Volume 4, No. 4, April 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
RESEARCH PAPER
Available Online at www.jgrcs.info

MAPPING OF DATA SECURITY COUNCIL OF INDIA SECURITY FRAMEWORK WITH ISO/IEC 27002:2005 AND COBIT 4.1

Watika Gupta, Sanchita Dwivedi* and Dr. Vijay Kumar Chaurasiya
MS-Cyber Law& Information Security Indian Institute of Information Technology Allahabad, India
ims2011012@iiita.ac.in, ims2011032@iiita.ac.in*, vijayk@iiita.ac.in

Abstract : The In today's scenario modern organizations are adopting various IT standards/ frameworks to nurture the growth of their companies in order to obtain customer satisfaction, revenue and business from customer, building of trust worldwide, maintaining IT operations consistent etc. IT security frameworks are essential to ensure improved efficiency and effectiveness of resources i.e. people, process and product. The different available IT frameworks like ISO, COBIT, COSO, ITIL etc. are in line. Organizations often find themselves in a state of turmoil, as they do not get the clear idea of what standards to be followed and what to leave behind. This paper aims at mapping of DSCI Security Framework with ISO/IEC 27002:2005 and COBIT 4.1 that will provide a picture that if the DSCI security framework is followed then what extent of other standards can be achieved, so that we need not to comply with the common provisions again and again. This helps to minimize the cost and save time instead of following multiple standards.

Keywords – COBIT 4.1, Compliance, DSCI Security Framework, Frameworks, ISO/IEC27002:2005, Information Security, Information Technology, Mapping

INTRODUCTION

The necessity of an IT framework is that IT infrastructure is complex and diverged and the implementation of standards ensures the effectiveness and reliability of the IT security measures in an organization. This helps to achieve stakeholder's confidence, building of trust, direction and control of enterprises and other service industries in this domain. ISO/IEC 27002:2005 and COBIT provide regulatory compliance. These two standards play a major role for serving the purpose of information security. But there is no structured standard or framework available in India within the aspect of security of information asset. So Data Security Council of India (DSCI) Security Framework approaches best practices which deal with privacy issues, information security standards and strategy for the security discipline in order to address IT governance. This framework is suitable enough to implement irrespective of any kind of organization like telecom sector, banking institutions, government bodies, private organizations, BPO and other service industries.

OBJECTIVE

The objective of this paper is to align DSCI security framework with the other compliance standards i.e. ISO/IEC 27002:2005 and COBIT 4.1. This gives an overview of DSCI framework that what are the provisions it comprises of and a statistical image of gap analysis to understand the provisions it lacks when compared with the other two standards. The mapping considers the discrete areas of ISO/IEC 27002:2005 and control objectives of COBIT 4.1 to map with the disciplines of Data Security Council of India Security Framework. The approach of mapping and gap analysis is a guidance material.

STANDARDS

ISO/IEC 27002:2005- Code of Practice for Information Security Management:

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provide best practices for information security management system. In the series of ISO 27000, the ISO 27001 standard is the rename of ISO BS7799, which provides the specification for information security management system consist of PDCA lifecycle i.e. Plan-Do-Check-Act. The ISO 27002 was previously known as ISO 17799. It provides a code of practice for information security. The standard establishes guidelines and general principles to plan, implement and operate, monitor and review, maintain and improve the information security management within an organization. It helps to achieve confidentiality, integrity and availability of an organization's sensitive information. It has 11 information security domains, 39 control objectives and 133 controls.

Control Objectives for Business and Information & Related Technologies (COBIT) 4.1:

The Control Objectives for Information and related Technology (COBIT) is a globally accepted framework based on industry standards and best practices. The main objective of COBIT is to align IT with the business goals so that benefits are maximized, IT resources are used efficiently and IT risks are managed appropriately. In this way it provides that IT is aligned effectively and efficiently with the business goals and provide a better direction to the way of IT for business growth. Implementation of COBIT 4.1 ensures IT governance and compliance processes for the IT industries. COBIT 4.1 has 4 domains which contains 34 processes. These four domains are plan and organize, acquire and implement, deliver and support, monitor and evaluate. It also provides control objectives, goals and metrics, RACI chart and maturity model for each of the processes. COBIT is a set of proven and internationally

accepted tool and techniques. Implementation of COBIT is a sign of a well-run organization. Also it maps 100% to COSO.

