes for identifying how PCS risks may proliferate throughout the ecosystem or for communicating PCS risks or requirements to other entities in the ecosystem.
- **Technology:** The PCS technology strategy is unclear with ad hoc use of PCS profiles and controls. Cybersecurity controls are primarily focused on perimeter security. The organization has no formal programs or technology in place to detect and respond top people-centric threats.

Tier 1: Developing

- **GRC:** PCS Risk practices are approved by management but may not be established as organization-wide policy. Prioritization of PCS activities is sometimes informed by organizational risk management priorities, PCS risk assessments or mission or business objectives, resulting in ad hoc funding. Consideration of PCS in organizational objectives and programs may occur at some but not at all levels of the organization. PCS risk assessment occurs but is not typically repeatable or reoccurring. There is some understanding of an organization's role(s) in the larger ecosystem with respect to other entities (examples: buyers, suppliers, service providers, business associates, partners). The organization is aware of the PCS ecosystem risks associated with the products and services it provides and uses but does not act consistently or formally upon those risks.
- **People:** There is an awareness of PCS risk at the organizational level, but an organization-wide approach to managing PCS risk has not been established. Information about PCS risks is shared within the organization on an informal basis. There are personnel with specific PCS responsibilities, but they may have non-PCS responsibilities as well. PCS training is conducted regularly for PCS personnel, although there is no consistent process for updates on best practices.
- **Process:** The organization may have some processes that enable the sharing of information about PCS risks within the organization. The organization has some processes for identifying how PCS risks may proliferate throughout the ecosystem or for communicating PCS risks or requirements to other entities in the ecosystem.
- **Technology:** The PCS technology strategy is approved by management, but implementation is unclear with ad hoc use of PCS profiles and controls, and IT is responsible for responding to any realized threat actions. Cybersecurity controls sometimes include PCS, but are still primarily focused on perimeter security.

Tier 2: Defined

- **GRC:** PCS Risk practices are approved by management and established as organization-wide policy. Prioritization of PCS activities is informed by organizational risk management priorities, PCS risk assessments and mission or business objectives, resulting in budget that is planned and approved. Consideration of PCS in organizational objectives and programs occurs at all levels of the organization. PCS risk management is formalized but is not typically repeatable or reoccurring There is an understanding of an organization's role(s) in the larger ecosystem with respect to other entities (examples: buyers, suppliers, service providers, business associates, partners). The organization is aware of the PCS ecosystem risks associated with the products and services it provides and uses. Key performance indicators (KPIs) are being developed.

  Recommended KPI: Policy exceptions are documented, approved and occur less than 5% of the time.

- **People:** There is an awareness of PCS risk at the organizational level, with an established organization-wide approach to managing PCS risk. Information about PCS risks is shared within the organization. There are personnel with specific PCS responsibilities, but they may have non-PCS responsibilities as well. PCS training is conducted regularly for PCS personnel and the organization at large, although there is no consistent process for updates on best practices.

  Recommended KPI: Less than 50% exceptions for adaptive control profile membership.

- **Process:** The organization has defined processes that enable the sharing of information about PCS risks within the organization. The organization has defined processes for identifying how PCS risks may proliferate throughout the ecosystem or for communicating PCS risks or requirements to other entities in the ecosystem.

  Recommended KPI: Less than 10% exceptions for adaptive control process documentation.

Technology: The PCS technology strategy is approved by management, with communicated implementation planned for use of PCS profiles and controls. PCS Risk Assessment and Control Review is included in the SDLC. The focus is on the use of technologies and the cross-team communication required to identify some high-risk users.

Recommended KPI: Less than 10% exceptions are granted for systems and solutions.

Tier 3: Repeatable

- **GRC:** Organizational PCS practices are regularly updated based on the application of risk management processes to changes in mission or business objectives and a changing risk, policy and technology landscape. Risk-informed policies, processes and procedures are defined, implemented as intended and reviewed. Consistent PCS risk management methods are in place to respond effectively to changes in risk. The organization consistently monitors PCS risk. Senior executives ensure consideration of PCS through all lines of operation in the organization. The organization understands its role(s), dependencies and dependents in the larger ecosystem and may contribute to the communities broader understanding of risks. The organization is aware of the PCS ecosystem risks associated with the products and services it provides and uses. Additionally, it sometimes acts upon those risks, including mechanisms such as written agreements to communicate PCS requirements, governance structures and policy implementation and monitoring. The organization has defined organizational compliance functions, including the ability to monitor the activity and conduct independent audits of the personnel responsible for managing PCS with access to threat information and tools. KPIs have been defined.

