From: Laura Lindsay (CELA) <laurali@microsoft.com>
Sent: Wednesday, October 23, 2019 9:17 AM
To: privacyframework <privacyframework@nist.gov>
Cc: Lefkovitz, Naomi B. (Fed) <naomi.lefkovitz@nist.gov>; Nadeau, Ellen M. (Fed) <ellen.nadeau@nist.gov>
Subject: NIST Privacy Framework: Preliminary Draft Comments

Naomi, Ellen and the NIST Privacy Framework team –

On behalf of Jason Matusow, General Manager at Microsoft Corporation, please accept the attached documents as Microsoft's response to the Call for Public Comment on the Preliminary draft of *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*.

The PDF is the overview of Microsoft's comments, an Excel spreadsheet of the actual comments and an Excel spreadsheet of an Informative Mapping.

I look forward to continue working with everyone and please let myself and/or Jason know if you have any questions or comments.

Laura Lindsay
US National Standards Officer, Corporate Standards Group, Microsoft

Microsoft's Response to the National Institute of Standards and Technology Call for Public Comments on the Preliminary draft of *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*

Microsoft Corporation ("Microsoft") appreciates the opportunity to provide these comments to the National Institute of Standards and Technology ("NIST") in response to the call for comments on the Preliminary Draft of the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. Microsoft shares NIST's goal of developing a voluntary framework that consists of outcomes and approaches that align policy, business, technological, and legal approaches to improve risk management processes. The Privacy Framework provides a common taxonomy to have discussions about incorporating Privacy elements into the risk management and governance of the organization.

Microsoft mentioned in previous RFI response that any Privacy Framework that was developed should be: (1) interoperable with other global approaches, (2) forward-looking, and (3) risk-based and outcome-focused. We believe that the inclusion of Informative References can help address interoperability requirements with other privacy regimes around the world. We applaud NIST for providing a means for organizations to contribute to this mechanism. With that in mind, please find, as a part of our comments, a suggested Informative Reference, ISO/IEC 27701:2019.

In addition, guidance about how to implement the Privacy Framework would benefit potential users of the tool. Rather than " Fulfilling current compliance obligations, as well as future-proofing products and services to meet these obligations in a changing technological and policy environment" (NIST Privacy Framework Preliminary Draft published Sept 6, 2019, lines 93-94) users might be encouraged to use existing compliance data and proposed informative reference mapping to draft business rules about how to translate their current compliance data into Tier ratings that enable risk based discussions between executives and operations. Contextualizing the relationship between compliance standards and use of the Framework will help strengthen understanding that the Framework is Risk Management tool and not a compliance standard. The value of the Framework is in the common taxonomy and as a discussion tool. It does not introduce new requirements. This enhances its interoperability with existing global approaches.

Microsoft would welcome opportunities to work with NIST, and with the Department of Commerce more broadly in considering how to address the important privacy issues raised by the Privacy Framework.

Respectfully submitted,

Jason P. Matusow
General Manager
Microsoft Corporation

23 October 2019

Comment #	Organization Name	Submitted By (Name/Email)	Page #	Line #	Section	Comment (Include rationale for comment)	Suggested Change	Type of Comment (General/Editorial /Technical)
1	Microsoft	Laura Lindsay/laurali@microsoft.com	3, 4	79-85 and 120-127	Executive Summary and Introduction	Both the Executive Summary and the Introduction's first paragraph are identical and since they are so close together they should probably be slightly different. The text in question is "For more than two decades, the Internet and associated information technologies have driven unprecedented innovation, economic value, and access to social services. Many of these benefits are fueled by data about individuals that flow through a complex ecosystem—so complex that individuals may not be able to understand the potential consequences for their privacy as they interact with systems, products, and services. Organizations may not fully realize the consequences either. Failure to manage privacy risks can have direct adverse consequences for people at both the individual and societal level, with follow-on effects on organizations' reputation, bottom line, and future prospects for growth. "	Summarize either in the executive summary or in the Introduction: The benefits of the unprecedented innovation, economic value and access to social services is fueled by data about individuals in a complex ecosystem that may make it difficult for individuals or organizations to understand the full potential consequences on privacy as they interact with systems, products and services. These consequences can have an adverse effect on people both at individual and societal level, as well as effects on an organization, such as reputation, bottom line and future prospects for growth.	

