{databrackets cybersecurity • audit • compliance}

SOC 2 **Readiness** Report - Demo

databrackets

June 2, 2020

Prepared By:
Srini Kolathur

{databrackets cybersecurity · audit · compliance}

Contents

{databrackets cybersecurity · audit · compliance}

databrackets
cybersecurity • audit • compliance

1 Executive Summary

37

Assessment Score

THE IMPORTANCE OF SOC 2 COMPLIANCE
While SOC 2 compliance isn't a requirement for SaaS and cloud computing vendors, its role in securing your data cannot be overstated.

Imperva undergoes regular audits to ensure the requirements of each of the five trust principles are met and that we remain SOC 2-compliant. Compliance extends to all services we provide, including web application security, DDoS protection, content delivery through our CDN and load balancing.

There are two types of SOC reports:

Type I describes a vendor's systems and whether their design is suitable to meet relevant trust principles.
Type II details the operational effectiveness of those systems.
SOC 2 CERTIFICATION
SOC 2 certification is issued by outside auditors. They assess the extent to which a vendor complies with one or more of the five trust principles based on the systems and processes in place.

Trust principles are broken down as follows:

Security
The security principle refers to protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of software, and improper alteration or disclosure of information.

IT security tools such as network and web application firewalls (WAFs), two factor authentication and intrusion detection are useful in preventing security breaches that can lead to unauthorized access of systems and data.

Availability
The availability principle refers to the accessibility of the system, products or services as stipulated by a contract or service level agreement (SLA). As such, the minimum acceptable performance level for system availability is set by both parties.

This principle does not address system functionality and usability, but does involve security-related criteria

{databrackets cybersecurity · audit · compliance}

that may affect availability. Monitoring network performance and availability, site failover and security incident handling are critical in this context.

Processing integrity
The processing integrity principle addresses whether or not a system achieves its purpose (i.e., delivers the right data at the right price at the right time). Accordingly, data processing must be complete, valid, accurate, timely and authorized.

However, processing integrity does not necessarily imply data integrity. If data contains errors prior to being input into the system, detecting them is not usually the responsibility of the processing entity. Monitoring of data processing, coupled with quality assurance procedures, can help ensure processing integrity.

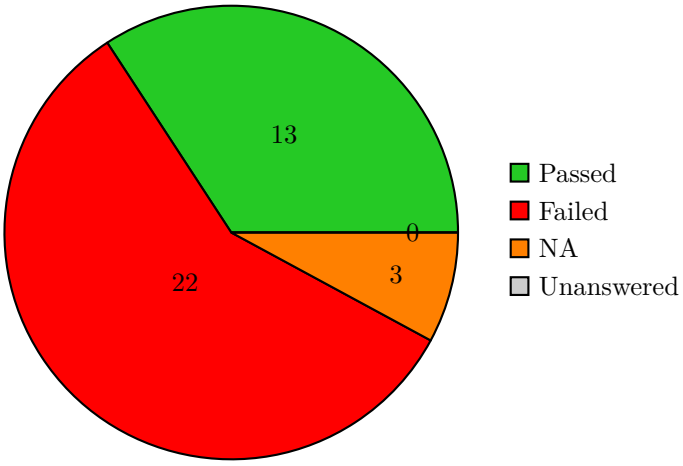
Confidentiality
Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations. Examples may include data intended only for company personnel, as well as business plans, intellectual property, internal price lists and other types of sensitive financial information.

Encryption is an important control for protecting confidentiality during transmission. Network and application firewalls, together with rigorous access controls, can be used to safeguard information being processed or stored on computer systems.

Privacy
The privacy principle addresses the system's collection, use, retention, disclosure and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's generally accepted privacy principles (GAPP).

Personal identifiable information (PII) refers to details that can distinguish an individual (e.g., name, address, Social Security number). Some personal data related to health, race, sexuality and religion is also considered sensitive and generally requires an extra level of protection. Controls must be put in place to protect all PII from unauthorized access.

