International Journal of Engineering & Technology, 7 (2.26) (2018) 125-128

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An integrated approach to the audit procedures to be followed during the implementation of Product Data Management (PDM) software

Sam George[1*] , Dr. K.David[2]

[1]Research Scholar, School of Computer Science, Bharathiar University, Coimbatore, Tamilnadu
[23]Associate Professor, Department of Computer Science, H.H. The Rajahs College (Autonomous), Pudukkottai, Tamilnadu
**Email: samtvmus@gmail.com*

Abstract

Product Data Management (PDM) is a domain which comes under the umbrella of Product Lifecycle Management (PLM). While PLM covers entire life cycle of the structure taken for consideration, PDM focus only the hardware portion of it. The implementation of a system which involves product life cycle is a challenging process as it involves an entire changeover of existing working procedures. Moreover, this works in a domain which is dispersed geographically across multiple locations across the globe. In this context, diversification is keyword during the entire phase of operation. This context throws open challenges to find uniformity in procedures, practices, guidelines and documentation in every phase. The first step in defining uniformity is adhering to certain standards and practices which are universally acclaimed. In this context, procedures and directives mentioned in International Standards Organisation (ISO) and Information Systems Audit and Control Association (ISACA) become handy. Audit procedures can be broadly classified in PDM domain as direct and indirect. Direct audit practices are procedure, document and resource oriented while indirect audit focus on finance and infrastructure. In most phases there shall be overlapping relations between these two areas. Management of these aspects is discussed in individual phases of this engineering domain.

Keywords: *Product Data, Risks, Change Over, Implementation phases*

1. Introduction

Product Data Management is a modern engineering domain which has stem out from the umbrella of Product Lifecycle Management. This novel area of application has wide acclaim to knowledge engineering as it archives the entire transactional operations carried out during the life cycle of any assembly or hardware. Bringing uniformity amongst diverse backgrounds is the key success factor in the implementation of this system. Hence there should be a globally acclaimed standard and practice put in place to hold on for authenticated results. International Standards Organisation (ISO) and Information Systems Audit and Control Association (ISACA) are accepted standards in information technology domain. Audit procedures and practices based on the standards needs to be carried out on the system, its implementation strategies, both on hardware and software infrastructure to ensure full proof working. This can broadly be classified as procedure oriented, document oriented, technology oriented and resource oriented on a hierarchical level. However in most cases, there can be overlapping of these standardised practices. Managing a concurrent software engineering application with diverse attributes constitutes the main challenge in this audit procedure.

2. Identification of Product Data features

Before getting into the audit procedures and practices to be followed during the implementation of product data management software, there should be some uniquely identifiable characteristic features of this system. This domain comes under the vast scope of knowledge engineering with intense archival and micro level tracking facility of operations. In an exploded overview of this system, there are hardware structures composed of parts and corresponding Bill of Material (BOM) with its unique characteristic features like corresponding number, description, size and shape to mention a few. Related to this are its drawings and documents which are referred to as documents in general. Archival of these documents is done in related hierarchical windows based structure termed as genealogy or ontology in computer terminology. Access permission to the system is module based with a pre-defined hierarchy based operational and user group based authentication mechanisms. Traversal of the documents in the system is carried out through pre-defined electronic mechanisms termed as workflows. Communication to every user in the group is done by means of customised messages and reporting mechanisms routed through workflows. Related modules of this domain includes electronic handling of minutes of meetings, cohesion and coupling of related modules, operational logs and customised reporting mech-

anisms. The entire domains specific features should be working in a concurrent engineering mode of operation. Secure authentication is provided to this system on database, vault and operational level. Only when these fundamental technological features are incorporated in the system, further audit procedures adhering to these standards can be carried out.

3. Identification of Audit Procedures and practices

Once the features expected in the product data management software is confirmed, the possibilities of commercialization of the technology can be sought to. Since the scope of deployment of this technology is on a wide engineering organization, there is always a need for statutory audit practice being done on every phase of system roll out. Audit procedures can broadly be classified as a. Direct and b.Indirect.