  Recommended KPI: Policy exceptions are documented, approved and occur less than 3% of the time.

- **People:** This is an organization-wide approach to manage PCS risk. Senior executives communicate regularly regarding PCS risk. Dedicated PCS personnel possess the knowledge and skills to perform their appointed roles and responsibilities. There is regular, up-to-date PCS training for all personnel.

  Recommended KPI: Less than 5% exceptions for adaptive control profile membership.

- **Process:** The organization has defined processes that enable the sharing of information about PCS risks within the organization. The organization has defined processes for identifying how PCS risks may proliferate throughout the ecosystem or for communicating PCS risks or requirements to other entities in the ecosystem.

  Recommended KPI: Less than 5% exceptions for adaptive control process documentation.

Technology: The PCS technology strategy is approved by management. Implementation planned for the use of PCS profiles and controls has been communicated and user activity monitoring capabilities have been established. PCS Risk Assessment and Control Review is included in the SDLC with the goal to identify potential or active threats as early as possible.

Recommended KPI: Less than 5% exceptions occur with minimal recurring exceptions.

Tier 4: Optimizing

- **GRC:** The organization adapts its PCS practices based on lessons learned from PCS events and identification of new PCS risks. Through a process of continuous improvement incorporating advanced PCS technologies and practices, the organization actively adapts to a changing policy and technology landscape and responds in a timely and effective manner to evolving PCS risks. There is an organization-wide approach to managing PCS risk that uses risk-informed policies, processes and procedures to address problematic data actions. The relationship between PCS risk and organizational objectives is clearly understood and considered when making decisions. Senior executives monitor PCS risk in the same context as cybersecurity risk, financial risk and other organizational risks. The organizational budget is based on an understanding of the current and predicted risk environment and risk tolerance. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. Business units implement executive vision and analyze system-level risks in the context of the organizational risk tolerances. The organization understands its role(s), dependencies and dependents in the larger ecosystem and contributes to the community's broader understanding of risks. The organization has implemented program compliance functions.

  Recommended KPI: Policy exceptions are documented and approved and occur less than 0.5% of the time.

- **People:** PCS risk management is part of the organizational culture and evolves from lessons learned and continuous awareness of actions resulting PCS risks. The organization can quickly and efficiently account for changes to business/mission objectives in how risk is approached and communicated. The organization has specialized PCS skillsets throughout the organizational structure; personnel with diverse perspectives contribute to the management of PCS risks. There is regular, up-to-date, specialized PCS training for all personnel. Personnel at all levels understand the organizational PCS principles and their role in maintaining them. PCS personnel conducts routine exercises to improve integration, analysis and response procedures and processes.

  Recommended KPI: Less than 1% exceptions for adaptive control profile membership.

- **Process:** The organization has defined processes that enable the sharing of information about PCS risks within the organization. The organization has defined processes for identifying how PCS risks may proliferate throughout the ecosystem or for communicating PCS risks or requirements to other entities in the ecosystem. The organization employs documented processes to validate information sources and identify and assess the use of new information sources.

  Recommended KPI: Less than 1% exceptions for adaptive control process documentation.

- **Technology:** PCS profiles and adaptive control implementation is being optimized. Technologies that employ data integration and behavioral science methodologies to help identify indicators of potential insider threat should be implemented, such as risk scoring capability based on behavioral and workplace factors to assist with detection of anomalous activity and potential people-centric threats and in the application of tailored mitigation strategies.

  Recommended KPI: Less than 1% exceptions occur with minimal recurring exceptions.

Appendix F: PCS Control Requirements

Governance, risk and compliance

Develop the organizational understanding manage PCS risk for individuals arising from user actions.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
1.1 Establish a people-centric security governance structure	Review documentation that establishes organizational governance structure.	This document should include people-centric security focused mission, goals and objectives, with a defined organizational structure that will support PCS goals.
1.2 Assign Roles and Responsibilities, indicating Lines of Reporting	a. Review documented roles, responsibilities and organization charts. b. Validate that roles and responsibilities include designated people-centric security responsibilities and segregation of duties.	This document should include logical structure for top down and bottoms up communication requirements (example: cybersecurity risk integration into enterprise risk).
1.3 Develop people-centric security policy requirements	Review the people-centric security policy requirements.	The policy requirements should align to PCS mission, goals and objectives.
1.4 Board members understand PCS criticality to the organization and are updated quarterly on security performance and breaches.	a. Review records used to determine external and internal issues that are relevant to organizational purpose and affect its ability to achieve the intended outcome(s) b. Review quarterly update content.	This document should highlight the critical concerns identified by assessing the risk of existing PCS measures and identifying gaps to be addressed.
1.5 The board has established a board risk committee (BRC) to ensure compliance with applicable laws and regulations and in mitigating organization risk.	a. Review documentation that establishes the BRC. b. Determine and manage compliance requirements based on user activity risk and magnitude of harm. - Mapping of assets (people, systems, information and more) to authorities - Mapping and analysis of data flows - Mapping of cross-board PCS requirements - Mapping of legal and regulatory requirements in relation to assets - Review process for maintaining user activity provenance and lineage. - Review that user activity provenance and lineage can be accessed for review or transmission/disclosure.	• This documentation should include the process to select BRC members and the experience required for each participating member. • Authorities should be determined based on the organization's role in the ecosystem. This information should include at minimum: - User categorizing based on risk. - Systems, products and services utilized by users. - Purpose, activities and ownership of systems, products and services. - Environmental location of assets (geographic location, internal, cloud, third parties)

