



**CYBER;**  
**Critical Security Controls for Effective Cyber Defence;**  
**Part 5: Privacy enhancement**

---

**Reference**

---

DTR/CYBER-0034-5

---

**Keywords**

---

cyber security, cyber-defence, information assurance, privacy**ETSI**

---

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**Important notice**

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

If you find errors in the present document, please send your comment to one of the following services:

<https://portal.etsi.org/People/CommitteeSupportStaff.aspx>

---

**Copyright Notification**

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2018.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

**3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**oneM2M** logo is protected for the benefit of its Members.

**GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

---

# Contents

Intellectual Property Rights .....	4
Foreword.....	4
Modal verbs terminology.....	4
Executive summary .....	4
Introduction .....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	5
3 Abbreviations .....	5
4 Critical Security Controls: Privacy Impact Assessment.....	6
4.1 Description .....	6
4.2 Privacy Impact Assessment of the Critical Security Controls .....	6
4.2.1 Overview .....	6
4.2.2 Authorities .....	6
4.2.3 Characterizing Control-Related Information .....	7
4.2.4 Uses of Control-Related Information.....	7
4.2.5 Security .....	8
4.2.6 Notice.....	8
4.2.7 Data Retention .....	9
4.2.8 Information Sharing .....	9
4.2.9 Redress.....	9
4.2.10 Auditing and Accountability.....	9
5 How to support the EU General Data Protection Regulation (GDPR) using the Critical Security Controls .....	10
5.1 Description .....	10
5.2 GDPR responsibilities .....	10
5.3 What data is in scope?.....	10
5.4 Assessing the data and the privacy risks .....	11
5.5 Specific Critical Security Controls in support of GDPR.....	11
5.6 Use of Hardened virtual machine images.....	12
History .....	13

---

## Intellectual Property Rights

### Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<https://ipr.etsi.org/>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

### Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

---

## Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 5 of a multi-part deliverable covering the Critical Security Controls for Effective Cyber Defence. Full details of the entire series can be found in part 1 [i.2].

---

## Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

---

## Executive summary

The present document is an evolving repository for privacy enhancement guidelines for Critical Security Control implementations. These guidelines include a privacy impact assessment mechanism and as well as implementations to meet provisions of the EU General Data Protection Regulation (GDPR) using the Critical Security Controls.

---

## Introduction

The Critical Security Controls ("the Controls") exist within a larger cyber security ecosystem that relies on the Controls as critically important defensive measures. There are a variety of mechanisms that facilitate and encourage their use - one of which notably includes privacy protection. In addition, the Controls can help meet provisions of the EU General Data Protection Regulation (GDPR) using the Critical Security Controls. The present document is directed at both privacy objectives.

NOTE: Clause 4 existed in a previous version of ETSI TR 103 305-4 [i.3] and was moved to the present document.

---

## 1 Scope

The present document is an evolving repository for privacy enhancing implementations using the Critical Security Controls [i.2]. These presently include a privacy impact assessment and use of the Controls to help meet provisions of the EU General Data Protection Regulation (GDPR) [i.1].

---

## 2 References

### 2.1 Normative references

Normative references are not applicable in the present document.

### 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- [i.2] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".
- [i.3] ETSI TR 103 305-4: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".
- [i.4] U.S. Department of Homeland Security (DHS): "Fair Information Practice Principles (FIPPs)".

NOTE: Available at <https://www.dhs.gov/publication/fair-information-practice-principles-fipps-0#>.

---

## 3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	3 <sup>rd</sup> Generation Partnership Project
CRM	Customer Relationship Management
CSC	Critical Security Control or Capability
DHS	Department of Homeland Security
EU	European Union
FIPP	Fair Information Practice Principles
GDPR	General Data Protection Regulation
GSM	Global System for Mobile
IP	Internet Protocol
IT	Information Technology
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

---

## 4 Critical Security Controls: Privacy Impact Assessment

### 4.1 Description

An effective posture of enterprise cybersecurity need not, and, indeed, should not compromise individual privacy. Many laws, regulations, guidelines, and recommendations exist to safeguard privacy, and enterprises will, in many cases, adapt their existing policies on privacy as they apply the Controls.