3.1 Direct Audit Procedures

Direct procedures has got a head on impact on the system being implemented as any anomaly found during this direct phase can have negative results or even stop project progress. The various phases in the sales process includes the presales phases, the order receipt phase, the implementation phase and finally the support phase. Every phase of the system can be a document oriented phase, resource oriented phase or a infrastructure oriented phase which can either be a hardware infrastructure, software infrastructure or both. This can be elaborated in detail as mentioned in Table-1.

3.2 Indirect Audit Procedures

Indirect procedures are the ones which doesn't have any head on impact on the system being implemented, rather it can project any delays or warnings during the entire phase. This is elaborated in Table – 2.

Table 1: Direct Audit - Infrastructure based audit Procedures

Sl.No	Audit Phase	Highlight	Main Record	Description
1	Pre-Sales	Document, Resource, Technology	Software Proposal, Resource Management	Software Technology, Interdependency, Infrastructure details, Client-Server details, Finance details
2	Order-receipt	Document	Purchase Order, Software Proposal	Payment terms, Integrations, Implementation strategies, Software License Agreement Policy, Acknowledgement
3	Post-Order	Document, Resource, Technology	Site Readiness Checklist	Infrastructure, Manpower availability, Resource Schedule, Mobilisation Plan
4	Implementation	Technology, Document	Scope Document, Business Blue Print Document, Acceptance Test Plan	Planned and Forecast schedule, Internal or External tools for progress monitoring
5	Go-Live	Document, Resource, Technology	Go-Live Certificate	Change over, User confidence, Training & Documentation
6	Support	Document, Resource	Support Log, Support Document	Support Matrix, Log
7	Project Closure	Document	Support Handover Document, Project Closure	Project Review, Budget Analysis, Helpdesk, Scope for Improvement, Legacy Data Migration

Table 2: Indirect Audit Procedure – Phase wise categorisation

Sl.No	Audit Phase	Highlight	Main Record	Description
1	Project Receivables	Cash Inflow & Outflow	Purchase Order	Payment Milestones on completion of each individual phase
2	Project Risks & Mitigation	Project risks & bottlenecks	Implementation Schedule, Purchase Order	Any foreseen or unforeseen risks and its corresponding mitigation strategies
3	Product Progress	Product shcedules	Version & Revision details	Evaluatethe project features undertaken and its build progress
4	Project Planing	Project Schedules	Implementation Scheule	Analyse the schedule wise project progress
5	Quality Assurance	Project progress bottlenecks like snags, bugs and error	Snag sheets / Bug Reports / Error message logs	Evaluate the bugs and snags occurred in the product and its frequency
6	Management Review Meeting	Review the entire projects running, cash flow, risks, future plans, financial year analysis	Project schedules, Purchase Orders, Implementation details, Risk documents	Analy the running projects and plan for future actions on an yearly basis

4. System Audit Procedures

Audit of computer systems along with hardware and software should be done on periodic basis to prevent any system breakdown or unauthorized system access. List of probable system level intrusions in a collaborative engineering platform is mentioned in Table-3.

Table 3: System Audit Procedure – Hardware & Software based

Sl. No	Type of Attack	Type of Vulnerabilities	Associated Risk
1	Denial of Service (DoS)	Network	Interruption in organisation network
2	Ping Attack	Database Server	Data Theft from database
3	SQL injection	Database driven website	Unauthorised access to database connected to internet website
4	Virus, Worms and Spyware	Network, Database, Application	Temporary shutdown of IT application and database
5	Unauthorised access through internet	Database, Network	Data theft
6	Malicious codes (Trojans)	Network, Application	Damage the computer data and storage on desktop machines

There should be effective preventive mechanisms to counter the attack in systems and some of the audits to be performed on a system level is mentioned in Table-4.