{databrackets cybersecurity · audit · compliance}



2 Results Overview

Module	Incl in Assessment	# Areas Covered	Pass %	Failure %	Not Applicable
Control Environment	Yes	5	20%	80%	0
Communication and Information	Yes	3	100%	0%	2
Risk Assessment	Yes	4	0%	100%	0
Monitoring Activities	Yes	2	50%	50%	0
Control Activities	Yes	3	0%	100%	0
Logical and Physical Access Controls	Yes	8	38%	62%	0
System Operations	Yes	5	60%	40%	0
Change Management	Yes	1	0%	100%	0
Risk Mitigation	Yes	2	100%	0%	1
Availability	Yes	3	33%	67%	0
Confidentiality	Yes	2	100%	0%	0
Processing Integrity	No				
Privacy	No				

3 Action Plan Summary

Module	Question	Action Plan	Priority	Due Date	Status
Availability	The entity maintains, monitors, and evaluates curr..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Availability	The entity tests recovery plan procedures supporti..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Environment	COSO Principle 2: The board of directors demonstra..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress

{databrackets cybersecurity · audit · compliance}

Control Environment	COSO Principle 3: Management establishes, with boa..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Environment	COSO Principle 4: The entity demonstrates a commit..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Environment	COSO Principle 5: The entity holds individuals acc..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Risk Assessment	COSO Principle 6: The entity specifies objectives ..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Risk Assessment	COSO Principle 7: The entity identifies risks to t..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Risk Assessment	COSO Principle 8: The entity considers the potenti..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Risk Assessment	COSO Principle 9: The entity identifies and assess..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Monitoring Activities	COSO Principle 17: The entity evaluates and commun..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Activities	COSO Principle 10: The entity selects and develops..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Activities	COSO Principle 11: The entity also selects and dev..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Control Activities	COSO Principle 12: The entity deploys control acti..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Logical and Physical Access Controls	Prior to issuing system credentials and granting s..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Logical and Physical Access Controls	The entity authorizes, modifies, or removes access..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Logical and Physical Access Controls	The entity restricts physical access to facilities..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Logical and Physical Access Controls	The entity discontinues logical and physical prote..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress

databrackets
cybersecurity · audit · compliance

Logical and Physical Access Controls	The entity implements controls to prevent or detec..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
System Operations	The entity monitors system components and the oper..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
System Operations	The entity evaluates security events to determine ..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress
Change Management	The entity authorizes, designs, develops or acquir..	Action plan for this control will be implemented a..	Medium	2020-12-02	In Progress

databrackets
cybersecurity · audit · compliance

4 Identified Risks with Action Plan

These are risks that have been identified, evaluated, and have an Action Plan. We have identified 0 high, 22 medium, and 0 low action items. Of all items in the action plan, 22 are pending and 0 are complete.

4.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. (A1.1)

Module: Availability

Response: Insufficient Information

Comments: Sufficient information is not available at this point in time to close this item. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.2 The entity tests recovery plan procedures supporting system recovery to meet its objectives. (A1.3)

Module: Availability

Response: In Progress

Comments: This control is currently in the process of being implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.3 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. (CC1.2)

Module: Control Environment

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 2.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.4 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. (CC1.3)

Module: Control Environment

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 3.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.5 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. (CC1.4)

Module: Control Environment

Response: In Progress

Comments: This control is currently in the process of being implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 4.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.6 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. (CC1.5)

Module: Control Environment

Response: Insufficient Information

Comments: Sufficient information is not available at this point in time to close this item. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 5.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.7 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. (CC3.1)

Module: Risk Assessment

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 6.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.8 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. (CC3.2)

Module: Risk Assessment

Response: Insufficient Information

Comments: Sufficient information is not available at this point in time to close this item. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 7.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.9 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. (CC3.3)

Module: Risk Assessment

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 8.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.10 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. (CC3.4)

Module: Risk Assessment

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 9.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.11 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. (CC4.2)

Module: Monitoring Activities

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 17.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.12 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. (CC5.1)

Module: Control Activities

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 10.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.13 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. (CC5.2)

Module: Control Activities

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 11.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.14 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. (CC5.3)

Module: Control Activities

Response: Not Implemented

Comments: This control is currently in the process of being implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle 12.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.15 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. (CC6.2)

Module: Logical and Physical Access Controls

Response: Insufficient Information

Comments: Sufficient information is not available at this point in time to close this item. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.16 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives. (CC6.3)

Module: Logical and Physical Access Controls

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.17 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. (CC6.4)

Module: Logical and Physical Access Controls

Response: Not Implemented

Comments: This control is not implemented yet according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

databrackets
cybersecurity • audit • compliance

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.18 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. (CC6.5)

Module: Logical and Physical Access Controls

Response: Insufficient Information

Comments: Sufficient information is not available at this point in time to close this item. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.19 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. (CC6.8)

Module: Logical and Physical Access Controls

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

{databrackets cybersecurity · audit · compliance}

4.20 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. (CC7.2)

Module: System Operations

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.21 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. (CC7.3)

Module: System Operations

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

Target Date for Completion: 2020-12-02

4.22 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. (CC8.1)

Module: Change Management

Response: Partially Implemented

Comments: This control is partially implemented according to the description and intent of the control. Required evidence, if any, is attached.