Use of the Controls should support the general principles embodied in the *General Data Protection Regulation* [i.1] and the *Fair Information Practice Principles* (FIPPs) [i.4]. All enterprises that apply the Controls should undertake - and make available - privacy impact assessments of relevant systems to ensure that appropriate protections are in place as the Controls are implemented. Every enterprise should also regularly review these assessments as material changes to its cybersecurity posture are adopted. The aim is to assess and mitigate the major potential privacy risks associated with implementing specific Controls as well as evaluate the overall impact of the Controls on individual privacy.

The following framework guides this efforts and provides an outline for a Privacy Impact Assessment.

### 4.2 Privacy Impact Assessment of the Critical Security Controls

#### 4.2.1 Overview

Outline the purpose of each Control and provide justification for any actual or potential intersection with privacy-sensitive information:

- Where possible, identify how technologies, procedures, and data flows are used to implement the Control. Provide a brief description of how the Control generally collects and stores information. Identify the type of data collected by the Control and the kinds of information that can be derived from this data. In discussing how the Control might collect and use PII, include a typical transaction that details the life cycle of that PII from collection to disposal.
- Describe the measures necessary to protect privacy data and mitigate any risks of unauthorized access or inadvertent disclosure of the data. The aim here is not to list every possible risk to privacy, but rather, to provide a holistic view of the risks to privacy that could arise from implementation of the Control.
- Describe any potential ad-hoc or routine information sharing that will result from the implementation of the Control both within the enterprise and with external sharing partners. Also describe how such external sharing is compatible with the original collection of the information, and what agreements would need to be in place to support this sharing.

#### 4.2.2 Authorities

Identify the legal authorities or enterprise policies that would permit or, conversely, limit or prohibit the collection or use of information by the Control:

- List the statutory and regulatory authorities that would govern operation of the Control, including the authorities to collect the information identified above. Explain how the statutory and regulatory authorities permit or would limit collection and use of the information or govern geographic storage requirements. If the Control would conceivably collect Personally Identifiable Information (PII), also identify the specific statutory authority that would permit such collection.
- Would the responsible office of an enterprise be able to rely on authorities of another parent organization, subsidiary, partner or agency?
- Might the information collected by the Control be received from a foreign user, organization or government? If so, do any international agreement, contract, privacy policy or memorandum of understanding exist to support or otherwise govern this collection?

### 4.2.3 Characterizing Control-Related Information

Identify the type of data the Control collects, uses, disseminates, or maintains:

- For each Control, identify both the categories of technology sources, logs, or individuals from whom information would be collected, and, for each category, list any potential PII, that might be gathered, used, or stored to support the Control:
  - Relevant information here includes (but is not limited to): name; date of birth; mailing address; telephone numbers; social security number; e-mail address; mother's maiden name; medical records locators; bank account numbers; health plan beneficiaries; any other account numbers; certificates or other license numbers; vehicle identifiers, including license plates; marriage records; civil or criminal history information; medical records; device identifiers and serial numbers; education records; biometric identifiers; photographic facial images; or any other unique identifying number or characteristic.
- If the output of the Control, or system on which it operates, creates new information from data collected (for example, a scoring, analysis, or report), might this new information have privacy implications? If so, perform the same above analysis on the newly created information.
- If the Control uses information from commercial sources or publicly available data to enrich other data collected, explain how this information might be used:
  - Commercial data includes information from data aggregators (such as threat feeds, or malware databases), or from social networking sources where the information was originally collected by a private organization.
  - Publicly available data includes information obtained from network services, news feeds, or from state or local public records, such as court records where the records are received directly from the state or local agency, rather than from a commercial data aggregator.
  - Identify scenarios with this enriched data might derive data that could have privacy implications. If so, perform the same above analysis on the newly created information.
- Identify and discuss the privacy risks for Control information and explain how they are mitigated. Specific risks may be inherent in the sources or methods of collection.
- Consider the following Fair Information Practice Principles (FIPPs):
  - *Principle of Purpose Specification:* Explain how the collection of PII by the Control links to the cybersecurity needs of the enterprise.
  - *Principle of Minimization:* Is the PII data directly relevant and necessary to accomplish the specific purposes of the Control?
  - *Principle of Individual Participation:* Does the Control, to the extent possible and practical, collect PII directly from individuals?

