An Approach for the Assessment of the Information Security and Its Measures

Kiran Kumar Kommineni, Adimulam Yesu Babu

***Abstract*— The information security management standard requires enterprises to undertake regular reviews of the effectiveness of their information security management system. According to ISO, the effectiveness of the implemented information security controls to verify that the security requirements, according to the business objectives, have been met. This paper focuses on the identification of a set of assessment measures that could be used in assessing information security readiness according to the recommended security controls of the information security management standard. This paper presents the suitable security measures that could be used as an input to an analytical model for numerically assessing enterprise information security.**

***Index Terms*— Information Security; Risk management; Assessment; Measures; ISO.**

I. INTRODUCTION

There is an increasing demand for security risk assessments in which the span of assessment usually encompasses threats. Risk assessment is the core process of information security risk management. Organizations use risk assessment to determine the risks within an information system to reduce these risks. An information security measurement program provides enterprises with a number of organizational and financial benefits. Major benefits include increasing accountability for information security performance; improving effectiveness of information security activities; demonstrating compliance with laws, rules and regulations; and providing quantifiable inputs for resource allocation decisions. The ISO/IEC 27004 information security management measurement standard is the main requirement that contribute to the success of information security measurement program.

The knowledge acquisition continue with an in-depth text analysis of the ISO/IEC 27002 clauses, objectives and controls to identify the most suitable information security assessment measures associated with ISO security control. The process of choosing and refining the security measures of the ISO/IEC 27002 information security policy clause.

1.1 Security Policy Measures

The information security policy objective of ISO / IEC 27002 is stated as follows: “to provide management direction and support for information security in accordance with business requirements and relevant laws and regulations”. The required response, to this main objective, is expressed in terms of the following two controls.

These strategic objective and associated controls indicate that the information security policy of organizations.

- “An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties”.
- “The information security policy should be reviewed at planned intervals, or if significant changes occur, to ensure its continuing suitability, adequacy and effectiveness”.

II. LITERATURE REVIEW

To determine potential categories that would be useful in classifying the various types of measures. The literature was searched for documented manuals for information security controls and for investigating the common characteristics of these controls by many of the experts such as Chunlin Liu et al [1] presented a brief description of the approach taken by the author's organization based on a systematic computation of ratings. Serap Atay and Marcelo Masera [2] evaluated the current vulnerability, threat and risk analysis methods from the point of view of the new security requirements of NGNs. Rok Bojanc., Borka Jerman-Blažič [3] presented an approach enabling economic modeling of information security risk management and analyzes several approaches enabling assessment of the necessary investment in security technology from the economic point of view. Azzam Mourad et al [4] presented an aspect-oriented approach for the systematic security hardening of source code. Chi-Chun Lo., Wan-Jia Chen [5] proposed a hybrid procedure for evaluating risk levels of information security under various security controls. Sanjay Goel., InduShobha N. Chengalur-Smith [6] examined the policies and identifies three dimensions that could be used to characterize and evaluating the effectiveness of security policies. Daniel Mellado et al [7] presented a Common Criteria centred and reuse-based process that deals with security requirements at the early stages of software development in a systematic and intuitive way, by providing a security resources repository as well as integrating the Common Criteria into the software lifecycle. Shaun Posthumus., Rossouw von Solms [8] presented the importance of protecting an organization's vital business information assets by integrate information security into corporate governance through the development of an information security governance (ISG) framework. Michael Workman et al [9] investigated the technical side of this critical issue, but securing organizational systems has its grounding in personal behavior. Chung-Hung Tsai., Cheng-Wu Chen [10]

Manuscript received on March 2013

Mr. Kiran Kumar Kommineni, Lecturer, Department of Information Technology, Bapatla Engineering College, Bapatla - 522101, Guntur, AP, India.

