Doc. No. : LITD 17 (12702)

IS/ISO/IEC 27035-2:2016

BUREAU OF INDIAN STANDARDS

DRAFT FOR COMMENTS ONLY

Draft Indian Standard

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY INCIDENT MANAGEMENT Part 2: GUIDELINES TO PLAN AND PREPARE FOR INCIDENT RESPONSE

ICS 35.040

Last date for receipt of comments is: 13 August 2018

Information Systems Security and Biometrics Sectional Committee, LITD 17

NATIONAL FOREWORD

(Formal clauses to be added later)

This Draft Indian Standard (Part 2) which is identical with ISO/IEC 27035-2:2016 'Information technology – Security techniques – Guidelines to Plan and Prepare for Incident Response' issued by International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) will be adopted by the Bureau of Indian Standards on the recommendations of the Information Systems Security and Biometrics Sectional Committee, and approval of the Electronics and Information Technology Division Council.

This standard was originally published in 2016 and was identical with ISO/IEC 27035:2011. ISO/IEC 27035 has been replaced by ISO/IEC 27035-1:2016 and ISO/IEC 27035-2:2016 accordingly IS/ISO/IEC 27035 is being replaced by IS/ISO/IEC 27035-1:2016 and IS/ISO/IEC 27035-2:2016

Other parts in this series are:

Part 1: Principles of Incident management

The text of ISO/IEC Standard may be approved as suitable for publication as an Indian Standard without deviations. Certain conventions are, however, not identical to those used in Indian Standards. Attention is particularly drawn to the following:

a) Wherever the words 'International Standard' appear referring to this standard, they should be read as 'Indian Standard'.

b) Comma (,) has been used as a decimal marker while in Indian Standards, the current practice is to use a point (.) as the decimal marker.

In this adopted standard, reference appears to certain International Standards for which Indian Standard also exist. For undated references, the latest edition of the referenced document applies, including any corrigenda and amendment .The corresponding Indian Standard which is to be substituted in its respective place is listed below along with its degree of equivalence for the edition indicated:

International Standard	*Corresponding Indian Standard*	*Degree of Equivalence*
ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary	IS/ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems – Overview and vocabulary(Under Print)	Identical with ISO/IEC 27000:2016
ISO/IEC 27035-1 Information technology — Security techniques — Information security incident management — Part 1: Principles of Incident management	Doc No LITD 17(12701) / ISO/IEC 27035-1:2016 Information technology — Security techniques — Information security incident management – Part 1: Principles of Incident management	Identical with ISO/IEC 27035-1:2016

For the purpose of deciding whether a particular requirement of this standard is complied with, the final value, observed or calculated, expressing the result of a test or analysis, shall be rounded off in accordance with IS 2 : 1960 'Rules for rounding off numerical values (revised)'. The number of significant places retained in the rounded off value should be the same as that of the specified value in this standard.

Scope of ISO/IEC 27035-2:2016 is as follows:

"This part of ISO/IEC 27035 provides the guidelines to plan and prepare for incident response. The guidelines are based on the "Plan and Prepare" phase and the "Lessons Learned" phase of the "Information security incident management phases" model presented in ISO/IEC 27035-1.

The major points within the "Plan and Prepare" phase include the following:

— information security incident management policy and commitment of top management;

— information security policies, including those relating to risk management, updated at both corporate level and system, service and network levels;

— information security incident management plan;

— incident response team (IRT) establishment;

— establish relationships and connections with internal and external organizations;

— technical and other support (including organizational and operational support);

— information security incident management awareness briefings and training;

— information security incident management plan testing.

The principles given in this part of ISO/IEC 27035 are generic and intended to be applicable to all organizations, regardless of type, size or nature. Organizations can adjust the guidance given in this part of ISO/IEC 27035 according to their type, size and nature of business in relation to the information security risk situation. This part of ISO/IEC 27035 is also applicable to external organizations providing information security incident management services.**"**

Note: The Technical content of this document has not been enclosed as these are identical with the corresponding ISO/IEC Standard. For details please refer ISO/IEC 27035-2:2016 or kindly contact.

Head
Electronics & IT Department
Bureau of Indian Standards 9,
B.S. Zafar Marg, New Delhi-110002
Email: hlitd@bis.gov.in
litd17@bis.gov.in
Telefax: 011-23608235