Action Plan: Action plan for this control will be implemented according to the stated and intended description provided in COSO principle.

Status: In Progress

Priority: Medium

{databrackets} cybersecurity • audit • compliance

Target Date for Completion: 2020-12-02

5 Managed or Not Present Risks

Problems that have been managed or are not present in your organization.

5.1 Control Environment

5.1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. (CC1.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.2 Communication and Information

5.2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. (CC2.1)

Response: Not Applicable

Comments: This control is not applicable to our organization. Required evidence, if any, is attached.

5.2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. (CC2.2)

Response: Not Applicable

Comments: This control is not applicable to our organization. Required evidence, if any, is attached.

5.2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. (CC2.3)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

{databrackets} cybersecurity · audit · compliance

5.3 Monitoring Activities

5.3.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. (CC4.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.4 Logical and Physical Access Controls

5.4.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives. (CC6.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.4.2 The entity implements logical access security measures to protect against threats from sources outside its system boundaries. (CC6.6)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.4.3 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives. (CC6.7)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.5 System Operations

5.5.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. (CC7.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

{databrackets} cybersecurity • audit • compliance

5.5.2 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. (CC7.4)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.5.3 The entity identifies, develops, and implements activities to recover from identified security incidents. (CC7.5)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.6 Risk Mitigation

5.6.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. (CC9.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.6.2 The entity assesses and manages risks associated with vendors and business partners. (CC9.2)

Response: Not Applicable

Comments: This control is not applicable to our organization. Required evidence, if any, is attached.

5.7 Availability

5.7.1 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. (A1.2)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

{databrackets} cybersecurity • audit • compliance

5.8 Confidentiality

5.8.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. (C1.1)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

5.8.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality. (C1.2)

Response: Implemented

Comments: This control is fully implemented according to the description and intent of the control. Required evidence, if any, is attached.

---

6 Unidentified Risks

Risks that have not been identified yet due to question not being answered.

6.1 Processing Integrity

6.1.1 The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services. (Pl1.1)

6.1.2 The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives. (Pl1.2)

{databrackets} cybersecurity · audit · compliance

6.1.3 **The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives. (Pl1.3)**

6.1.4 **The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives. (Pl1.4)**

6.1.5 **The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives. (Pl1.5)**

6.2 Privacy

6.2.1 **The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. (P1.1)**

6.2.2 **The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented. (P2.1)**

{databrackets} cybersecurity · audit · compliance

6.2.3 **Personal information is collected consistent with the entity's objectives related to privacy. (P3.1)**

6.2.4 **For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information, and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy. (P3.2)**

6.2.5 **The entity limits the use of personal information to the purposes identified in the entity's objectives related to privacy. (P4.1)**

6.2.6 **The entity retains personal information consistent with the entity's objectives related to privacy. (P4.2)**

6.2.7 **The entity securely disposes of personal information to meet the entity's objectives related to privacy. (P4.3)**

6.2.8 **The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy. (P5.1)**

6.2.9 **The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy. (P5.2)**

{databrackets} cybersecurity · audit · compliance

6.2.10 **The entity discloses personal information to third parties with the explicit consent of data subjects, and such consent is obtained prior to disclosure to meet the entity's objectives related to privacy. (P6.1)**

6.2.11 **The entity creates and retains a complete, accurate, and timely record of authorized disclosures of personal information to meet the entity's objectives related to privacy. (P6.2)**

6.2.12 **The entity creates and retains a complete, accurate, and timely record of detected or reported unauthorized disclosures (including breaches) of personal information to meet the entity's objectives related to privacy. (P6.3)**

6.2.13 **The entity obtains privacy commitments from vendors and other third parties who have access to personal information to meet the entity's objectives related to privacy. The entity assesses those parties' compliance on a periodic and as-needed basis and takes corrective action, if necessary. (P6.4)**

6.2.14 **The entity obtains commitments from vendors and other third parties with access to personal information to notify the entity in the event of actual or suspected unauthorized disclosures of personal information. Such notifications are reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's objectives related to privacy. (P6.5)**

6.2.15 **The entity provides notification of breaches and incidents to affected data subjects, regulators, and others to meet the entity's objectives related to privacy. (P6.6)**

{databrackets cybersecurity • audit • compliance}

6.2.16 The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy. (P6.7)

6.2.17 The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy. (P7.1)

6.2.18 The entity implements a process for receiving, addressing, resolving, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance to meet the entity's objectives related to privacy. Corrections and other necessary actions related to identified deficiencies are made or taken in a timely manner. (P8.1)