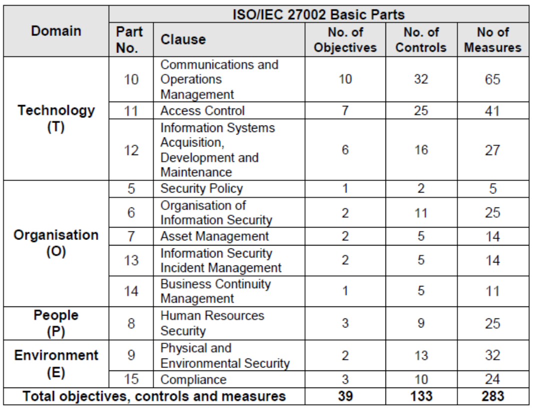
Dr. Adimulam Yesu Babu, I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru -534007, West Godavari (Dt), AP., India.

reported a mechanism for earthquake disaster risk assessment and management for the tourism industry, focusing on insurance and prevention. Xingzhi Wang et al [11] presented the problem of parallel dynamic security assessment applications from static homogeneous cluster environment to dynamic heterogeneous grid environment. Ray Bernard [12] described an information lifecycle security risk assessment and used to extend the reach of information security programs to encircle all forms of critical data from creation to destruction. Rogério de Paula et al [13] describe our explorations of everyday security practices in collaborative workgroups. Karin P. Badenhorst., Jan H.P. Eloff [14] proposed the Target Optimum Portfolio Management approach to information technology risk management.

III. ISO/IEC 27002 ASSESSMENT MEASURES

The main part of the standard, together with their objectives and security controls, are structured according to the TOPE domains and after several iterations of each step, based on the updated information. These are Technology Issues; Organisation Issues; People and Environment Issues. The purpose of using hybrid of knowledge acquisition methodologies was to ensure thorough coverage of the knowledge necessary to identify the information security measures. The details of the mapping process between the TOPE domains and the ISO/IEC 27002 standard is shown in Table 1.

Table 1: TOPE view of ISO/IEC 27002 main security clauses, objectives, controls and assessment measures



Domain	ISO/IEC 27002 Basic Parts				
	Part No.	Clause	No. of Objectives	No. of Controls	No of Measures
Technology (T)	10	Communications and Operations Management	10	32	65
	11	Access Control	7	25	41
	12	Information Systems Acquisition, Development and Maintenance	6	16	27
Organisation (O)	5	Security Policy	1	2	5
	6	Organisation of Information Security	2	11	25
	7	Asset Management	2	5	14
	13	Information Security Incident Management	2	5	14
	14	Business Continuity Management	1	5	11
People (P)	8	Human Resources Security	3	9	25
Environment (E)	9	Physical and Environmental Security	2	13	32
	15	Compliance	3	10	24
Total objectives, controls and measures			39	133	283

3.1 TECHNOLOGY ISSUES

Technology issues in the management of information security are the issues associated with the technology itself that enables ICT applications and services and with accessing and using the technology applications and services. Based on this, three parts of ISO/IEC 27002 would be associated with technology issues and shown in Table 1.

3.1.1 Communications and Operations Management

Communications and Operations Management is concerned with ten main technology issues: operational procedures, third party service delivery, system planning and acceptance, protection against malicious codes, software and information back-up, network security, media handling, exchange of information and software, e-commerce services and monitoring activities. These measures are derived from the "controls" of the standard, as shown above. It should be noted here that the protection measures introduced in the following tables are given in the same way.

3.1.2 Access Control

Access Control is concerned with seven main technology issues: access to business resources, user access management, user access responsibilities, network access, operating systems access, access to applications and information and access to mobile computing and tele-working.

3.1.3 Information Systems Acquisition, Development and Maintenance

Information Systems Acquisition, Development and Maintenance is concerned with six main technology issues: information systems security requirements, correct processing in applications, cryptographic controls, security of system files, security in development and support processes and technical vulnerability management.

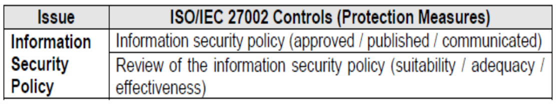
3.2 ORGANISATION ISSUES

The organisation issues are concerned with handling resources and managing events. ISO/IEC 27002 has five parts associated with these issues as shown in Table 1.

3.2.1 Information Security policy document

Information Security policy document has one main organisation issue: security policy. The protection measures associated with this issue are given in Table 2.

