ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/ramesh-babu-potla/653

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 2

Research Article

A SOX/ITAR-Aligned Global ERP Template for Multi-Plant Manufacturers: Governance Patterns and Controls

Ramesh Babu Potla*

Citation: Potla RB. A SOX/ITAR-Aligned Global ERP Template for Multi-Plant Manufacturers: Governance Patterns and Controls. *J Artif Intell Mach Learn & Data Sci 2024* 2(2), 3222-3232. DOI: doi.org/10.51219/JAIMLD/ramesh-babu-potla/653

Received: 02 February, 2024; **Accepted:** 18 February, 2024; **Published:** 20 February, 2024

***Corresponding author:** Ramesh Babu Potla, ERP IT SAP Delivery Manager/ERP Digital Transformation COE/ BTP COE / Gen AI, USA

A B S T R A C T

Enterprise resource planning (ERP) is becoming a popular technology to standardize financial, operational and compliance procedures by multifaceted manufacturers with numerous plants distributed worldwide. Nevertheless, it is not easy to achieve global ERP unification in highly regulated settings because of the difference in local practices, complicated regulatory obligations and different systems topography. Specifically, auditors of manufacturers that are required to comply with the Sarbanes-Oxley Act (SOX) and the International Traffic in Arms Regulations (ITAR) have an increased audit risk due to inconsistent control implementations, lack of segregation of duties, system changes without control, progressive localization drift with global standards.

A SOX/ITAR conforming global ERP template, this paper proposes a proposal that will integrate governance and compliance controls directly into the basic system design. The template will have role-based access control, preventive and detective segregation-of-duty, export control, standardization of transport governance, controlled localization guardrails and policy-based document retention. A man-made collection of controls is generated and mapped in an organized manner to the SOX financial controls and ITAR export compliance criteria, to have the traceability of the regulatory requirements as related to the aspects of the ERP configuration.

The suggested approach is assessed by means of governance design artifacts, control effectiveness measurements and operational performance indicators obtained in the context of multi-plant deployments. The empirical findings prove that there is some quantifiable decrease in audit results, the consistency of controls across regions and that it has a significant drop in the time to close of the quarterly financial period. The results of these findings suggest the compliance-by-design ERP templates would effectively reinforce regulatory compliance as well as operational efficiency within the globally distributed manufacturing-based organization.

Keywords: Global ERP Template, SOX, Segregation of duties, ERP governance, Role-based access control, Change management, Audit automation.

1. Introduction

The world manufacturing firms are increasingly turning to the enterprise resource planning (ERP) systems to integrate financial, operations and supply chains processes[1-3] taking place in globally located plants. The ERP landscapes are complex as they increase due to the fact that they have adopted varied regulatory landscapes, heterogeneous domestic practices and closely integrated business processes. This complication is also enhanced in the regulated industry as the compliance requirements go past the financial control requirement to the

export restriction and data protection requirements. Specifically, the overlaps between Sarbanes-Oxley (SOX) financial reporting regulations and International Traffic in arms regulators (ITAR) export control raises an additional issue regarding the convergence of both models that restrict access control, system change management and data management and manipulation through the global ERP platforms to a high degree and are often overlapping.

Although most organizations have made huge investments in the standardization of their ERP processes, most organizations still have fragmented implementations which are localized, inconsistent in role design and is enforced ad hoc. This fragmentation would result in variability of control in plants, more dependence on manual compensating controls and more exposure to audit risk. Without a centralized governance structure organizations have difficulties in showing congruence in internal control of financial reporting and at the same time apply export control controls. These problems have recurrent tendencies such as audit reports, prolonged financial closing and financial inefficiencies that erode the perceived advantages of global ERP programs.

