ISACA

TRUST IN, AND VALUE FROM, INFORMATION SYSTEMS

ISACA.ORG

Formed in 1969 as an audit organisation, but has grown to cover all aspects of IT governance, security, risk, audit and cybersecurity

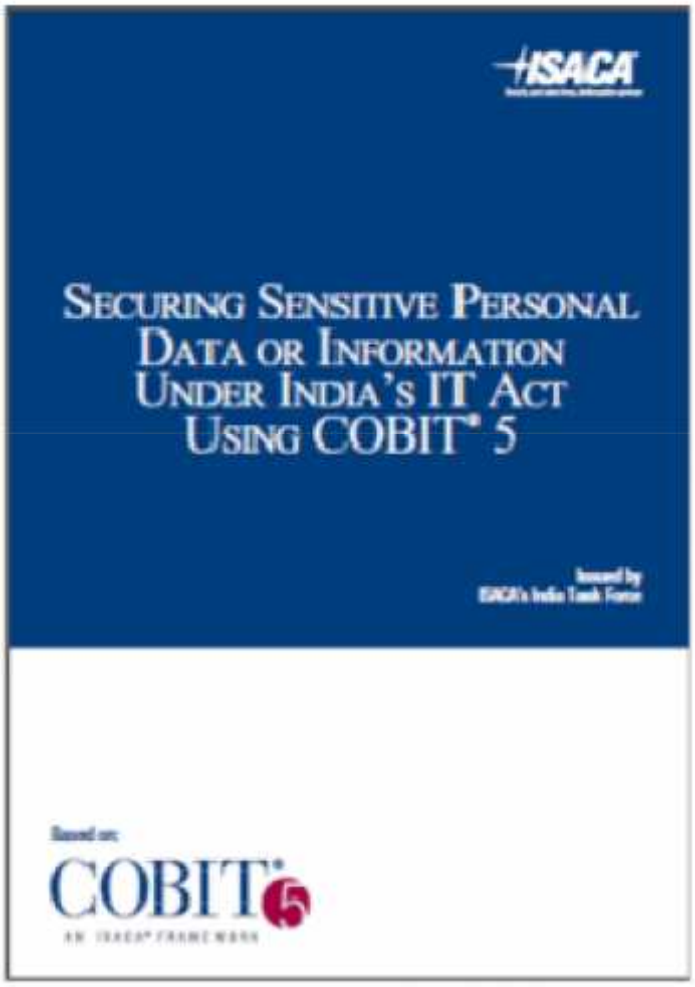
ISACA FACTS

- Founded in 1969 as the EDP Auditors Association
- More than 115,000 members in over 180 countries
- More than 200 chapters worldwide

Business Framework for Governance and Management of Enterprise Information Technology

ISACA
Trust in, and value from, information systems

SECURING SENSITIVE PERSONAL DATA OR INFORMATION UNDER INDIA'S IT ACT USING COBIT - 5



You can download it from www.isaca.org/topic-india

ISACA
Trust in, and value from, information systems

Objective of the publication

Securing SPDI is now mandated by India's IT (Amendment) Act, 2008. This publication helps provide an approach to achieve this objective using the COBIT 5 framework.

ISACA
Trust in, and value from, information systems

Hackers have stolen information on tens of millions of Anthem Inc. customers, in a massive data breach that ranks among the largest in corporate history

- On January 29, 2015, Anthem, Inc. (Anthem) learned of a cyberattack to our IT system. The cyberattackers tried to get private information about current and former Anthem members. We believe **it happened over the course of several weeks beginning in early December 2014.**
- What did the cyberattackers access?

Accessed information may have included:

- Names
- Dates of birth
- Social Security numbers
- Health care ID numbers
- Home addresses
- Email addresses
- Work information like income data

Anthem doesn't believe these kinds of information were targeted or accessed:

- Credit card or banking information
- Medical information like claims, test results or diagnostic codes

ISACA®
Trust in, and value from, information systems

LESSON TO LEARN

- The question to ask yourself is –
  - ☹ **When will this happen to me ?**
  - ~~😐(and not - Will this happen to me?)~~
  - ☺ **Am I ready**
- Prepare yourself well
- Answer all the questions given in the checklist
- Make sure you have all the (correct) answers

ISACA
Trust in, and value from, information systems

2. Who is obliged to protect sensitive personal data as per the IT Act and Rules? **(See Section 43 A of the IT Act.)** **(See explanation (i) to Section 43 A of the IT Act.)**	The obligation to protect sensitive personal data applies to every entity (body corporate) that: • Possesses, deals with or handles any SPDI • In a computer resource that it owns, controls or operates 'Body corporate' means any company and includes: • A firm (such as a partnership firm) • Sole proprietorship (such as a consultancy firm owned by a single person) • Other association of individuals (such as professional bodies and organisations) engaged in commercial or professional activities

Checklist

1. Is the entity concerned a firm—sole proprietorship or partnership? A private limited or public limited company? Or any other association of individuals (such as those registered as a society or public trust or other organisation)?
2. Does it possess, deal with or handle sensitive personal data (explained below)?
3. Are such data in a computer resource?
4. Does the entity own, control or operate such computer resource?
5. Is such firm, sole proprietorship or other association of individuals engaged in commercial or professional activities?