Table 2: Organisation: protection measures for "security policy"

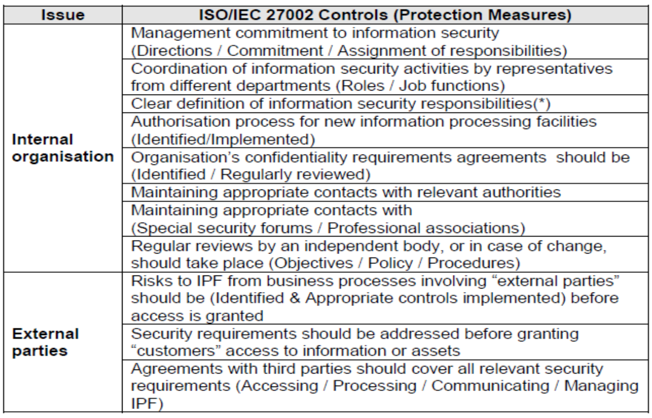


Issue	ISO/IEC 27002 Controls (Protection Measures)
Information Security Policy	Information security policy (approved / published / communicated)
	Review of the information security policy (suitability / adequacy / effectiveness)

3.2.2 Organisation of Information Security

Organisation of Information Security has two main organisation issues: internal organisation, i.e. within the enterprise concerned, and the enterprise concerned with external parties. The protection measures associated with these issues are given in Table 3.

Table 3: Organisation: Protection measures for "organisation of information security"

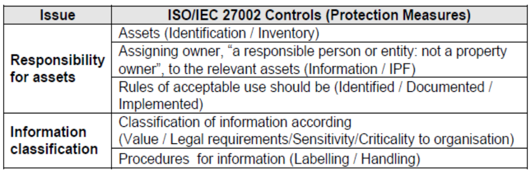


Issue	ISO/IEC 27002 Controls (Protection Measures)
Internal organisation	Management commitment to information security (Directions / Commitment / Assignment of responsibilities)
	Coordination of information security activities by representatives from different departments (Roles / Job functions)
	Clear definition of information security responsibilities(*)
	Authorisation process for new information processing facilities (Identified/Implemented)
	Organisation's confidentiality requirements agreements should be (Identified / Regularly reviewed)
	Maintaining appropriate contacts with relevant authorities
	Maintaining appropriate contacts with (Special security forums / Professional associations)
	Regular reviews by an independent body, or in case of change, should take place (Objectives / Policy / Procedures)
External parties	Risks to IPF from business processes involving "external parties" should be (Identified & Appropriate controls implemented) before access is granted
	Security requirements should be addressed before granting "customers" access to information or assets
	Agreements with third parties should cover all relevant security requirements (Accessing / Processing / Communicating / Managing IPF)

3.2.3 Asset Management

Asset Management has two main organisation issues: responsibility for organization's assets, and the classification of information. The protection measures associated with these issues are given in Table 4.

Table 4: Organisation: protection measures for "asset management"

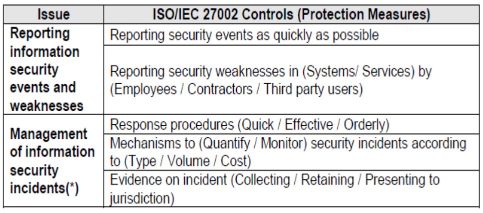


Issue	ISO/IEC 27002 Controls (Protection Measures)
Responsibility for assets	Assets (Identification / Inventory)
	Assigning owner, "a responsible person or entity: not a property owner", to the relevant assets (Information / IPF)
	Rules of acceptable use should be (Identified / Documented / Implemented)
Information classification	Classification of information according (Value / Legal requirements/Sensitivity/Criticality to organisation)
	Procedures for information (Labelling / Handling)

3.2.4 Information Security Incident Management

Information Security Incident Management has two main organisation issues: reporting information security events and weaknesses, and managing information security incidents. The protection measures associated with these issues are given in Table 5.

Table 5: Organisation: protection measures for "information security incident management"

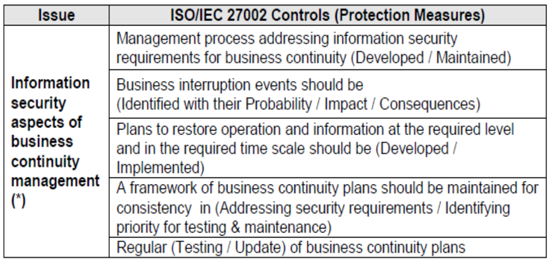


Issue	ISO/IEC 27002 Controls (Protection Measures)
Reporting information security events and weaknesses	Reporting security events as quickly as possible
	Reporting security weaknesses in (Systems/ Services) by (Employees / Contractors / Third party users)
Management of information security incidents(*)	Response procedures (Quick / Effective / Orderly)
	Mechanisms to (Quantify / Monitor) security incidents according to (Type / Volume / Cost)
	Evidence on incident (Collecting / Retaining / Presenting to jurisdiction)

3.2.5 Business Continuity Management

Business Continuity Management is concerned with the security aspects that enable managing interruption events and ensures keeping business continuity. The protection measures associated with these issues are given in Table 6.