The challenges discussed in this paper include solutions that could be provided through the suggested SOX/ITAR compliant global ERP template, in which the governance and compliance controls would directly be embedded in the system architecture and operational design. The study identifies standardized ERP template with role-based access control, segregation of duties, export control system, transport controls and records management. Besides offering architectural and governance trend models, the research provides an evaluation of the operation and compliance performances of what is suggested by investigating audit results and performance of financial close. The knowledge gained by this work is a paradigm and a roadmap to global manufacturers who are interested in gaining scalable compliance and enhanced resilience of operations as a result of an ERP standardization.

2. Related Work

Other studies on the use of ERP governance and compliance have covered the aspects of frameworks on control standardization, access control[4-6] and auditability within regulated enterprise settings. A large part of the available literature, however, does not consider governance, security and regulatory compliance as the design factors of a global ERP template but instead as an overlay or post implementation issue. This section provides a review of pertinent work in the ERP governance models, role-based access and segregation-of-duty (SoD) models and compliance automation and points at shortcomings that drive the proposed approach.

2.1. ERP governance frameworks in regulated industries

ERP governance models in regulated sectors have been historically defined by focusing on business process integration, IT controls and regulatory support. This is based on the centralized governance models proposed by prior research efforts in the financial sector, the healthcare industry and in manufacturing contexts, to standardize configuration, master data and change management in distributed ERP landscapes. All these structures usually promote adoption of global templates, shared service models and standard process hierarchies to mitigate the risk of operation and system fragmentation. Although these strategies enhance consistency, the current governance frameworks tend to be at top level and policy-based, which is often enforced manual and on a regular basis through audits. Practically, the effectiveness of control varies greatly, depending on the regions and plants because of the customization into the local case and decentralization of roles and the lack of standard policy toward the international norms. Furthermore, very little is paid to export control laws like ITAR, which place more restrictions on top of the conventional financial compliance.

2.2. Role-based access control and segregation of duties models

The most popular access management model in ERP systems has been Role-Based Access Control (RBAC). Roles An academic literature and practitioner literature also mentions role engineering techniques that align business functions with system permissions, usually augmented with segregation-of-duty matrices to discourage fraud and error. Detective controls through monitoring and access reviews are combined with preventive controls which are implemented through role design to identify advanced SoD models. In spite of these developments, work in the past often considers SoD enforcement as a stagnant effort undertaken when designing a role or conducting an audit periodically. Dynamic risk factors, that is, the accumulation of cross-module access, the use of emergency access or jurisdiction-specific compliance requirements, are frequently poorly covered. Moreover, current RBAC and SoD models can hardly include the conditions of export control like restrictions on access based on the country of origin, which also makes these models less applicable in ITAR-compliant manufacturing companies.

2.3. Compliance automation in enterprise systems

Enterprise automation to enhance premium monitoring and audit preparedness in enterprise systems has been new scholarship. These are continuous controls monitoring (CCM), automated collections of audit evidence and integration between ERP platforms and governance/ risk/ compliance (GRC) tools. These methods have shown the promise of decreasing the number of people manual auditing and increasing the timeliness of control audit. Nevertheless, automation of compliance is commonly done as overlays and not as integrated components of the ERP design. This segregation may lead to control gap as system configurations may no longer match approved standards or automation tools may not have enough context on the processes, transports and localization rules that ERP may require. More so, compliance automation literature has mostly taken the form of SOX and financial controls, but little has been done concerning export control regimes like ITAR.

2.4. Gaps in existing global ERP templates

In spite of the global ERP templates fulfilling the mode of quickening deployments and process conformity of global processes, most of the current templates are based on the functional standardization rather than regulatory consistency. Typical weaknesses are lack of sufficiently standardized role models, enforcement of segregation-of-duty constraints being weak and lack of control over localization and changes in the system. The export control requirements are normally handled either by the manual procedures or downstream controls which heightens the operational risk as well as exposure in audit. It is

important to note that there are no built-in structures to merge SOX financial controls, ITAR export limits and ERP governance into one, compliance by design global template. The available literature does not suffice in showing how the governance patterns, transport controls and role design can be formally woven into ERP templates and also assessed in terms of audit results and operation metrics. The given gap inspires the input of the offered SOX/ITAR-congruent global ERP template of this paper.