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
1.6 Develop and implement a Risk Management program	a. Review documentation that establishes the BRC. b. Determine and manage compliance requirements based on user activity risk and magnitude of harm. c. Review processes used to determine organizational risk tolerance.	a. Documentation should clearly establish Risk Management processes. b. Evidence must demonstrate that they are agreed to by organizational stakeholders. c. Thresholds for Risk tolerance levels should be clearly indicated.
1.7 Develop and implement a PCS Risk Assessment process	a. Review risk assessment process. b. Review operational criteria requirements produced from risk assessment. c. Review records of user weakness identification and incorporate into new preventative and mitigating controls. d. Review process to categorize user behavior based on levels of risk and magnitude of harm. e. Review documentation of completed risk assessments. f. Review standard contract language. g. Review factors included to ensure that PCS is represented. h. Review documentation of bias review processes. i. Review problem management records of problematic user activities to determine if the risk calculations are aligned. j. Review records for risk responses to problematic behavior. k. Review KPIs and KRIs.	This documentation should be based on known risk assessment concepts. PC factors should include social network visibility, attack data, education, system vulnerabilities, HR input (pass over for promotion, low performance reviews, flight potential) Ensure that contracts are used to implement appropriate measures designed to meet the objectives of the organization's PCS program. Contextual factors related to the users, systems, products, services and the user actions are identified (examples: individuals' vulnerabilities, attack demographics, privilege and visibility of user activities to individuals and third parties). User behavior analytic inputs and outputs are identified and evaluated for bias. Potential problematic user activities and associated problems are identified. Problematic user activities, likelihoods and impacts are used to determine and prioritize risk. Risk responses are identified, prioritized and implemented.
1.8 Establish internal assurance policies, guidelines and procedures.	a. Review policies, guidelines and procedures b. Review audit, test results, or other forms of evaluation performed c. Review records that show how PCS roles and responsibilities are coordinated and aligned with third-party stakeholders (examples: service providers, customers, partners). d. Review records of testing for response and recovery plans. e. Review records that demonstrate that backups of user activity information are conducted, maintained and tested. f. Validate that policy and regulations regarding the physical operating environment for organizational assets are met. (examples: review application security reviews, exceptions tracking and more)	Policies should require that organizational ecosystem parties are routinely assessed using audits, test results or other forms of evaluations on a periodic schedule. The processes should ensure that they are meeting their contractual, interoperability framework or other SLA defined obligations.
1.9 PCS factors are integrated into BCP planning	a. Review BCP Planning to validate that PCS factors have been considered (example: ability to manage user behavior even when they work via mobile devices or from remote locations).	a. Mechanisms (examples: failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.