Data Security Council of India (DSCI) Security Framework (DSF):

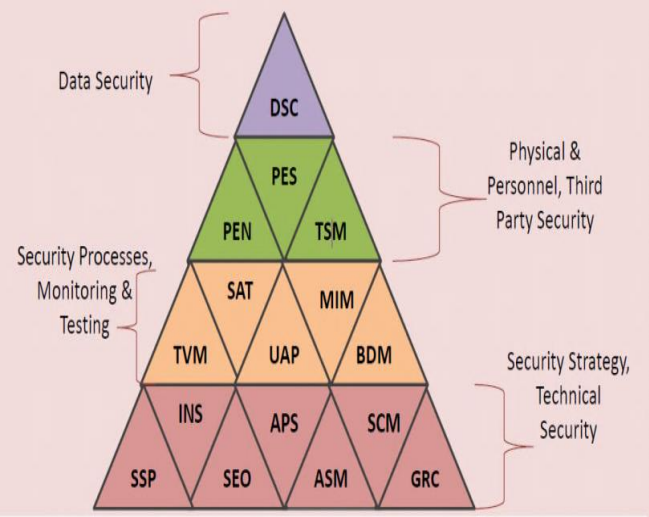


Figure. 1 DSCI Security Framework

Data Security Council of India (DSCI) Security framework was developed by Data Security Council of India. DSCI is a centralized body on data protection in India. It is an independent Self-Regulatory Organization (SRO) by NASSCOM®. It promotes protection of data, develop best practices & standards to provide security and privacy in order to encourage the Indian industries to implement the same. DSCI promotes best practices for Indian IT/BPO industry, banking, telecom sectors, industry associations, data protection authorities. DSCI Security Framework (DSF©) comprises of 16 disciplines that have been aligned to the following 4 layers -Security Strategy & Technical Security; Security Processes, Monitoring & Testing; Physical, Personnel & Third Party security; and Data Security. This gives an outlook to the security initiatives by following a layered approach and focusing on each disciplines of security. These disciplines consist of areas such as infrastructure security, application security, user access management security, business continuity and disaster management, monitoring and incident management which are stringent and rigorous to maintain IT security. From time to time new approaches, technical elucidations and services have evolved that are suitable and precise to these disciplines.[4]

MAPPING OF STANDARDS

There are various compliance frameworks available for IT governance on global scale. The different components of IT governance are strategy, infrastructure, operation, risk and compliance, resource optimization, business continuity etc. The Data Security Council of India (DSCI) also rejuvenates its efforts on the similar components. There is a mapping that shows how DSCI Security Framework is able to achieve the same as of ISO/IEC and COBIT in order to maintain IT governance in any organization. The following analysis has been maintained within 4 layer of context. These layers are- Security Strategy, Technical Security, Security Processes, Monitoring & Testing, Physical & Personnel, Third Party Security & Data Security. Further for the purpose of mapping the key feature shows the basis on which the all three frameworks are compared and mapped.

Security Strategy, Technical Security:

The context of Security strategy and technical security deals with the alignment of IT strategy and policy with business objectives that brings structured approach to provide effective protection to the information asset. After making a strategy, there needs an implementation of the same by assigning responsibility to the management and staff of the organization. The organization is assigned with the set of roles and responsibilities in a hierarchical manner, on which effectiveness of work done is highly depends. The next step is asset management where the asset is classified on the basis of its sensitivity level. This also includes labelling, integration, updating, acceptable use of asset, accountability, licensing, warranty and maintenance support. The concept of Governance risk and compliance is an integrated and holistic approach that ensures that the organization complies with the regulatory requirements and risks are diligently managed. Infrastructure security addresses security threats at network layer. Then application infrastructure ensures security of data and privacy of personal information. Secure content management deals with legitimate network traffic, exchange of information and execution of a transaction.