3. What is sensitive personal data or information? **(See Rule 3 of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	**SPDI has been defined under the Rules to mean such personal information that consists of information relating to:** • Password • Financial information such as bank account, credit card, debit card or other payment instrument details • Physical, physiological and mental health condition • Sexual orientation • Medical records and history • Biometric information • Any detail relating to the above clauses as provided to the body corporate for providing service • Any of the information received under the above clauses by the body corporate for processing, stored or processed under lawful contract or otherwise

Checklist

1. Do we have mechanisms in place to identify sensitive personal data already with us or provided to us for use, processing or storage?
2. Do we have in place mechanisms to determine if combinations of data available with us would apply to the aforesaid definition of sensitive personal data?

5. What happens if the body corporate fails to keep sensitive personal data secure? **(See Section 43 A of the IT Act.)**	Where an entity that is obliged to maintain security of sensitive personal data is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such entity would be liable to **pay damages by way of compensation** to the person so affected. (See item 27 in this chapter on how compensation is decided.) **Checklist** 1. Was the entity negligent in implementing and maintaining reasonable security practices and procedures (explained below)? 2. Was wrongful loss or wrongful gain caused to any person by such negligence?
27. How will compensation be decided? **(See Section 47 of the IT Act.)**	While adjudging the quantum of compensation, the adjudicating officer shall have due regard to the following factors: • The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default • The amount of loss caused to any person as a result of the default • The repetitive nature of the default
28. What is the IT Act provision for providing punishment for disclosure of information in breach of lawful contract ? **(See Section 72A of the IT Act, inserted in 2008.)**	**Punishment for disclosure of information in breach of lawful contract:** Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, **with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain** discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees (rupees 0.5 million) or with both.

6. What are the reasonable security practices to be implemented? **(See Section 43 A of the IT Act.)**	'Reasonable security practices and procedures'* means security practices and procedures designed to protect information from unauthorised access, damage, use, modification, disclosure or impairment: • As may be specified in an agreement between the parties • As may be specified in any law for the time being in force • And in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit *See items 23 and 24 below for the relevant provisions of the Rules under the IT Act that explain reasonable security practices and procedures. Item 24 refers to the International standard ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*, as being a Government approved standard for reasonable security practices and procedures.
	Checklist
	1. Is it sensitive personal information? 2. Does any agreement specify protection from unauthorised access, etc.? 3. Does any sector-specific law specify such protection? 4. Is protection specified under the Central Government notified Rules issued on 11 April 2011 and titled 'Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules', 2011?

7. What are a body corporate's obligations as to privacy policy? **(See Rule 4 of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	Rule 4. Body corporate to provide policy for privacy and disclosure of Information. (1) The body corporate or any person who on behalf of body corporate collects, receives, possesses, stores, deals or handles information of provider of information, shall provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that the same are available for view by such providers of information who have provided such information under lawful contract. The Department of Information Technology of the Ministry of Communications & Information Technology, Government of India, issued a press release on 24 August, 2011 stating, among other things: *It is also clarified that privacy policy, as prescribed in Rule 4, relates to the body corporate and is not with respect to any particular obligation under any contract.* **Note:** The purpose of this clarification appears to be that any contractual obligations assumed by a body corporate would not necessarily be covered by the privacy policy prescribed under Rule 4.
	Checklist
	1. Do we collect, receive, possess, store, deal with or handle personal information (including sensitive personal data)? 2. Is the personal information made available under lawful contract? **Note:** Although the IT Act does not say so specifically, the term "contract" here presumably refers to a contract between the body corporate and the provider of information. 3. Do we have a privacy policy? 4. Is the personal information available for viewing by the people who provide their personal information?

8. Where should the privacy policy be posted? What should it cover? *(cont.)* (See Rule 4 of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)	**Checklist**
	1. Is our privacy policy clear? Have we obtained feedback after review by persons who have provided their personal information? Have we provided an email address to which visitors could write for clarifications if the policy is not clear to them? 2. Does it cover both our policies and practices? • A policy is an overall intention and direction as formally expressed by management. • A good practice is a proven activity or process that has been successfully used by multiple enterprises and has been shown to produce reliable results. 3. Does it explain the type of personal information that we collect? 4. Does it explain why we collect and use the personal data (the purpose)? 5. Is the purpose stated by us broad enough to cover potential uses of the personal information that we can foresee? 6. Do we state how and to whom we may disclose the personal data? 7. Is such statement of possible disclosure broad enough to cover potential disclosures that we can foresee? 8. Does the policy state how we adopt the 'reasonable security practices and procedures', as explained below?