People

Develop and implement organizational communication, culture, security training and awareness activities.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
2.1 Establish PCS Communication	a. Review documented mission, goals and objectives. b. Review policies and guidelines. c. Review documented processes and procedures. d. Review examples of execution.	Mission, goals and objectives should be defined to drive cultural recognition of PCS.
2.2 Develop PCS Communication Policies	a. Review documented roles, responsibilities and organization charts. b. Validate that roles and responsibilities include designated people-centric security responsibilities and segregation of duties.	Communication policies should include requirements related to communication of changes related to assessment, education and behavioral monitoring. Factors increasing the risks for certain users should be communicated to increase awareness (example: if specific users or groups of users are being targeted via email, phone or another vector).
2.3 Develop policies processes and procedures to identify, address and respond to risky user activities.	a. Review user behavior analytics policies and requirements b. Review KPIs and KRIs to confirm people-centric factors have been included. c. Review RACIs and Swimlane flow charts to understand how processes are integrated across organizational teams/business departments to manage people-centric risk activities. d. Review change logs and data flow demonstrating ongoing improvement.	a. Develop policies for managing risky user activities, including those related to internal employees, contractors, vendors and third parties. b. Develop guidelines for KPIs and KRIs to monitor user risk. c. Integrate processes across organizational teams/business departments to manage people-centric risk activities d. Processes should include the integration into Cybersecurity Problem Management with post-mortem analysis outcomes feeding into future risk assessments and improvements.
2.4 Develop PCS feedback policies	a. Review feedback policies. b. Review records form the mechanisms for obtaining feedback from individuals (example: surveys or focus groups) about PCS and associated PCS risks.	Policies should include requirements for receiving, tracking and responding to complaints, concerns and questions from individuals about organizational PCS practices.
2.5 Workforce is informed and trained on its roles and responsibilities.	a. Review workforce roles and responsibilities. b. Ensure that roles and responsibilities are specific to the user activities being performed. c. Review the mechanism used for communicating PCS purposes, practices, associated PCS risks and options for enabling individuals' user roles and requests. d. Review that user training and education is aligned to role requirements.	User activity mapping category activity should align to represent the roles and responsibilities of business users, the board, senior executives, security personnel and third parties.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
2.6 Users, contractors and vendors should be assessed for fit prior to employment and contracting	a. Review pre-hiring screening requirements. b. Review terms and conditions of employment and contracting. c. Review records to validate that contractors are held to at least the same standards as employees. d. Review Acceptable Use content. e. Review training, security awareness and education records f. Review disciplinary processes and records. g. Review termination processes, voluntary and involuntary	Screening should include education, experience, skills and criminal and financial history where allowed. Minimum requirements should be pre-defined for each role. Onboarding and separation processes should include risk categorization of users based on role and activity flows.

Process

Develop and implement appropriate processes to enable organizations or individuals to manage privileges and controls.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
3.1 Incorporate PCS requirements into system, product and service design	a. Review assessment and SDLC documentation b. Review testing procedures that validate the user activity flow visibility c. Review that records of PCS events, disclosure and sharing are maintained and can be accessed.	Mission, goals and objectives should be defined to drive cultural recognition of PCS.
3.2 Incorporate user activity flow changes into change management processes	Review change management processes to validate visibility to user activity flow corrections or deletions and how they are communicated to individuals or organizations in the ecosystem.	a. User activity flow corrections or deletions can be communicated to individuals or organizations in the ecosystem. b. Configuration change control processes are established and in place. c. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. d. Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
3.3 Data protection processes are integrated with PCS control requirements	a. Review data protection policies addressing management of user activity data. b. Review processes for used by PCS personnel to re-link anonymized data during investigations. c. Review PCS personnel user activity flows to validate that user activity data are processed to decrease observability and link ability, while adhering to organizational PCS requirements. d. Review anonymized user activity data to validate that formulation of inferences about individuals' behavior or activities is limited. e. Review system and/or device configuration documentation and actual settings permit selective collection or disclosure of user activity data elements. f. Review reports where user data is aggregated to confirm that attribute references are substituted for attribute values.	a. User activity data is processed to decrease observability and attribution, while adhering to organizational PCS requirements. b. Data are processed to limit the identification of individuals (example: de-identification privacy techniques, tokenization). c. User activity data are processed to limit the formulation of inferences about individuals' behavior or activities. d. System or device configurations permit selective collection or disclosure of user activity data elements. e. Attribute references are substituted for attribute values. (example: When data is aggregated)
3.4 Incorporate user activity flow changes into change management processes	a. Review change management processes to validate visibility to user activity flow corrections or deletions and how they are communicated to individuals or organizations in the ecosystem.	a. User activity flow corrections or deletions can be communicated to individuals or organizations in the ecosystem. b. Configuration change control processes are established and in place. c. Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools. d. Remote maintenance of organizational assets is approved, logged and performed in a manner that prevents unauthorized access.