2	Microsoft	Laura Lindsay/laurali@microsoft.com	18	622-624	Appendix A	The following text is very confusing. While we agree that the framework Core and in particular the Subcategories should not be read as a checklist this statement makes it more confusing. "The Subcategories should not be read as a checklist in isolation from their Categories, which often provide a risk-based modifier on Subcategory selection. " Similar content is in the Cybersecurity Framework "The Core is not a checklist of actions to perform. It presents key cybersecurity outcomes identified by stakeholders as helpful in managing cybersecurity risk. " could be used to better clarify what is intended.	Rewrite sentence: The Core is not a checklist of actions to perform. The outcomes (subcategories) will be chosen based on the organizations privacy risk management process.	
3	Microsoft	Laura Lindsay/laurali@microsoft.com				As noted earlier interoperability is an important part of the NIST Privacy Framework and we believe that Informative References can be a help in that Interoperability. With this in mind we have provided in the attachment an Informative reference between the NIST Privacy Framework and ISO/IEC 27701.	Post the Informative Reference for ISO/IEC 27701	

Function	Category	Subcategory	Mapping
IDENTIFY-P (ID-P): Develop the organizational understanding to manage privacy risk for individuals arising from data processing.	**Inventory and Mapping (ID.IM-P):** Data processing by systems, products, or services is understood and informs the management of privacy risk.	**ID.IM-P1:** Systems/products/services that process data are inventoried.	**ISO/IEC 27701:2019** 7.2.8, 8.2.6
		ID.IM-P2: Owners or operators (e.g., 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 (e.g., internal or external) that process data are inventoried.	**ISO/IEC 27701:2019** 5.2.3, 7.2.8, 8.2.6
		ID.IM-P3: Categories of individuals (e.g., customers, employees or prospective employees, consumers) whose data are being processed are inventoried.	ISO/IEC 27701:2019 7.2.8, 8.2.6
		ID.IM-P4: Data actions of the systems/products/services are inventoried.	ISO/IEC 27701:20197.2.8, 8.2.6
		ID.IM-P5: The purposes for the data actions are inventoried.	ISO/IEC 27701:2019 7.2.1, 8.2.2, 7.2.5
		ID.IM-P6: Data elements within the data actions are inventoried.	ISO/IEC 27701:2019 7.2.5, 7.2.8, 8.2.6
		ID.IM-P7: The data processing environment is identified (e.g., geographic location, internal, cloud, third parties).	ISO/IEC 27701:2019 5.2.3, 7.2.5, 7.2.8, 8.2.5, 8.2.6

		ID.IM-P8: Data processing is mapped, illustrating the data actions and associated data elements for systems/products/services, including components; roles of the component owners/operators; and interactions of individuals or third parties with the systems/products/services.	ISO/IEC 27701:2019 5.2.3, 7.2.5, 7.2.8, 8.2.5, 8.2.6
	Business Environment (ID.BE-P): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform privacy roles, responsibilities, and risk management decisions.	**ID.BE-P1:** The organization's role in the data processing ecosystem is identified and communicated.	ISO/IEC 27701:2019 5.2.1, 7.3.3, 8.3.1
		ID.BE-P2: Priorities for organizational mission, objectives, and activities are established and communicated.	ISO/IEC 27701:2019 5.2.4
		ID.BE-P3: Systems/products/services that support organizational priorities are identified and key requirements communicated.	ISO/IEC 27701:2019 5.2.1, 5.2.4
	Risk Assessment (ID.RA-P): The organization understands the privacy risks to individuals and how such privacy risks may create follow-on impacts on organizational operations, including mission, functions, other risk management priorities (e.g. compliance, financial), reputation, workforce, and culture.	**ID.RA-P1:** Contextual factors related to the systems/products/services and the data actions are identified (e.g., individuals' demographics and privacy interests or perceptions, data sensitivity, visibility of data processing to individuals and third parties).	ISO/IEC 27701:2019 5.2.1, 5.2.2
		ID.RA-P2: Data analytic inputs and outputs are identified and evaluated for bias.	ISO/IEC 27701:2019 6.11.2.1, 6.11.2.5, 7.3.10
		ID.RA-P3: Potential problematic data actions and associated problems are identified.	ISO/IEC 27701:2019 5.4.1.2
		ID.RA-P4: Problematic data actions, likelihoods, and impacts are used to determine and prioritize risk.	ISO/IEC 27701:2019 5.4.1.2
		ID.RA-P5: Risk responses are identified, prioritized, and implemented.	ISO/IEC 27701:2019 5.4.1.2, 5.4.1.3