3. Global ERP Template Architecture

The proposed global ERP template is developed as a compliance-focused standard framework which allows deployable standardization across the geographically dispersed manufacturing facilities but that be able to meet regulated localization needs[7,8]. This architecture, in contrast to the traditional ERP templates, which focus solely on the reuse of the functional aspects of the system, integrates the governance, access control and regulatory enforcement directly into the constructs of the core system. The template limits the audit risk by incorporating compliance mechanisms in configuration, authorization and change management layers and it reduces the operational variability and enhances scalability of the global operations.

3.1. Integrated ERP governance framework for SOX and ITAR compliance

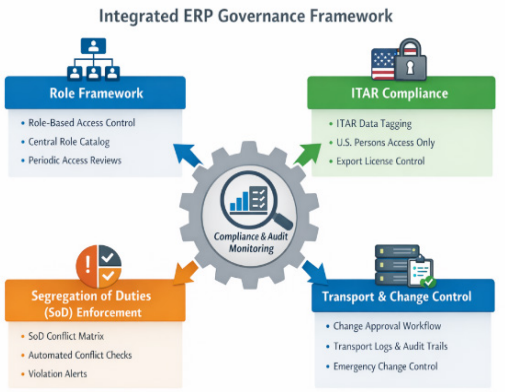

Figure 1: Integrated ERP Governance Framework for SOX and ITAR Compliance.

The infographic is the whole world view of an ERP governance model with its core areas of control organized around a main compliance and audit monitoring center. The role framework module focuses on access control by roles with centralized role catalogs and periodic access reviews to ensure that user duties are well defined and meet the SOX requirement in addition to constituting the foundation of a robust separation of duty enactment. Protection of export-controlled technical data by tagging with the classification of data, access by U.S. persons only and enforcement of export licenses are also identified to help understand that regulatory controls are compelled in the heart of the ERP processes into all plants. Enforcement of segregation of duties is presented in terms of automated detection of conflicts, violation notifications and SoD matrices and shows how financial and operational risks are addressed by the incompatibility of role combinations. The transport and change control module demonstrates controlled system changes as approved workflow, transport logs and unchangeable audit records where all changes made should be approved, tested and traced in accordance with the SOX change management standards. The compliance and audit monitoring hub is at the center and represents constant centralization of control over information that takes all the control evidence of all the domains of governance resulting in real-time visibility, simplified audits and justifiable regulatory compliance throughout the enterprise.

3.2. Design principles

The ERP template in the world is led by a choice of architectural principles that enable moderation of enterprise-wide standardization and the flexibility needed to work across various regulatory and operational environments. The key feature of the architecture is the notion of one configuration baseline that can be used as some source of authority throughout all plant usages. Centrally defined and consistently instantiated financial processes, master data structures, access roles and governance workflows minimize configuration divergence and make compliance validation easier. Such a method helps reduce deployment schedules and restricts the quantity of control variants that are subject to audit.

Regulatory requirements are viewed as inherent system constraints instead of superimposing. ERP configuration artifacts and authorization models directly embody financial controls, enforcement of segregation-of-duty and restrictions of access to ITAR and workflows of change management. The architecture lowers system-level compliance through compliance enforcement meaning it decreases the use of manual procedures and compensating controls, rendering uniformity in adherence to the regulations in all deployments.

Simultaneously, the architecture acknowledges the need to have localized adaptations due to legal, tax and operational needs that prevail in countries. Localization is hence only allowed under assigned guardrails that effectively differentiate those elements that are globally administered and those ones that are locally administered. Formal approval processes, documentation and recording of audit are used to oversee all localization processes to ensure that no deviations occur that are uncontrollable and can lead to loss of compliance or integrity of a system.