Technology

Develop and implement appropriate people-centric safeguards.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
4.1 Incorporate PCS requirements into system, product and service design	a. Review assessment and SDLC documentation. b. Review testing procedures that validate the user activity flow visibility. c. Review that records of PCS events, disclosure and sharing are maintained and can be accessed.	PCS should be incorporated into base processes in order to build security-mitigating activities into user activity flows.
4.2 Authentication, Authorization and Access Management principles are established	a. Review Authentication, Authorization and Access policies b. Review Authentication, Authorization and Access processes c. Review records demonstrating that policies and processes for managing Identities and credentials are being followed. d. Review that records include the management of physical access to data and devices in alignment to the user activity flows. e. Review that records ensure user, data and network integrity aligned to the user activity flows. f. Review records that validate prerequisites, like background checks, category, profile assignments and authorization, have been completed prior to access being granted.	a. Identities and credentials are issued, managed, verified, revoked and audited for authorized individuals, processes, and devices. b. Physical access to data and devices is managed. c. Remote access is managed. d. Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties. e. Network integrity is protected (example: network segregation, network segmentation). f. Individuals and devices are vetted and bound to credentials and authenticated commensurate with the risk of the transaction (example: individuals' PCS risks and other organizational risks).
4.3 Manage PCS behavioral data following sensitive data practices	a. Review that policies require user analytics data to be protected at rest and in transit. b. Review the process for managing user analytics data throughout its lifecycle. c. Review capacity-planning records d. Review activity maps to ensure that protections against data leaks and data tampering are implemented. e. Review the processes to ensure that user analytics data solutions use development and testing environment(s) separate from the production environment.	a. Data-at-rest and data-in-transit is protected. b. Assets and associated data are formally managed throughout removal, transfers and disposition. c. Adequate capacity to ensure availability is maintained. d. Protections against data leaks are implemented. e. Integrity checking mechanisms are used to verify software, firmware and information integrity. f. Integrity checking mechanisms are used to verify hardware integrity. g. The development and testing environment(s) are separate from the production environment.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
4.4 IT Operations requirements for managing user activity data are established	a. Review requirements for managing user activity data. b. Validate that user activity elements can be accessed for review randomly selecting solutions from the user activity flows. c. Review records demonstrating user activity elements can be accessed for alteration (example: to remove PHI or sensitive personal information inadvertently captured). d. Review records for user retention policy and process pertaining to user activity data. e. Review audit log records demonstrating adherence to retention policies. f. Review that user activity data is stored using standardized formats as documented in process. g. Review records for transmitting user privileges and related values and evaluate against policy and procedures. h. Review audit and log records to ensure than they follow requirements for managing user activity data.	a. User activity elements can be accessed for review. b. User activity elements can be accessed for transmission or disclosure. c. User activity elements can be accessed for alteration. d. User activity elements can be accessed for deletion. e. User activity data is destroyed according to policy. f. Data is transmitted using standardized formats. g. Mechanisms for transmitting user privileges and related values with user activities are established and in place. h. Audit/log records are determined, documented, implemented and reviewed in accordance with policy and incorporating the principle of user data minimization. i. Stakeholder PCS preferences are included in algorithmic design objectives, and outputs are evaluated against these preferences.
4.5 PCS factors are integrated into BCP planning	• Review BCP Planning to validate that PCS factors have been considered (example: ability to manage user behavior even when they work via mobile devices or from remote locations).	• Mechanisms (example: failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
4.6 IT Operations requirements for managing user activity data are established	a. Review requirements for managing user activity data. b. Validate that user activity elements can be accessed for review randomly selecting solutions from the user activity flows. c. Review records demonstrating user activity elements can be accessed for alteration (example: to remove personal health information [PHI] or sensitive personal information inadvertently captured). d. Review records for user retention policy and process pertaining to user activity data. e. Review audit log records demonstrating adherence to retention policies. f. Review that user activity data is stored using standardized formats as documented in process. g. Review records for transmitting user privileges and related values and evaluate against policy and procedures. h. Review audit and log records to ensure than they follow requirements for managing user activity data.	a. User activity elements can be accessed for review. b. User activity elements can be accessed for transmission or disclosure. c. User activity elements can be accessed for alteration. d. User activity elements can be accessed for deletion. e. User activity data is destroyed according to policy. f. Data is transmitted using standardized formats. g. Mechanisms for transmitting user privileges and related values with user activities are established and in place. h. Audit/log records are determined, documented, implemented and reviewed in accordance with policy and incorporating the principle of user data minimization. i. Stakeholder PCS preferences are included in algorithmic design objectives and outputs are evaluated against these preferences.

REQUIREMENT	TESTING PROCEDURE	GUIDANCE
4.7 PCS factors are integrated into BCP planning	• Review BCP Planning to validate that PCS factors have been considered (example: ability to manage user behavior even when they work via mobile devices or from remote locations).	• Mechanisms (examples: failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.
4.8 Develop Event and Incident Response Plan	a. Review policies b. Review procedures c. Review Event Plan d. Review Incident Response Plan e. Review people-centric security event and incident reporting f. Review records of Event and Incident Response Plan testing	• Event and Incident plans include process workflows defining how people-centric security events are managed (example: If an employee gives notice, what are the cross-team procedures that are put in place?).

LEARN MORE

For more information, visit **proofpoint.com**.