	Data Processing Ecosystem Risk Management (ID.DE-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing privacy risk and third parties within the data processing ecosystem. The organization has established and implemented the processes to identify, assess, and manage privacy risks within the data processing ecosystem.	**ID.DE-P1:** Data processing ecosystem risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	ISO/IEC 27701:2019 5.4.1.2
		ID.DE-P2: Data processing ecosystem parties (e.g., service providers, customers, partners, product manufacturers, application developers) are identified, prioritized, and assessed using a privacy risk assessment process.	ISO/IEC 27701:2019 5.4.1.2
		ID.DE-P3: Contracts with data processing ecosystem parties are used to implement appropriate measures designed to meet the objectives of an organization's privacy program.	ISO/IEC 27701:2019 6.12.1.2, 7.2.7, 7.2.6, 8.2.1
		ID.DE-P4: Interoperability frameworks or similar multi-party approaches are used to manage data processing ecosystem privacy risks.	ISO/IEC 27701:2019 5.4.1.2
		ID.DE-P5: Data processing ecosystem parties are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual or framework obligations.	ISO/IEC 27701:2019 6.12.1.2
GOVERN-P (GV-P): Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's risk management priorities that are informed by privacy risk.	**Governance Policies, Processes, and Procedures (GV.PP-P):** The policies, processes, and procedures to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are	**GV.PP-P1:** Organizational privacy values and policies (e.g., conditions on data processing, individuals' prerogatives with respect to data processing) are established and communicated.	ISO/IEC 27701:2019 6.2.1.1
		GV.PP-P2: Processes to instill organizational privacy values within system/product/service development and operations are established and in place.	ISO/IEC 27701:2019 6.11.2.1, 6.11.2.5
		GV.PP-P3: Roles and responsibilities for the workforce are established with respect to privacy.	ISO/IEC 27701:2019 6.3.1.1

	understood and inform the management of privacy risk.	**GV.PP-P4:** Privacy roles and responsibilities are coordinated and aligned with third-party stakeholders (e.g., service providers, customers, partners).	ISO/IEC 27701:2019 6.12.1.2
		GV.PP-P5: Legal, regulatory, and contractual requirements regarding privacy are understood and managed.	ISO/IEC 27701:2019 6.15.1.1, 5.2.1
		GV.PP-P6: Governance and risk management policies, processes and procedures address privacy risks.	ISO/IEC 27701:2019 5.4.1.2, 5.4.1.3
	Risk Management Strategy (GV.RM-P): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**GV.RM-P1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	ISO/IEC 27701:2019 5.4.1.2, 5.4.1.3
		GV.RM-P2: Organizational risk tolerance is determined and clearly expressed.	ISO/IEC 27701:2019 5.4.1.2, 5.4.1.3, 5.2.4
		GV.RM-P3: The organization's determination of risk tolerance is informed by its role in the data processing ecosystem.	ISO/IEC 27701:2019 5.4.1.2, 5.4.1.3
	Awareness and Training (GV.AT-P): The organization's workforce and third parties engaged in data processing are provided privacy awareness education and are trained to perform their privacy-related duties and responsibilities consistent with related policies, processes, procedures, and agreements and organizational privacy values.	**GV.AT-P1:** The workforce is informed and trained on its roles and responsibilities.	ISO/IEC 27701:2019 6.3.1.1, 6.4.2.2
		GV.AT-P2: Senior executives understand their roles and responsibilities.	ISO/IEC 27701:2019 6.3.1.1
		GV.AT-P3: Privacy personnel understand their roles and responsibilities.	ISO/IEC 27701:2019 6.3.1.1
		GV.AT-P4: Third parties (e.g., service providers, customers, partners) understand their roles and responsibilities.	ISO/IEC 27701:2019 6.12.1.2, 6.2.1.1, 7.2.6, 8.2.1, 8.2.4, 7.3.3, 8.3.1