### 4.2.4 Uses of Control-Related Information

Describe the Control's use of PII or privacy protected data. Describe how and why the Control uses this data:

- List likely uses of the information collected or maintained, both internal and external to the enterprise. Explain how and why different data elements will be used. If national personal identifiers such as Social Security numbers are collected for any reason, for example, describe why such collection is necessary and how such information would be used. Describe types of procedures and protections to be in place to ensure that information is handled appropriately, and policies that need to be in place to provide user notification.
- Does the Control make use of technology to conduct electronic searches, queries, or analyses in a database to discover or locate a predictive pattern or an anomaly? If so, describe what results would be achieved and if there would be possibility of privacy implications.

- Some Controls require the processing of large amounts of information in response to user inquiry or programmed functions. The Controls may help identify data that were previously not identifiable and may generate the need for additional research by analysts or other employees. Some Controls are designed to perform complex analytical tasks resulting in other types of data, matching, relational analysis, scoring, reporting, or pattern analysis.
- Discuss the results generated by the uses described above, including link analysis, scoring, or other analyses. These results may be generated electronically by the information system, or manually through review by an analyst. Would these results potentially have privacy implications?
- Are there other offices or departments within or connected to the enterprise that would receive any data generated? Would there be privacy implications to their use or collection of this data?
- Consider the following FIPPs:
  - *Principle of Transparency*: Is the PIA and related policies clear about the uses of information generated by the Control?
  - *Principle of Use Limitation*: Is the use of information contained in the system relevant to the mission of the Control?

## 4.2.5 Security

Complete a security plan for the information system(s) supporting the Control:

- Is there appropriate guidance when implementing the Control to ensure that appropriate physical, personnel, IT, and other safeguards are in place to protect privacy protected data flowing to and generated from the Control?
- Consider the following Fair Information Practice principle:
  - *Principle of Security*: Is the security appropriate and proportionate to the protected data?

## 4.2.6 Notice

Identify if any notice to individuals should be put in place regarding implementation of the Control, PII collected, the right to consent to uses of information, and the right to decline to provide information (if practicable):

- Define how the enterprise might require notice to individuals prior to the collection of information.
- Enterprises often provide written or oral notice to employees, customers, shareholders, and other stakeholders before they collect information from individuals. For private companies, collecting information from consumers, publicly available privacy policies are used. Describe what notice might be relevant to individuals whose information might be collected by the Control.
- If notice might not, or cannot be provided, define if one is required or how it can be mitigated. For certain law enforcement operations, notice may not be appropriate - enterprises would then explain how providing direct notice to the individual at the time of collection would undermine a law enforcement mission.
- Discuss how the notice provided corresponds to the purpose of the Control and the declared uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how implementation of the Control mitigates the risks associated with potentially insufficient notice and opportunity to decline or consent.
- Consider the following FIPPs:
  - *Principle of Transparency*: Will this Control allow sufficient notice to be provided to individuals?
  - *Principle of Use Limitation*: Is the information used only for the purpose for which notice was provided either directly to individuals or through a public notice? What procedures can be put in place to ensure that information is used only for the purpose articulated in the notice?



- *Principle of Individual Participation*: Will the enterprise be required to provide notice to individuals regarding redress, including access and correction, including other purposes of notice such as types of information and controls over security, retention, disposal, etc.?

#### 4.2.7 Data Retention

Will there be a requirement to develop a records retention policy, subject to approval by the appropriate enterprise authorities (e.g. management, Board), to govern information gathered and generated by the Control?

- Consider the following FIPPs below to assist in providing a response:
  - *Principle of Minimization*: Does the Control have the capacity to use only the information necessary for declared purposes? Would the Control be able to manage PII retained only for as long as necessary and relevant to fulfill the specified purposes?
  - *Principle of Data Quality and Integrity*: Does the PIA describe policies and procedures required by an organization for how PII is purged once it is determined to be no longer relevant and necessary?