9. How do we get consent for collection or usage of personal data? **(See Rule 5 of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data Information] Rules, 2011.)**	The body corporate or any person on its behalf shall obtain: • Consent in writing through letter or fax or consent given by any mode of electronic communication* • From the provider of the sensitive personal data • Regarding purpose of usage • Before collection of such information * The Department of Information Technology of the Ministry of Communications & Information Technology, Government of India, issued a press release on 24 August 2011 stating, among other things: *Further, in Rule 5(1) consent includes consent given by any mode of electronic communication.* **Notes:** • Hence, web-based consent or mobile-message-based consent could qualify as valid consent. • It is logical to assume that the consent should be available for retrieval as long as the SPDI is maintained. Care must be taken to retain such consent until all copies of the SPDI are destroyed or deleted.
	Checklist
	1. Have we obtained consent from the provider of personal data? (**Note:** It is a good practice to check if the provider of the personal information is a major, that is to say, at least 18 years of age, because consent obtained from a minor may not be adequate in law.) 2. Was the consent in writing (including any mode of electronic communication)? 3. Did we get consent before we collected the data? 4. Did the consent cover the proposed usage of the data? 5. Will such consent be retrievable when needed?

10. What is 'lawful purpose' for collection of sensitive personal data? (See Rule 5 [2] [a] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)	A lawful purpose is: • Connected with a function or activity of the body corporate or any person on its behalf • One for which the collection of the sensitive personal data or information is considered necessary for that purpose **Checklist** 1. Have we defined the purpose for collection of sensitive personal data? 2. Is such purpose connected with one or more of our functions or activities? **Note:** It is a good practice to check if the provider of the personal information is a major, that is to say, at least 18 years of age, because consent obtained from a minor may not be adequate in law.) 3. Are the data collected necessary for such function or activity? 4. Who (in the organisation) considered it necessary? Is the reasoning for such consideration duly documented?

11. How do we collect sensitive personal data? **(See Rule 5 [3] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of: • The fact that the information is being collected • The purpose for which the information is being collected • The intended recipients of the information • The name and address of: – The agency that is collecting the information – The agency that will retain the information
	Checklist
	1. Have we disclosed that we are collecting the data? 2. Have we disclosed the purpose for such collection? Is the purpose stated broad enough to cover potential future uses of the data? 3. Have we indicated who will be the recipients of the data? Is such indication broad enough to cover all contemplated future recipients? 4. Have we indicated the full name and address of the agency collecting the data and of the agency that will retain the information? 5. Have the appropriate management personnel determined the steps that are needed to ensure the aforesaid and whether such steps are reasonable in the circumstances? Have they documented their reasons for considering these steps reasonable and adequate? 6. Has a responsible officer of the body corporate "signed-off" to signify that the measures stated above have been undertaken?

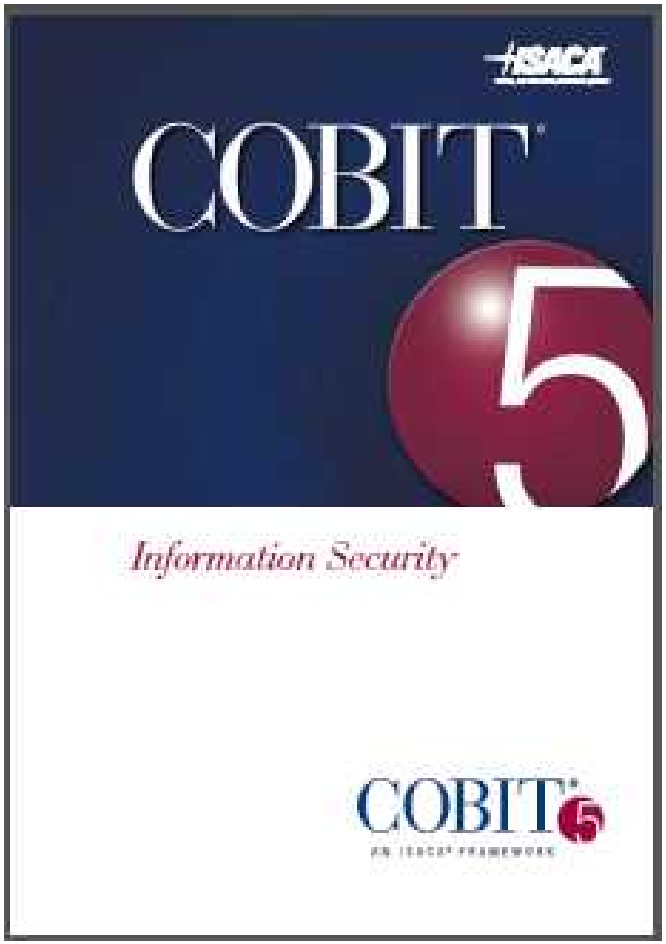
12. How do we address retention/use? (See Rule 5 [4] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)	The body corporate or any person on its behalf holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force. The information collected shall be used for the purpose for which it has been collected. **Checklist** 1. Do we have a retention policy for sensitive personal data? 2. Does that policy indicate how long we will retain such data or different types of such data? 3. Do we have a mechanism to determine whether such retention periods are no longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law that may apply? Who (in the organisation) decides this and how? Are the reasons for such retention periods documented? 4. Do we have mechanisms to ensure retention per such policy? 5. Do we have mechanisms for checking if the data are used only for the stated purposes? 6. Are these mechanisms tested and reviewed? 7. If the personal data resides on multiple computers and/or at multiple locations, have we taken care to ensure that the aforesaid is complied with in respect of all such computers?