	Monitoring and Review (GV.MT-P): The policies, processes, and procedures for ongoing review of the organization’s privacy posture are understood and inform the management of privacy risk.	**GV.MT-P1:** Privacy risk is re-evaluated on an ongoing basis and as key factors, including the organization’s business environment, governance (e.g., legal obligations, risk tolerance), data processing, and systems/products/services change.	ISO/IEC 27701:2019 5.4.1.2
		GV.MT-P2: Privacy values, policies, and training are reviewed and any updates are communicated.	ISO/IEC 27701:2019 6.2.1.1, 6.3.1.1
		GV.MT-P3: Policies, processes, and procedures for assessing compliance with legal requirements and privacy policies are established and in place.	ISO/IEC 27701:2019 6.15.2.1, 6.15.2.3
		GV.MT-P4: Policies, processes, and procedures for communicating progress on managing privacy risks are established and in place.	ISO/IEC 27701:2019 5.4.1.2
		GV.MT-P5: Policies, processes, and procedures are established and in place to receive, analyze, and respond to problematic data actions disclosed to the organization from internal and external sources (e.g., internal discovery, privacy researchers).	ISO/IEC 27701:2019 6.13.1.2, 6.13.1.3
		GV.MT-P6: Policies, processes, and procedures incorporate lessons learned from problematic data actions.	ISO/IEC 27701:2019 6.13.1.5
		GV.MT-P7: Policies, processes, and procedures for receiving, tracking, and responding to complaints, concerns, and questions from individuals about organizational privacy practices are established and in place.	ISO/IEC 27701:2019 7.3.9, 8.3.1
CONTROL-P (CT-P): Develop and implement appropriate activities to enable organizations or individuals to manage data with	**Data Management Policies, Processes, and Procedures (CT.PO-P):** Policies, processes, and procedures are maintained and used to	**CT.PO-P1:** Policies, processes, and procedures for authorizing data processing (e.g., organizational decisions, individual consent), revoking authorizations, and maintaining authorizations are established and in place.	ISO/IEC 27701:2019 7.2.1, 7.2.2, 7.2.3, 7.2.4, 8.2.2, 8.2.3

sufficient granularity to manage privacy risks.	manage data processing (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) consistent with the organization’s risk strategy to protect individuals’ privacy.	**CT.PO-P2:** Policies, processes, and procedures for enabling data review, transfer, sharing or disclosure, alteration, and deletion are established and in place.	ISO/IEC 27701:2019 7.3.1, 7.3.4, 7.3.5, 7.3.6, 7.3.8, 7.3.10 7.5.1, 7.5.2, 7.5.3, 7.5.4, 8.3.1, 8.5.1, 8.5.2, 8.5.3, 8.5.4, 8.5.5, 8.5.6, 8.5.7, 8.5.8
		CT.PO-P3: Policies, processes, and procedures for enabling individuals’ data processing preferences and requests are established and in place.	ISO/IEC 27701:2019 7.3.1, 7.3.4, 7.3.5, 7.3.6, 7.3.8, 7.3.10, 8.3.1
		CT.PO-P4: An information life cycle to manage data is aligned and implemented with the system development life cycle to manage systems.	ISO/IEC 27701:2019 6.11.2.5
	Data Management (CT.DM-P): Data are managed consistent with the organization’s risk strategy to protect individuals’ privacy, increase manageability, and enable the implementation of privacy principles (e.g., individual participation, data quality, data minimization).	**CT.DM-P1:** Data elements can be accessed for review.	ISO/IEC 27701:2019 7.3.6, 8.3.1
		CT.DM-P2: Data elements can be accessed for transmission or disclosure.	ISO/IEC 27701:2019 7.3.6, 8.3.1
		CT.DM-P3: Data elements can be accessed for alteration.	ISO/IEC 27701:2019 7.3.6, 8.3.1
		CT.DM-P4: Data elements can be accessed for deletion.	ISO/IEC 27701:2019 7.3.6, 8.3.1
		CT.DM-P5: Data are destroyed according to policy.	
		CT.DM-P6: Data are transmitted using standardized formats.	ISO/IEC 27701:2019 7.3.6, 8.3.1
		CT.DM-P7: Metadata containing processing permissions and related data values are transmitted with data elements.	ISO/IEC 27701:2019 6.5.3.2, 6.8.2.7, 7.4.8, 7.4.6, 7.4.7, 8.4.1, 8.4.2
		CT.DM-P8: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy and incorporating the principle of data minimization.	ISO/IEC 27701:2019 6.9.4.1, 6.9.4.2, 6.15.1.3
	Disassociated Processing (CT.DP-P): Data processing solutions increase	**CT.DP-P1:** Data are processed in an unobservable or unlinkable manner (e.g., data actions take	ISO/IEC 27701:2019 7.4.4