Table 1

KEY	DSF[4]	ISO/IEC 27002:2005 [1]	COBIT-Control Objective[2]
Security Policy	**SSP-** Security Strategy & Policy	**5.1.1** Information security policy document **5.1.2** Review of information security policy	**PO1.4** IT Strategic Plan **PO1.5** IT Tactical Plans **PO2.1** Enterprise Information Architecture Model **PO3.1** Technological direction planning **PO3.2** Technology Infrastructure Plan **PO4.2** Strategy Committee **PO5.3** Information Technology budgeting **PO5.4** Cost management **PO6.1** Information Technology policy and control environment **PO6.2** Enterprise Information Technology risk and control framework **PO6.3** IT policies Management **PO6.5** Communication of IT objectives and direction **PO9.4** Risk assessment **DS5.2** Information Technology security plan **DS5.3** Identity management **ME2.1** Monitoring of internal control framework

			ME2.2 Supervisory review **ME2.5** Assurance of internal control **ME2.7** Remedial actions **ME4.7** Independent assurance
Organization **Hhhh**	**SEO**– Security Organization	**6.1.1** Management commitment to information security **6.1.2** Information security co-ordination **6.1.3** Allocation of information security responsibilities **6.1.4** Authorization process for information processing facilities **6.1.5** Confidentiality agreements **6.1.6** Contact with authorities **6.1.7** Contact with special interest groups **6.1.8** Independent review of information security **6.2.1** Identification of risks related to external parties **6.2.2** Addressing security when dealing with customers **6.2.3** Addressing security in third-party agreements	**PO3.3** Monitor future trends and regulations **PO3.5** Information Technology architecture board **PO4.3** Information Technology steering committee **PO4.4** Organisational placement of Information Technology function **PO4.5** IT Organisational Structure **PO4.6** Establishment of roles and responsibilities **PO4.8** Responsibility for risk, security, compliance **PO4.9** Data and system ownership **PO4.10** Supervision **PO4.14** Contracted staff policies and procedures **PO4.15** Relationships **DS5.4** User account management **PO6.2** Enterprise IT risk and control framework **PO6.3** IT policies management **PO6.4** Policy, standard and procedures rollout **PO6.5** Communication of Information Technology objectives and direction **PO8.3** Development and acquisition standards **AI1.4** Requirements and feasibility decision and approval **AI2.4** Application security and availability **AI5.1** Procurement control **AI5.2** Supplier contract management **AI7.6** Testing of changes **DS2.1** Identification of all supplier relationship **DS2.2** Supplier relationship management **DS2.3** Supplier risk Management **DS2.4** Supplier performance monitoring **DS4.1** Information Technology continuity framework **DS4.2** Information Technology continuity plans **DS5.1** Management of IT Security **DS5.2** Information Technology security plan **DS5.3** Identity management **DS5.4** User account management **DS5.7** Protection of security Technology **DS5.9** Malicious software prevention detection and correction **DS5.11** Exchange of sensitive data **DS12.3** Physical access **ME3.1** Identification of external legal, regulatory, and contractual compliance requirements **ME2.6** Internal control at third parties **ME3.3** Evaluation of compliance with external requirements **ME3.4** Positive assurance of compliance
Asset Management	**ASM**– Asset Management	**7.1.1** Inventory of assets **7.1.2** Ownership of assets **7.1.3** Acceptable use of assets **7.2.1** Classification guidelines **7.2.2** Information labeling and handling	**PO2.2** Enterprise data dictionary and data syntax rules **PO2.3** Data classification scheme **PO4.9** Data and system Ownership **PO4.10** Supervision **PO6.2** Enterprise IT risk & control framework **AI2.4** Application security and availability **AI5.3** Supplier Selection **DS9.1** Configuration repository and baseline **DS9.2** Identification and maintenance of configuration items **DS9.3** Configuration integrity review
Application of GRC	**GRC**– Governance, Risk & Compliance	**4.1** Assessing security risks **4.2** Treating security risks **10.1.2** Change management **15.1.1** Identification of applicable legislation **15.1.2** Intellectual property rights (IPR) **15.1.4** Data protection and privacy of personal information **15.1.6** Regulation of cryptographic controls **15.2.1** Compliance with security policies and Standards **15.2.2** Technical compliance checking	**PO4.8** Responsibility for risk, security and compliance **PO6.2** Enterprise IT risk & control framework **PO9.4** Risk assessment **PO9.5** Risk Response **PO9.6** Maintenance and Monitoring of a Risk Action Plan **AI6.1** Change standards and procedures **AI6.2** Impact assessment, prioritisation and authorisation **AI6.3** Emergency changes **AI6.4** Change status tracking and reporting **AI6.5** Change closure and documentation **DS5.8** Cryptographic key Management **ME1.5** Board and Executive Reporting **ME2.1** Monitoring of internal ctrl. framework **ME2.2** Supervisory review **ME2.3** Control exceptions **ME2.4** Control self-assessment **ME2.5** Assurance of internal control **ME2.6** Internal control at third parties **ME2.7** Remedial actions **ME3.1** Identification of external legal, regulatory and contractual compliance requirements