Table 6: Organisation: protection measures for "business continuity management"

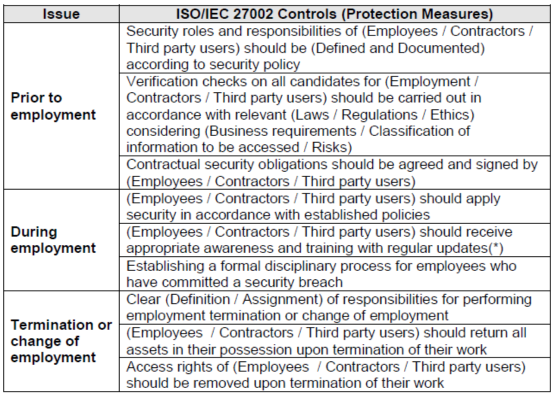


Issue	ISO/IEC 27002 Controls (Protection Measures)
Information security aspects of business continuity management (*)	Management process addressing information security requirements for business continuity (Developed / Maintained)
	Business interruption events should be (Identified with their Probability / Impact / Consequences)
	Plans to restore operation and information at the required level and in the required time scale should be (Developed / Implemented)
	A framework of business continuity plans should be maintained for consistency in (Addressing security requirements / Identifying priority for testing & maintenance)
	Regular (Testing / Update) of business continuity plans

3.3 PEOPLE ISSUES

Three types of issue are associated with people; they include: issues of concern prior to employment, issues of importance during employment and issues related to employment termination or change of employment. The protection measures associated with issues are given in Table 7.

Table 7: People: protection measures for "human resources security"

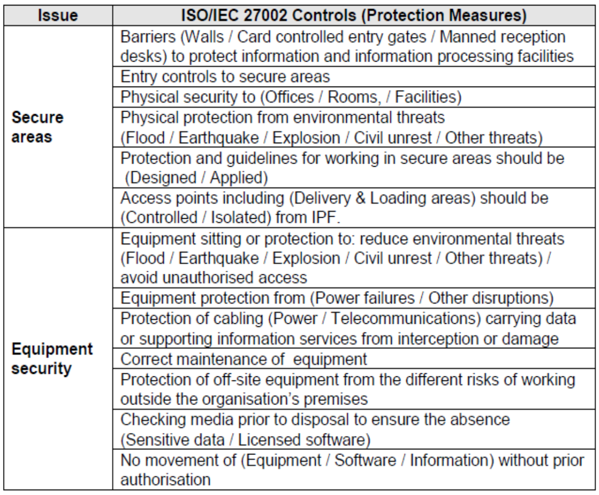


Issue	ISO/IEC 27002 Controls (Protection Measures)
Prior to employment	Security roles and responsibilities of (Employees / Contractors / Third party users) should be (Defined and Documented) according to security policy
	Verification checks on all candidates for (Employment / Contractors / Third party users) should be carried out in accordance with relevant (Laws / Regulations / Ethics) considering (Business requirements / Classification of information to be accessed / Risks)
	Contractual security obligations should be agreed and signed by (Employees / Contractors / Third party users)
During employment	(Employees / Contractors / Third party users) should apply security in accordance with established policies
	(Employees / Contractors / Third party users) should receive appropriate awareness and training with regular updates(*)
	Establishing a formal disciplinary process for employees who have committed a security breach
Termination or change of employment	Clear (Definition / Assignment) of responsibilities for performing employment termination or change of employment
	(Employees / Contractors / Third party users) should return all assets in their possession upon termination of their work
	Access rights of (Employees / Contractors / Third party users) should be removed upon termination of their work

3.4 ENVIRONMENT ISSUES

The environment issues are concerned with the physical environment on the one hand, and with professional environment on the other hand. ISO/IEC 27002 has two parts associated with these issues. This part has two main issues: an issue concerned with providing secure areas, and another concerned with equipment security. The protection measures associated with these issues are given in Table 8.