	disassociability consistent with related policies, processes, procedures, and agreements and the organization’s risk strategy to protect individuals’ privacy.	place on local devices, privacy-preserving cryptography).	
		CT.DP-P2: Data are processed to limit the identification of individuals (e.g., differential privacy techniques, tokenization).	ISO/IEC 27701:2019 7.4.2, 7.4.4
		CT.DP-P3: Data are processed to restrict the formulation of inferences about individuals’ behavior or activities (e.g., data processing is decentralized, distributed architectures).	ISO/IEC 27701:2019 7.4.2, 8.2.2, 8.2.3, 8.2.4
		CT.DP-P4: System or device configurations permit selective collection or disclosure of data elements.	ISO/IEC 27701:2019 7.4.1, 7.4.2
		CT.DP-P5: Attribute references are substituted for attribute values.	ISO/IEC 27701:2019 7.4.4, 7.4.5
		CT.DP-P6: Data processing is limited to that which is relevant and necessary for a system/product/service to meet mission/business objectives.	ISO/IEC 27701:2019 7.4.1, 7.4.2
COMMUNICATE-P (CM-P): Develop and implement appropriate activities to enable organizations and individuals to have a reliable understanding about how data are processed and associated privacy risks.	**Communication Policies, Processes, and Procedures (CM.PP-P):** Policies, processes, and procedures are maintained and used to increase transparency of the organization’s data processing practices (e.g., purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities) and associated privacy risks.	**CM.PP-P1:** Transparency policies, processes, and procedures for communicating data processing purposes, practices, and associated privacy risks are established and in place.	ISO/IEC 27701:2019 7.3.2, 7.3.3, 8.3.1
		CM.PP-P2: Roles and responsibilities (e.g., public relations) for communicating data processing purposes, practices, and associated privacy risks are established.	ISO/IEC 27701:2019 6.3.1.1, 7.3.2, 7.3.3, 8.3.1

	Data Processing Awareness (CM.AW-P): Individuals and organizations have reliable knowledge about data processing practices and associated privacy risks, and effective mechanisms are used and maintained to increase predictability consistent with the organization's risk strategy to protect individuals' privacy.	**CM.AW-P1:** Mechanisms (e.g., notices, internal or public reports) for communicating data processing purposes, practices, associated privacy risks, and options for enabling individuals' data processing preferences and requests are established and in place.	ISO/IEC 27701:2019 7.3.2, 7.3.3, 8.3.1
		CM.AW-P2: Mechanisms for obtaining feedback from individuals (e.g., surveys or focus groups) about data processing and associated privacy risks are established and in place.	ISO/IEC 27701:2019 5.2.2, 7.3.9, 8.3.1,
		CM.AW-P3: System/product/service design enables data processing visibility.	ISO/IEC 27701:2019 7.3.2, 7.3.3, 8.3.1
		CM.AW-P4: Records of data disclosures and sharing are maintained and can be accessed for review or transmission/disclosure.	ISO/IEC 27701:2019 7.5.4, 8.5.3, 8.5.4, 8.5.5
		CM.AW-P5: Data corrections or deletions can be communicated to individuals or organizations (e.g., data sources) in the data processing ecosystem.	ISO/IEC 27701:2019 7.3.2, 7.3.3, 7.3.7, 8.3.1
		CM.AW-P6: Data provenance and lineage are maintained and can be accessed for review or transmission/disclosure.	ISO/IEC 27701:2019 7.2.8, 8.2.6, 6.5.2.1, 6.5.2.2
		CM.AW-P7: Impacted individuals and organizations are notified about a privacy breach or event.	ISO/IEC 27701:2019 6.13.1.5
		CM.AW-P8: Individuals are provided with mitigation mechanisms to address impacts to individuals that arise from data processing.	ISO/IEC 27701:2019 7.3.6, 8.3.1
PROTECT-P (PR-P): Develop and implement appropriate data processing safeguards.	**Identity Management, Authentication, and Access Control (PR.AC-P):** Access to data and devices is limited to authorized individuals,	**PR.AC-P1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized individuals, processes, and devices.	ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2, 6.6.4.2
		PR.AC-P2: Physical access to data and devices is managed.	ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2, 6.3.2.1