			ME4.1 Establishment of an IT Governance Framework **ME4.2** Strategic Alignment **ME4.3** Value Delivery **ME4.4** Resource Management **ME4.6** Performance Measurement
Technology Infrastructure	**INS**– Infrastructure Security	**9.1.5** Working in secure areas **9.2.4** Equipment maintenance **10.1.4** Separation of development, test and operational facilities **10.4.1** Controls against malicious code **10.4.2** Controls against mobile code **12.1.1** Security requirements analysis and specification **12.4.1** Control of operational software **12.4.2** Protection of system test data **12.5.2** Technical review of applications after operating system changes **12.6.1** Control of technical vulnerabilities	**AI3.1** Technological infrastructure acquisition plan **AI3.2** Infrastructure resource protection and availability **AI3.3** Infrastructure maintenance **AI3.4** Feasibility test environment **DS13.3** IT Infrastructure Monitoring
Application Infrastructure	**APS –** Application Security	**6.1.4** Authorisation process for information processing facilities **6.1.5** Confidentiality agreements **6.2.3** Addressing security in third-party agreements **7.2.1** Classification guidelines **8.2.2** Information security awareness, education and training **10.1.1** Documented operating procedures **10.3.2** System acceptance **11.6.2** Sensitive system isolation **12.1.1** Security requirements analysis and specification **12.2.1** Input data validation **12.2.2** Control of internal processing **12.2.3** Message integrity **12.2.4** Output data validation **12.3.1** Policy on the use of cryptographic controls **12.3.2** Key management **12.4.3** Access control to program source code **12.5.1** Change control procedures **12.5.2** Technical review of applications after operating system changes **12.5.3** Restrictions on changes to software packages **12.5.4** Information leakage **12.5.5** Outsourced software development **15.3.2** Protection of IS audit tools	**PO1.6** IT Portfolio Management **PO8.2** IT standards and quality practices **PO8.3** Development and acquisition standards **AI2.4** Application security and Availability **AI7.1** Training **AI7.2** Test plan **AI7.3** Implementation plan **AI7.6** Testing of changes **DS5.8** Cryptographic Key Management **DS4.9** Offsite Backup Storage **DS11.5** Backup and Restoration **DS11.6** Security Requirements for Data Management
Network Control	**SCM**– Security Content Management	**10.8.3** Physical media in transit **10.8.4** Electronic messaging **10.9.3** Publicly available information **11.4.1** Policy on use of network services **11.4.2** User authentication for external connections **11.4.3** Equipment identification in networks **11.4.4** Remote diagnostic and configuration port protection **11.4.5** Segregation in Networks **11.4.6** Network connection Control **11.4.7** Network routing control	**PO3.2** Technology Infrastructure Plan **DS5.7** Protection of security technology **DS5.9** Malicious software prevention, detection and correction **DS5.11** Exchange of sensitive data **DS9.2** Identification and maintenance of configuration items

Security Processes, Monitoring & Testing:

In the context of security processes, monitoring and testing new threats and vulnerabilities are identified analysed and managed. User access & privilege management provides access control mechanism for the authorized users in order to access information regarding network, server systems, databases, and applications etc. Thereafter to ensure and maintain the continuous operation of the business, business continuity and disaster recovery management is required to protect and create back up for critical information. Security test and audit is required against threats and malicious behaviour that ensures design implementation and compliance requirement. Threats can be treated only when they are recognized to the organization, so if any new incident occur; it should be duly reported, communicated and monitored which is done under incident reporting mechanism.

Table 2

KEY	DSF[4]	ISO/IEC 27002:2005 [1]	COBIT-Control Objective[2]
Risk Management	**TVM**– Threat & Vulnerability Management	**4.1** Assessing security Risks **4.2** Treating Security Risks **10.3.1** Capacity management	**PO9.1** Information Technology Risk Management Framework **PO9.2** Establishment of Risk Context **PO9.3** Event Identification **PO9.4** Risk Assessment **PO9.5** Risk response **PO9.6** Maintenance & monitoring of risk action plan **AI2.5** Configuration and Implementation of Acquired Application Software