13. What are the personal information provider's rights to review accuracy, etc., of his/her information with the body corporate? **(See Rule 5 [6] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	The body corporate or any person on its behalf shall: • Permit the providers of information to review the information they have provided as and when requested by them • Ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient is corrected or amended as feasible **Notes:** • The right to review extends not just to sensitive personal information **but to all personal information provided**. The provider can also seek corrections or amendments to address any inaccuracies or deficiencies, which could include, for example, spelling errors, wrong addresses and incomplete details. • Although the word "feasible" means "possible", "practical", "viable" or "reasonable", bodies corporate should consider whether they would be in a position to establish that any required amendments or corrections were not "feasible", in the event of a legal challenge or investigation. **Checklist** 1. Do we have a mechanism for personal information providers to seek review at any time of the information they have provided? 2. Does such mechanism provide ways in which to verify if the information is inaccurate or deficient (e.g., the information is different from that provided by the information provider or the information is not complete)? 3. Do we have a mechanism to organise corrections or amendments?

18. What are the non-disclosure duties? **(See Rule 6 [1] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	Disclosure of sensitive personal data or information by the body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. **Checklist** 1. Do we disclose sensitive personal data to third parties? 2. Are such third parties identified and listed? 3. Do we have the prior permission of the providers of the sensitive personal information for such disclosure? 4. Or, is there a contract with the provider of the sensitive personal information that allows such disclosure? 5. Or, is such disclosure necessary for compliance with a legal obligation? 6. Is there a mechanism to review requests for disclosure of sensitive personal information in compliance with a legal obligation (e.g., in 'returns' or forms filed with the state or central government)?

23. What constitutes compliance with requirements of reasonable security practices and procedures? **(See Rule 8 [1] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	A body corporate or a person on its behalf shall be considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies. **Note:** Refer to item 24 below for options of government approved standard. **Checklist** 1. Do we have in place appropriate information security policies? 2. Do such policies contain managerial, technical, operational and physical security control measures? 3. Are such measures commensurate with the information assets being protected and the nature of our business? 4. Do we have in place a comprehensive information security programme? 5. Is the information security programme well documented? 6. Do we consistently implement such security practices and standards? 7. Can we demonstrate, whenever called upon to do so by an agency mandated under the law, that we have implemented security control measures as per our documented information security programme and policies? (Such requests can be anticipated whenever there is an information security breach.)

24. What are the options of government-approved standards? **(See Rules 8 [2] and 8 [3] of the Information Technology [Reasonable Security Practices and Procedures and Sensitive Personal Data or Information] Rules, 2011.)**	The international standard ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements*[8] is one such standard referred to in sub-Rule (1). Any industry association or an entity formed by such an association, whose members are self-regulating by following other than ISO/IEC codes of best practices for data protection as per sub-Rule(1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation. **Checklist** 1. Have we adopted and implemented the international standard ISO/IEC 27001:2005, *Information technology—Security techniques—Information security management systems—Requirements* (Note: Annexure A.15 of ISO/IEC 27001:2005 deals with compliance with legal requirements. Item A.15.1.1.of the said annexure requires 'Identification of applicable legislation'. The control for this requires the following: 'All relevant statutory, regulatory and contractual requirements and the organisation's approach to meet these requirements shall be explicitly defined, documented, and kept up-to-date for each information system and the organisation'.) 2. Are we certified as having done so? 3. Is our certification valid and current? 4. Are any alternative standards as permitted under the IT Act and Rule 8 (2) available? 5. Have we evaluated such alternative standards?



You may use COBIT 5 for Information Security to integrate the information security practices within a comprehensive business framework to govern and manage enterprise IT

ISACA
Trust in, and value from, information systems

Thank you!

Avinash W. Kadam
awkadam@isaca.org

ISACA®
Trust in, and value from, information systems