	processes, and devices, and is managed consistent with the assessed risk of unauthorized access.	**PR.AC-P3:** Remote access is managed.	ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2
		PR.AC-P4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties.	ISO/IEC 27701:2019 6.6.2.1, 6.6.2.2
		PR.AC-P5: Network integrity is protected (e.g., network segregation, network segmentation).	ISO/IEC 27701:2019 6.11.1.2
		PR.AC-P6: Individuals and devices are proofed and bound to credentials, and authenticated commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	ISO/IEC 27701:2019 6.6.4.2
	Data Security (PR.DS-P): Data are managed consistent with the organization's risk strategy to protect individuals' privacy and maintain data confidentiality, integrity, and availability.	**PR.DS-P1:** Data-at-rest are protected.	ISO/IEC 27701:2019 6.7.1.1
		PR.DS-P2: Data-in-transit are protected.	ISO/IEC 27701:2019 6.5.3.3, 6.11.1.2
		PR.DS-P3: Systems/products/services and associated data are formally managed throughout removal, transfers, and disposition.	ISO/IEC 27701:2019 6.5.3.2, 6.8.2.7, 7.4.5, 7.4.6, 7.4.8, 7.4.9, 8.4.2
		PR.DS-P4: Adequate capacity to ensure availability is maintained.	ISO/IEC 27701:2019 6.9.1.3
		PR.DS-P5: Protections against data leaks are implemented.	ISO/IEC 27701:2019 All of section 6
		PR.DS-P6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	ISO/IEC 27701:2019 6.15.2.3
		PR.DS-P7: The development and testing environment(s) are separate from the production environment.	ISO/IEC 27701:2019 6.11.3.1
		PR.DS-P8: Integrity checking mechanisms are used to verify hardware integrity.	ISO/IEC 27701:2019 6.15.2.3

	Data Protection Policies, Processes, and Procedures (PR.DP-P): Security and privacy policies (which address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of data.	**PR.DP-P1:** A baseline configuration of information technology is created and maintained incorporating security principles (e.g., concept of least functionality).	ISO/IEC 27701:2019 7.4.1, 7.4.2
		PR.DP-P2: Configuration change control processes are established and in place.	ISO/IEC 27701:2019 6.11.2.2
		PR.DP-P3: Backups of information are conducted, maintained, and tested.	ISO/IEC 27701:2019 6.9.3.1
		PR.DP-P4: Policy and regulations regarding the physical operating environment for organizational assets are met.	ISO/IEC 27701:2019 All of 6.8
		PR.DP-P5: Protection processes are improved.	ISO/IEC 27701:2019 5.2.4
		PR.DP-P6: Effectiveness of protection technologies is shared.	ISO/IEC 27701:2019 7.3.3, 8.3.1
		PR.DP-P7: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are established, in place, and managed.	ISO/IEC 27701:2019 6.13.1.1, 6.14.1.1
		PR.DP-P8: Response and recovery plans are tested.	ISO/IEC 27701:2019 6.14.1.3
		PR.DP-P9: Privacy procedures are included in human resources practices (e.g., deprovisioning, personnel screening).	ISO/IEC 27701:2019 6.10.2.4, 6.6.2.2, 6.8.2.9
		PR.DP-P10: A vulnerability management plan is developed and implemented.	ISO/IEC 27701:2019 6.15.2.3
	Maintenance (PR.MA-P): System maintenance and repairs are performed consistent with policies, processes, and procedures.	**PR.MA-P1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools.	ISO/IEC 27701:2019 6.8.2.4
		PR.MA-P2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	ISO/IEC 27701:2019 6.3.2.2

	Protective Technology (PR.PT-P): 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.	**PR.PT-P1:** Removable media is protected and its use restricted according to policy.	ISO/IEC 27701:2019 6.5.3.1, 6.5.3.2
		PR.PT-P2: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	ISO/IEC 27701:2019 7.4.1, 7.4.2
		PR.PT-P3: Communications and control networks are protected.	ISO/IEC 27701:2019 6.10.1.1, 6.10.1.2, 6.10.1.3, 6.10.2.1
		PR.PT-P4: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	**ISO/IEC 27701:2019 6.14.1.2**