			AI2.6 Major Upgrades to Existing Systems **AI2.8** Software Quality Assurance **AI2.9** Applications Requirements Management **AI2.10** Application Software Maintenance **AI4.2** Knowledge Transfer to Business Mgmt. **AI4.3** Knowledge Transfer to End Users **AI7.7** Final Acceptance Test **AI7.9** Post-implementation Review **ME1.4** Performance Assessment **ME4.5** Risk Management
Access Control	**UAP**–User, Access & Privilege Management	**10.1.3** Segregation of duties **10.6.1** Network controls **10.6.2** Security of network services **11.1.1** Access control policy **11.2.1** User registration **11.2.2** Privilege management **11.2.3** User password Management **11.2.4** Review of user access Rights **11.3.1** Password use **11.3.2** Unattended user Equipment **11.3.3** Clear-desk and clear-screen Policy **11.4.1** Policy on use of network services **11.4.2** User authentication for external connections **11.4.4** Remote diagnostic & configuration port protection **11.4.5** Segregation in Networks **11.4.6** Network connection Control **11.4.7** Network routing control **11.5.1** Secure logon Procedures **11.5.2** User identification and Authentication **11.5.3** Password management System **11.5.4** Use of system utilities **11.5.5** Session time-out **11.5.6** Limitation of connection time **11.6.1** Information access Registration **11.6.2** Sensitive system Isolation **11.7.1** Mobile computing and Communication **11.7.2** Teleworking	**PO2.2** Enterprise data dictionary and data syntax rules **PO2.3** Data classification Scheme **PO3.4** Technology standards **PO4.11** Segregation of Duties **PO4.12** Information Technology Staffing **PO4.13** Key Information Technology Personnel **PO6.2** Enterprise Information Technology risk and control framework **AI1.2** Risk analysis report **AI2.4** Application security and availability **AI6.3** Emergency changes **DS5.2** Information Technology security plan **DS5.3** Identity management **DS5.4** User account Management **DS5.7** Protection of security Technology **DS5.9** Malicious software prevention detection and correction **DS5.10** Network security **DS5.11** Exchange of sensitive data **DS7.3** Evaluation of Training Received **DS9.2** Identification and maintenance of configuration items **DS13.1** Operations Procedures and Instructions **DS13.2** Job Scheduling
BCP & DRP	**BDM** – Business Continuity & Disaster Management	**10.5.1** Information back-up **14.1.1** Information Security in the BCP management process **14.1.2** Business continuity and risk assessment **14.1.3** Developing and implementing continuity plans including Information Security **14.1.4** BCP framework **14.1.5** Testing, maintaining and reassessing BCP	**PO1.2** Business- Information Technology Alignment **PO1.3** Assessment of Current Capability and Performance **PO3.1** Technological direction planning **PO9.1** Information Technology risk management framework **PO9.2** Establishment of risk Context **PO9.4** Risk assessment **PO10.2** Project Management Framework **PO10.3** Project Management Approach **PO10.5** Project Scope Statement **PO10.8** Project Resources **PO10.9** Project Risk Management **DS3.1** Performance and Capacity Planning **DS3.2** Current Performance and Capacity **DS3.3** Future Performance and Capacity **DS4.1** Information Technology continuity Framework **DS4.2** Information Technology continuity plans **DS4.3** Critical Information Technology resources **DS4.4** Maintenance of the Information Technology continuity plan **DS4.5** Testing of the Information Technology continuity plan **DS4.6** Information Technology continuity plan training **DS4.7** Distribution of the Information Technology continuity plan **DS4.8** Information Technology services recovery and resumption **DS4.10** Post-resumption Review **DS8.1** Service desk **DS8.3** Incident escalation **ME1.6** Remedial Actions
Audit	**SAT**– Security Audit & Testing	**15.3.1** Information Security audit controls **15.3.2** Protection of Information Security audit tools	**PO2.4** Integrity Management **AI2.3** Application control and auditability **AI2.4** Application security and availability **AI4.1** Planning for Operational Solutions **DS5.5** Security testing, surveillance and monitoring **DS5.7** Protection of security technology **ME2.5** Assurance of internal Control
Monitoring	**MIM**– Monitoring & Incident Management	**10.10.1** Audit logging **10.10.2** Monitoring systems Use **10.10.3** Protection of log Information **10.10.4** Administrator and operator logs **10.10.5** Fault logging **10.10.6** Clock synchronisation **13.1.1** Reporting IS events **13.1.2** Reporting IS Weaknesses **13.2.1** Responsibilities and Procedures **13.2.2** Learning from IS Incidents	**PO5.4** Cost management **PO6.1** Information Technology policy and control environment **PO8.6** Quality Measurement, Monitoring and Review **PO9.3** Event identification **AI2.3** Application control and auditability **AI4.4** Knowledge transfer to operations and support staff **AI5.4** Information Technology Resources Acquisition **DS3.4** Information Technology Resources Availability **DS3.5** Monitoring and Reporting **DS5.5** Security testing, surveillance and monitoring