#### 4.2.8 Information Sharing

Describe the scope of the information sharing within and external to the enterprise that could be required to support the Control. External sharing encompasses sharing with other businesses, vendors, private sector groups, or federal, state, local, tribal, and territorial government, as well as with governments or official agencies of other countries:

- For state or local government agencies, or private sector organizations list the general types that might be applicable for the Control, rather than the specific names.
- Describe any agreements that might be required for an organization to conduct information sharing as part of normal enterprise operations.
- Discuss the privacy risks associated with the sharing of information outside of the enterprise. How can those risks be mitigated?
- Discuss how the sharing of information is compatible with the stated purpose and use of the original collection for the Control.

#### 4.2.9 Redress

Enterprises should have in place procedures for individuals to seek redress if they believe their PII may have been improperly or inadvertently disclosed or misused through implementation of the Controls. These procedures may include allowing them to file complaints about what data is collected or how it is used:

- Consider the following issue that falls under the FIPP principle of *Individual Participation*:
  - Can a mechanism be applied by which an individual can prevent PII obtained for one purpose from being used for other purposes without the individual's knowledge?

#### 4.2.10 Auditing and Accountability

Describe what technical and policy based safeguards and security measures might be needed to support the Control. Include an examination of technical and policy safeguards, such as information sharing protocols, special access restrictions, and other controls:

- Discuss whether the Control allows for self-audits, permits third party audits, or allows real time or forensic reviews by appropriate oversight agencies.
- Do the IT systems supporting the Control have automated tools to indicate when information is possibly being misused?

- Describe what requirements for privacy training should be provided to users either generally or specifically relevant to the Control, including information handling procedures and sensitivity of information. Discuss how individuals who have access to PII collected or generated by the Control should be trained to appropriately handle that information.
- Discuss the types of processes and procedures necessary to review and approve information sharing agreements, new uses of Control information, and new access to Control information by other parties.

---

## 5 How to support the EU General Data Protection Regulation (GDPR) using the Critical Security Controls

### 5.1 Description

The new European Union (EU) General Data Protection Regulation (GDPR) in effect since 25 May 2018 has many repercussions for any organization collecting, processing, and/or storing any EU citizen's information [i.1].

The regulation's specific requirements focus on the management and protection of personal data related to EU citizens. The essential characteristics of the regulation are to protect personal data as a fundamental right and that privacy is to be respected as an expectation of the GDPR. The GDPR creates a greater level of harmonization across the EU for the sharing and exchange of data. Implementation of the GDPR requirements necessitates a greater level of protection of a person's digital identity.

The reason for such an increased worldwide emphasis on compliance is due to the imposed fines that can be applied if one fail to manage the privacy data appropriately.

### 5.2 GDPR responsibilities

Two specific roles that are defined in the regulation are data controller and data processor:

- A "data controller" is the collector of the data for internal or outsourced processing. This role is responsible for documenting the format of how the data are to be utilized throughout its lifecycle within the organization, privacy policies, and the ability to process requests for data portability, rectification, objection, etc. The duties that are required for this role include compliance to protect the data subject's rights. Examples of data controllers include social media organizations, education institutions, health organizations, Banks, etc. If one organization determines how the data is to be processed and the purpose of that processing, this indicates a data controller.
- A "data processor" is a natural or legal person, public authority, agency or other body responsible for managing and storing data on behalf of the controller. Specific clauses within the regulation require the same technical and organizational measures to be applied to the controller as well as the processor. An example would be an outsourced payroll company; the data controller tells the payroll organization who to pay and what amount. If an entity is not making these decisions and just acting on a request, this indicates a data processor.

The required liability flows through the chain of data processing. Specifically, the data controller has liability if a data processor fails to fulfill his obligations.

### 5.3 What data is in scope?

Article 4(1) of GDPR states: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Elements of data types could include IP addresses, cookie data, or a photograph associated to an account. In many cases, personal customer data will be in multiple formats and forms in CRMs (Customer Relationship Management systems), contracts, sales contact databases, etc.