Table 8: Environment: protection measures for "physical and environmental security"



Issue	ISO/IEC 27002 Controls (Protection Measures)
Secure areas	Barriers (Walls / Card controlled entry gates / Manned reception desks) to protect information and information processing facilities
	Entry controls to secure areas
	Physical security to (Offices / Rooms, / Facilities)
	Physical protection from environmental threats (Flood / Earthquake / Explosion / Civil unrest / Other threats)
	Protection and guidelines for working in secure areas should be (Designed / Applied)
	Access points including (Delivery & Loading areas) should be (Controlled / Isolated) from IPF.
Equipment security	Equipment sitting or protection to: reduce environmental threats (Flood / Earthquake / Explosion / Civil unrest / Other threats) / avoid unauthorised access
	Equipment protection from (Power failures / Other disruptions)
	Protection of cabling (Power / Telecommunications) carrying data or supporting information services from interception or damage
	Correct maintenance of equipment
	Protection of off-site equipment from the different risks of working outside the organisation's premises
	Checking media prior to disposal to ensure the absence (Sensitive data / Licensed software)
	No movement of (Equipment / Software / Information) without prior authorisation

IV. INCREMENTAL ASSESSMENT APPROACH

Incremental approach for the assessment of enterprise information security is presented. The assessment approach is based on the TOPE scope, on one hand, and on the information security management recommendations of the ISO/IEC 27002 standard, on other hand. The proposed approach is of incremental nature, and has three levels of assessment, as shown in Figure 1, with increasing security controls. The first level considers the ISO/IEC 27002 19 essential and common security controls, as stated by the standard, which are refined into 45 measures. The second level is concerned with all the ISO/IEC 27002 133 base-line security controls, including those of level one, which are refined into 283 basic measures. The third level adds to the second level other security controls considered by other standards related to the ISO/IEC 27002, or required by various individual enterprises, depending on their business and information security strategies.

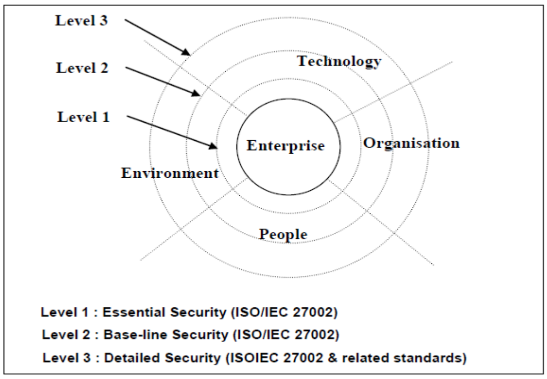

Level 3
Level 2
Level 1
Technology
Enterprise
Organisation
Environment
People
Level 1 : Essential Security (ISO/IEC 27002)
Level 2 : Base-line Security (ISO/IEC 27002)
Level 3 : Detailed Security (ISOIEC 27002 & related standards)

Figure 1: A TOPE scope for information security requirements

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

It provides an incremental approach for assessing and consequently applying information security according to three levels of increasing protection. It considers the refinement of each security control into a number of basic measures that ease both assessment and application of the ISO/IEC 27002 information security controls. The incremental method considered here has three levels of increasing information security protection.

4.1 Level 1: Essential and Common Security Measures

The first level is concerned with the essential and common ISO/IEC 27002 eight security objectives, and their associated 19 information security controls. This level represents the initial starting level that should enjoy priority in enterprises seeking information security protection. The controls of this level have been refined into 45 security protection measures that ease the assessment and support the application of this level.

4.2 Level 2: ISO/IEC 27002 Security Measures

The second level is associated with all ISO/IEC 27002 39 objectives and their associated 133 controls, including those of the first level. This level represents the internationally recommended base-line information security protection that should be followed by all enterprises. The controls of this level have been refined into 283 basic security protection measures.

4.3 Level 3: ISO Other Security Standards

The third level goes beyond the base-line security protection provided by ISO/IEC 27002. It considers the additional security controls of other ISO standards. This level may also consider other security controls related to various national standards, and it may also include the special information security protection requirements of individual enterprises, that related to their business objectives.