		13.2.3 Collection of evidence	**DS5.6** Security incident definition **DS5.7** Protection of security Technology **DS8.2** Registration of customer queries **DS8.3** Incident escalation **DS8.4** Incident closure **DS8.5** Reporting and trend analysis **DS10.1** Identification and classification of problems **DS10.2** Problem tracking and resolution **DS10.4** Integration of Configuration, Incident and Problem Management **ME1.1** Monitoring Approach **ME1.3** Monitoring Method **ME1.2** Definition and collection of monitoring data **ME2.2** Supervisory review **ME2.5** Assurance of internal control **ME4.7** Independent Assurance

Physical & Personnel, Third Party Security:

In the context of Physical & Personnel, Third Party Security the criticality of the business is addressed by physical and environmental security. For this purpose a significant level of centralized visibility to maintain the physical security initiatives, activities, functions, solutions, processes, adequacy of measures deployed for environment security, their current state against geographical and local conditions and historical incidents pertaining to environmental measures. In order to manage effective and efficient services to the third party contractual agreement, compliance requirement should be satisfied. Such services may relate with customer data, employee information, health and financial data, intellectual property etc. Internal security threat is addressed by personnel security as the human involvement is the greater source of risk. Employees have access to the sensitive personal data of customers and others that is why their screening, training, monitoring and confidentiality agreement are necessary.

Table 3

KEY	**DSF[4]**	**ISO/IEC 27002:2005 [1]**	**COBIT-Control Objective[2]**
Physical Environment	**PEN–** Physical & Environmental Security	**9.1.1** Physical security Perimeter **9.1.2** Physical entry controls **9.1.3** Security offices, rooms and facilities **9.1.4** Protecting against external & environmental threats **9.1.5** Working in secure areas **9.1.6** Public access, delivery and loading areas **9.2.1** Equipment sitting and Protection **9.2.2** Supporting utilities **9.2.3** Cabling security **9.2.4** Equipment maintenance **9.2.5** Security of equipment off premises **9.2.6** Secure disposal or reuse of equipment **9.2.7** Removal of property	**PO4.9** Data and system ownership **PO4.14** Contracted staff policy and Procedure **PO6.2** Enterprise IT risk and cntrl framework **AI3.3** Infrastructure Maintenance **AI7.4** Test Environment **DS5.7** Protection of security Technology **DS11.4** Disposal **DS12.1** Site selection and layout **DS12.2** Physical security Measures **DS12.3** Physical access **DS12.4** Protection against environmental factors **DS12.5** Physical facilities Management **DS13.5** Preventive maintenance for hardware
Third Party Services	**TSM–** Third Party Security Management	**10.2.1** Service delivery **10.2.2** Monitoring and review of third-party services **10.2.3** Managing changes to third-party services	**DS1.1** Service level management Framework **DS1.2** Definition of services **DS1.3** Service level Agreements **DS1.5** Monitoring and reporting of service level achievements **DS2.2** Supplier relationship management **DS2.3** Supplier risk management **DS2.4** Supplier performance Monitoring **ME2.6** Internal control at third parties **ME3.2** Optimisation of Response to External Requirements
Human Resources	**PES–** Personnel Security	**8.1.1** Roles and Responsibilities **8.1.2** Screening **8.1.3** Terms and conditions of Employment **8.2.1** Management Responsibilities **8.2.2** Information security awareness, education, and training **8.2.3** Disciplinary process **8.3.1** Termination Responsibilities **8.3.2** Return of assets **8.3.3** Removal of access rights **10.1.3** Segregation of duties **10.6.1** Network controls	**PO4.6** Establishment of role and Responsibility **PO4.8** Responsibility for risk, security and compliance **PO4.10** Supervision **PO 4.11** Segregation of Duties **PO6.2** Enterprise Information Technology risk and control framework **PO6.3** Information Technology policies Management **PO6.4** Policy, standard and procedures rollout **PO7.1** Personnel recruitment and retention **PO7.2** Personnel competencies **PO7.3** Staffing of roles **PO7.4** Personnel training **PO7.5** Dependence Upon Individuals **PO7.6** Personnel clearance Procedures **PO7.7** Employee job performance evaluation **PO7.8** Job change and termination **AI1.1** Definition and maintenance of business functional and technical requirements **AI7.1** Training **DS2.3** Supplier risk Management