Table 4: System based audit checks

Sl. No	Test	Test Criteria	Objective
1	Configuration of Network devices	Check for network configuration policy	To ensure security to customer information
2	Security controls, standards and certifications	Check for standardisation of network configuration and connected devices	to ensure security to customer information
3	Firewalls, intrusion detection systems	Ensure servers, database and web servers are protected with firewalls	Prevent risk of any unauthorised attack
4	Network intrusion, cyber attacks and phishing attacks should be documented and resolution mechanisms recorded and reported	Antivirus patches applied on timely basis, check for any network intrusion attempts	Prevent cyber criminals, prevent risk of virus coming through external network causing havoc inside the organisations servers and IT systems

5. Applicable standards and guidance

In carrying out the audit procedures, there are certain guidelines, standards and audit procedures provided by Information Systems Audit and Control Association (ISACA) which is described below. These guidelines can act as preventive measure to avoid any catastrophe in computer networks. Some of the notable standards are mentioned in Table-5.

Table 5: Standards and Procedures for audit

Sl. No	Standard / Guidance	Key points / Objectives
1	1202 / Risk Assessment in planning	(i) Risks pertaining to system availability, data integrity and business information confidentiality. (ii) Carry out risk assessment at least once in a year
2	1205 / Audit Evidence	(i) Use of manual audit procedures, computer assisted audit techniques (CAAT) or combination of both (ii) Electronic evidence should be time stamped and have clear trail or source (iii) Source (internal, third party, management) and form (oral, written, representation) of evidence must be evaluated to understand reliability of evidence
3	2208 / Audit Sampling	This method can be used when volume of information requires very high time to examine. (ii) To examine whether sample represents the entire population in both quantitative and qualitative aspects
4	2401 / Audit Reporting	Statutory Audit Report - In case the overall assessed and tested level of IT controls risk is very high and information obtained by statutory auditor is inadequate to support True or False view.
5	1402 / Follow-up Activities	IT auditor should carry out adequate and timely follow up on audit procedures to evaluate the actions taken by management on audit report observations

6. Conclusion

Product Data Management is knowledge based domain under Product Lifecycle Management which has rapid chances of growth in ever-growing engineering industry. With its wide scope of application in diverse backgrounds, it has input and outputs from multiple sources geographically dispersed. In this context, there is always a chance of data loss or system breakdown on account of an unexpected event or attack. This calls for streamlined audit procedures both in the operational aspects of the domain and hardware. There must be procedures and practices which are widely acclaimed in engineering industry and universally accepted. A strenuous audit carried out on a periodic basis can ensure proper working of both the hardware and software systems of this vast domain.

References

[1] Integrated Approach to Financial and IT Audit- Ashish Agarwal. CA, The Chartered Accountant, October, 2017.
[2] Knowledge Management of Part and Bill of Material in an Engineering Industry: Sam George, Dr. K. David. International Journal of Applied Engineering Research [IJAER] Volume 10, Number 69 (2015)

[3] Workflow enabled data processing in a concurrent engineering environment: Sam George, Dr. K. David. Elsevier ProcediaTechnology 24 (2016) 1643 – 1650

[4] An Ontological approach for Product Data Management through workflow – A Case Study Approach Sam George, Dr. K. David. Journal of Computation in Biosciences and Engineering, Volume 2 Issue 3: ISSN: 2348 – 7321

[5] Security strategies for safe data and content access in operational modules of Product Data Management Software Sam George, Dr. K. David, International Conference on Data Security (INCODS), Kalasalingam University, Krishnankoil.Tamilnadu. December 11, 2017**. (Publication awaited)**

[6] Standardisation of Product Data functionalities for automation in Construction Industry : Sam George, Dr. K. David, Third International Conference on advances in Industrial Engineering Applications (ICAIEA 2018), Anna University, Chennai. Jan. 3-5, 2018**(Publication awaited)**

[7] Design Strategies for Part and Bill of Material in Manufacturing Industries: Sam George, Dr.K.David, International Conference on contemporary design and analysis of manufacturing and industrial engineering systems (CDAMIES 2018): National Institute of Technology, Tiruchirappalli, Tamilnadu. **(Publication awaited)**