## 5.4 Assessing the data and the privacy risks

Specific items that may be required by the GDPR:

- Mandatory breach notifications - fast response and large fines
- The 'Right To Be Forgotten' - necessitating the 'ability to be found'
- Consumer profiling restrictions - personal data should not be used without consent
- Be accountable for your data - conduct a Privacy Impact Assessment to determine what type of Personal Data is handled, processed and stored, and for what purpose
- Access to personal data - right to access and control based on a 'need to know'
- Right to rectification - right to update data and correct inaccurate data
- Privacy by Design - new functions and elements of future processing capability or personal data management should utilize this as a non-functional requirement in the conceptualization of the business process, and
- Manage privacy risk - the correlation of processes requiring access and use of personal data need to be understood and controlled

Key provisions in the GDPR relating to management of privacy risk include:

- Appropriate technical measures
- Demonstrate compliance
- Appropriate safeguards
- Measures reviewed and updated
- Implement appropriate data protections

## 5.5 Specific Critical Security Controls in support of GDPR

Specific to the data controller and the data processor roles, responsibilities are to "implement appropriate technical and organizational measures to ensure and be able to demonstrate that processing is performed in accordance with the regulation".

The Critical Security Controls are a prioritized set of cybersecurity best practices to help organizations improve their security posture as well as be applied in support of GDPR compliance. The Controls can serve both as a measurement process to encourage compliance as well as for implementing a security control framework within an organization. In many cases, the entire Critical Security Controls can be applicable to implement a structured and measured approach to compliance and security for the organization.

Examples of applying the Critical Security Controls to GDPR compliance are described in table 5-1. This clause is specifically designed as guidance to initiate a control program that includes elements of in support for compliance to the GDPR.

**Table 5-1: Critical Security Controls Applied in support of GDPR**

NOTE: The use of *shall* in table 5-1 is taken from the indicated GDPR provision citations. The citations are provided for reference and not intended to make the related Critical Security Controls normative [i.1].

<b>CSC</b>	<b>Critical Security Control</b>	<b>GDPR Provision Citations</b>
6	Maintenance, Monitoring and Analysis of Audit Log	<i>Art. 30 Records of processing activities</i>
13	Data Protection	<p><i>Art. 5(1)(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures</i></p> <p><i>Art. 24(2) the implementation of appropriate data protection policies</i></p> <p><i>Art. 25(2) only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility</i></p> <p><i>Art. 28(4) requirement to fulfill the data protection requirements across the data processing supply chain</i></p> <p><i>Art. 32(1) (a-d) the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk</i></p> <p><i>Art. 32(2) appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed</i></p> <p><i>Art. 35(1) carry out an assessment of the impact of the envisaged processing operations on the protection of personal data</i></p> <p><i>Art. 35(7)(d) including safeguards, security measures and mechanisms to ensure the protection of personal data</i></p>
14	Controlled Access Based on the Need to Know	<p><i>Art. 5(1)(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes</i></p> <p><i>Art. 5(1)(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures</i></p> <p><i>Art. 6(4)(e) the existence of appropriate safeguards, which may include encryption or pseudonymization</i></p> <p><i>Art. 25(2) only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility</i></p> <p><i>Art. 32(1)(a-d) the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk</i></p> <p><i>Art. 35(1) carry out an assessment of the impact of the envisaged processing operations on the protection of personal data</i></p>
17	Implement a Security Awareness and Training Program	<i>Art. 39(1)(b) training of staff involved in processing operations</i>
19	Incident Response and Management	<i>Art. 33(3)(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects</i>

Implementers should review and implement all appropriate security controls in order to conform to the full compliance requirements. This review includes a complete understanding and visualization of the data flows for personal information throughout the enterprise.

## 5.6 Use of Hardened virtual machine images

When the enterprise makes use of cloud data centers, implementors should consider the use of pre-hardened virtual machines for the principal marketplace platforms described in Part 4 of the present Technical Report. Such hardened images conform to the applicable security standards of the Critical Security Control benchmarks, and provide on-demand security to cloud computing environments.

---

## History

<b>Document history</b>		
V1.1.1	September 2018	Publication