			DS5.1 Management of Information Technology security **DS5.2** Information Technology security plan **DS5.3** Identity management **DS5.4** User account Management **DS5.6** Security incident definition **DS7.1** Identification of education and training needs **DS7.2** Delivery of training and education

Data Security:

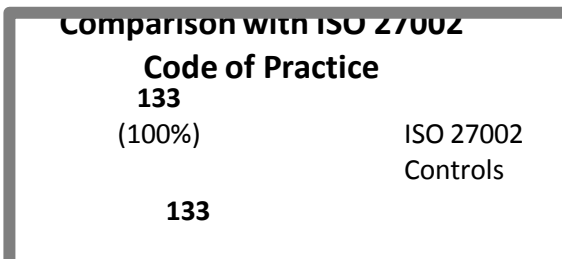
Data security is the key concern for any organization. When we talk about the domain of information technology, then information asset becomes the most critical factor to protect. Each data item produces some business value. Sometimes it may carry high risk which may damage an organization's reputation. Also privacy issue is the major concern for the end users. They need assurance that their information and data is kept safe when it is collected and processed by the organization.

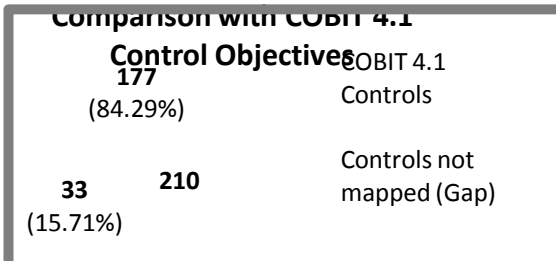
Table 4

KEY	DSF[4]	ISO/IEC 27002:2005 [1]	COBIT-Control Objective[2]
Security of Data	**DSC**–Data Security	**7.1.1** Inventory of assets **7.2.1** Classification guidelines **10.7.1** Management of removable data **10.7.2** Disposal of media **10.7.3** Information handling procedures **10.7.4** Security of system documentation **10.8.1** Information exchange policies and procedures **10.8.2** Exchange agreements **10.8.5** Business information system **11.1.1** Access control policy **15.1.3** Protection of organizational records **15.1.4** Data protection and privacy of personal information **15.1.5** Prevention of misuse of information processing facilities	**PO2.2** Enterprise data dictionary and data syntax rules **PO2.3** Data classification Scheme **PO3.4** Technology standards **PO6.2** Enterprise Information Technology risk and control framework **AI2.4** Application security and availability **AI5.2** Supplier contract management **DS2.3** Supplier risk Management **DS5.2** Information Technology security plan **DS5.3** Identity management **DS5.4** User account management **DS9.2** Identification and maintenance of configuration items **DS9.3** Configuration integrity review **DS11.1** Business requirements for data mgmt. **DS11.2** Storage and retention arrangements **DS11.3** Media library management system **DS11.4** Disposal

GAP ANALYSIS

ISO 27002 (code of practice) has 133 controls and COBIT 4.1 provides 210 controls while DSCI framework provides its own strategy and best practices within 16 disciplines. After analyzing both of the frameworks with DSCI security framework, we find that most of the provisions of it are similar to the ISO/ IEC 27002:2005 – Code of Practice and COBIT – Control Objectives. But still there are certain provisions which are not mapped with the DSF. The following gap analysis and statistical image shows the gap between them.





Here both the frameworks are compared with the DSCI Security framework separately. Hence, on the basis of above analysis we can say that the DSF 100% maps to ISO 27002. But if we compare DSF with the COBIT 4.1 framework it was found that out of 210 controls of COBIT 4.1, only 177 controls were mapped. Remaining there are 33 controls of COBIT 4.1 which do not map with DSF. These controls are-

Plan & Organize	Acquire & Implement
PO1.1 IT Value Management **PO4.1** IT Process Framework **PO4.7** Responsibility for IT Quality Assurance **PO5.1** Financial Management Framework **PO5.2** Prioritisation Within IT Budget **PO5.5** Benefit Management **PO8.1** Quality Management System **PO8.4** Customer Focus **PO8.5** Continuous Improvement	**AI1.3** Feasibility Study and Formulation of Alternative Courses of Action **AI2.1** High-level Design **AI2.2** Detailed Design **AI2.7** Development of Application Software **AI7.5** System and Data Conversion **AI7.8** Promotion to Production
	Deliver & Support