V.CONCLUSION

The work presented in this paper supports the future use of the ISO/IEC 27002 information security management standard in two main ways. On the one hand, it gives an integrated view of the standard, according to the TOPE domains, with illustrations of how to provide valid security measures for evaluating the effectiveness of applied information security management practices, according to the standard. On the other hand, it introduces an incremental approach for assessing and consequently managing information security inside enterprises according to three levels of increasing protection measures. The paper promotes the use of the ISO/IEC 27002 standard and helps enterprises to move gradually and in a well structured approach toward enhancing their information security according to the ISO international information security management standards.

REFERENCES

1. Chunlin Liu., Chong-Kuan Tan., Yea-Saen Fang., Tat-Seng Lok "The Security Risk Assessment Methodology" Procedia Engineering, Volume 43, 2012, pp 600–609.
2. Serap Atay & Marcelo Masera "Challenges for the security analysis of Next Generation Networks" Information Security Technical Report, Vol.16, Issue 1, 2011, pp 3–11
3. Rok Bojanc., Borka Jerman-Blažič "An economic modelling approach to information security risk management" International Journal of Information Management, Volume 28, Issue 5, October 2008, pp 413–422
4. Azzam Mourad., Marc-André Laverdière., Mourad Debbabi "An aspect-oriented approach for the systematic security hardening of code" Computers & Security, Volume 27, Issues 3–4, May–June 2008, pp 101–114
5. Chi-Chun Lo., Wan-Jia Chen "A hybrid information security risk assessment procedure considering interdependences between controls" Expert Systems with Applications, Volume 39, Issue 1, January 2012, pp 247–257
6. Sanjay Goel., InduShobha N. Chengalur-Smith "Metrics for characterizing the form of security policies" The Journal of Strategic Information Systems, Volume 19, Issue 4, December 2010, pp 281–295
7. Daniel Mellado., Eduardo Fernández-Medina., Mario Piattini "A common criteria based security requirements engineering process for the development of secure information systems" Computer Standards & Interfaces, Volume 29, Issue 2, February 2007, pp 244–253
8. Shaun Posthumus., Rossouw von Solms "A framework for the governance of information security" Computers & Security, Volume 23, Issue 8, December 2004, pp 638–646
9. Michael, W., William, H, B., Detmar Straub "Security lapses and the omission of information security measures: A threat control model and empirical test" Computers in Human Behavior, Volume 24, Issue 6, 17 Sept 2008, pp 2799–2816
10. Chung-Hung Tsai., Cheng-Wu Chen "An earthquake disaster management mechanism based on risk assessment information for the tourism industry-a case study from the island of Taiwan" Tourism Management, Volume 31, Issue 4, August 2010, pp 470–481
11. Xingzhi Wang., Zheng Yan., Li Li "A grid computing based approach for the power system dynamic security assessment" Computers & Electrical Engineering, Volume 36, Issue 3, May 2010, pp 553–564
12. Ray Bernard "Information Lifecycle Security Risk Assessment: A tool for closing security" Computers & Security, Volume 26, Issue 1, February 2007, pp 26–30
13. Rogério de Paula., Xianghua Ding., Paul Dourish., Kari Nies., Ben Pillet., Roberto Silva Filho "In the eye of the beholder: A visualization-based approach to information system security" International Journal of Human-Computer Studies, Volume 63, Issues 1–2, July 2005, pp 5–24
14. Karin P. Badenhorst., Jan H.P. Eloff "TOPM: a formal approach to the optimization of information technology risk management" Computers & Security, Volume 13, Issue 5, 1994, pp 411–435

AUTHORS PROFILE

Mr. Kiran Kumar Kommineni, Pursuing PhD in Computer Science & Engineering from CMJ University, Meghalaya. Received Master of Engineering in Computer Science & Engineering from RMK Engineering College, Chennai affiliated to Anna University. Working as a Lecturer in Information Technology Department of Bapatla Engineering College, Bapatla, Guntur (Dt), AP

Dr. Adimulam Yesu Babu, received Ph. D in Computer Science & Systems Engineering from Andhra University, Visakhapatnam. Dr. Babu having 23 years of Academic & Academic Administration experience and presently working as a I/c Principal and Professor in Computer Science & Engineering, Sir. CR Reddy College of Engineering, Eluru, West Godavari (Dt), AP.