PO10.1 Programme Management Framework **PO10.4** Stakeholder Commitment **PO10.6** Project Phase Initiation **PO10.7** Integrated Project Plan **PO10.10** Project Quality Plan **PO10.11** Project Change Control **PO10.12** Project Planning Assurance of Method **PO10.13** Project Performance Measurement, Reporting, Monitoring **PO10.14** Project Closure	**DS1.4** Operating Level Agreements **DS1.6** Review of Service Level Agreements and Contracts **DS6.1** Definition of Services **DS6.2** IT Accounting **DS6.3** Cost Modelling and Charging **DS6.4** Cost Model Maintenance **DS10.3** Problem Closure **DS13.4** Sensitive Documents and Output Devices
	Monitor & Evaluate
	ME3.5 Integrated Reporting

CONCLUSION

After the above analysis it is proved that how much the DSCI Security Framework deviates from the other two standards respectively. The ISO framework 100% maps with the DSF and 84.29% of the COBIT framework are mapped with the DSF. Although the framework is not exhaustive yet the other strategies, best practices can be included by adding additional controls in order to enhance the scope of DSCI Security Framework. Once the scope is enhanced, then we do not need to comply with ISO/IEC 27002:2005 and COBIT 4.1 at the same time. Moreover, following a single framework will be enough for compliance that can minimize the cost and save the time. Besides, DSF is more structured than ISO and COBIT because it follows a layered approach. In order to attain data security layer – first the security strategy, technical security layer, security processes should be managed then monitoring & testing layer should be processed and physical & personnel thereafter third party security layer should be satisfied. So in this way moving one by one step upwards, data security can be achieved appropriately. This shows that the Data Security Council of India (DSCI) Security Framework is also capable enough to provide IT governance, similar to the ISO 27002 and COBIT 4.1 framework.

REFERENCES

[1] Information Systems Audit and Control Association (ISACA) "Text of ISO/IEC FDIS 17799: 2005-02-11 — Information techniques— Security techniques — Code of practice for information security management (2nd edition)", in 2005, February 11

[2] Information Systems Audit and Control Association (ISACA) "Control Objective for Information and Related Technology (COBIT) 4.1" for IT Governance and IT Management, in 2007

[3] Information System Audit & Control Association (ISACA) "Aligning CobiT®4.1, ITIL® V3 & ISO/IEC 27002 for Business Benefit, A Management Briefing From ITGI and OGC", in 2008, November 12 http://www.isaca.org/Knowledge-Center/Research/Documents/AligningCOBIT,ITILV3,ISO27002-Bus-Benefit-12Nov08-Research.pdf

[4] Data Security Council of India (DSCI) Promoting data protection – DSCI Security Framework, http://www.dsci.in/dsci-security-framework 2012 December, 12

[5] The ISO 27000 Directory – An Introduction to ISO 27000 http://www.27000.org, 2012, December 12

[6] IT Governance Institute, Leading the IT Governance Community http://www.itgi.org, 2012, December 16

Short Bio Data for the Author

Sanchita Dwivedi -IMS2011032, MS-CLIS, Indian Institute of Information Technology-Allahabad.

I am student of Cyber Law and Information Security. I have completed my Bachelor of technology from Computer Science & Engineering branch. I am also certified ISO 27001:2005 Lead Auditor. I have a keen interest in the domain of Information Security and regulatory compliance. As per the requirement of the curriculum I have to work on a research paper in the last semester and my enthusiasm in Compliance domain prompted me to take up this research paper. Our research work was guided by Dr. Vijay Kumar Chaurasiya.

Watika Gupta -IMS2011012, MS-CLIS, Indian Institute of Information Technology-Allahabad. I am student of Cyber Law and Information Security. I have completed my LL.B. from University of Allahabad. I am also certified ISO 27001:2005 Lead Auditor. I have a keen interest in the domain of Cyber Laws, Information Security and Corporate compliance. As per the requirement of the curriculum I have to work on a research paper in the last semester and my enthusiasm in Compliance domain prompted me to take up this research paper. Our research work was guided by Dr. Vijay Kumar Chaurasiya.