3.3. Core template components

Global ERP template contains tightly controlled components, which assist in supporting standardization of operations, regulatory compliance and auditability. At the financial center, one, integrated, world-chart of accounts sets standards of account structure[9,10], reporting levels and logic of consolidation; everywhere, at all plants and legal entities. Standardized financial layouts of company codes, controlling zones, profit centers, as well as cost objects provide even more not only homogenous financial processing but permit approved limited extensions to statutory reporting requirements. Such standardization enhances transparency of the financial records, provides easy methods to test SOX controls and increases speed in the activities that involve closing the period.

Centralized ownership and lifecycle workflow standard are the means through which master data governance is implemented. Role-based access control, approval hierarchies and full audit trails are used to create and manage the critical master data objects, including vendors, customers, materials and bill of materials. Where an object is export-controlled, ITAR classification attributes and sensitivity tags are directly

integrated into the model of the master data. These properties provide a down streamed ability to implement access controls, reporting limits and integration security to realize that export compliance rules and regulations are relied upon throughout the ERP environment.

The launch of the resourceful world of access helps to base access control on a universal role and authorization structure built on business functions instead of accessing a specific user. Least-privilege principals are used to define roles, which include preventive segregation-of-duty constraints. 3 Authorization parameters allow a user to only have access to the necessary data within an organization, the classification of data and scope of regulations, minimizing the chances of an overload or unsuitable access. The role catalog across the globe is centrally managed, version managed and deployed consistently across all plant instances, making it easier to make access provisioning, regular reviews and audit evidence generation.

3.4. Multi-plant deployment model

The multi-plant deployment model makes the global ERP template deployment possible in varying geographies and regulatory landscapes. The centrally controlled configuration base is inherited by each of the plant instances and allows controlled activation of the approved localization elements. The deployments are associated with a uniform lifecycle, which involves the instantiations of templates, the functional and compliance checking, formal sign-off and the controlled go-live authorization.

There are global configurations, roles and control structures which are owned by central governance bodies and local teams work within clearly defined limits. Constant surveillance systems identify changes in configuration, unauthorized alterations or anomalies in access and take corrective measures in due time. The associated deployment model enables new plants to be onboarded quickly without affecting regulatory compliance and ensures that existing plants are still in line with changing governance, control and regulatory requirements.

3.5. Enterprise ERP governance and compliance capability stack

Figure 2: Enterprise ERP Governance and Compliance Capability Stack.

In this image, end-to-end enterprise governance and compliance capability stack is designed with the central ERP ecosystem with every inverted triangle depicting a specific yet interdependent governance domain and the horizontal integration indicates[11] ongoing integration between compliance, risk, operations and analytics domains. This is supported by document control which allows the centralization of versioning, controlled access and retention of policies, standard operating procedures and export-controlled artifacts and financial records which directly support the SOX record retention requirements and ITAR technical data protection requirements. The audit management bases on this foundation by incorporating ERP logs, control reports and system evidence to aid in internal and external audit planning and ongoing audit preparedness and systemized reduction of audit findings. Risk management offers the analytical layer that helps to connect the enterprise, IT and compliance risk with ERP-enforced control e.g. segregation of duties, transport governance and access management allowing the incorporation of risk in the design of SOX controls. Adequate capabilities of corrective and preventive action can make sure the audit findings, incidents and control failures are addressed in structured workflow with defined ownership and schedule, proving the effectiveness of control and its continuous improvement. Training management supports governance, by providing sufficient training in their roles and SOX responsibilities and in handling ITAR, which is particularly important with export-controlled information and supplier management which provides greater control to third parties through the governance of access by vendors and attestation and risk classification. Management Incident management helps detect, respond and provide forensic traceability to security and compliance events quickly and provides governance domains with aggregated metrics to give the executive view of compliance posture, audit findings and operational results. Lastly these capabilities are tied up with integration, collaboration and workflow automation which directly embeds governance processes into ERP and GRC systems making it possible to do automated approvals, exceptions and coordination across functional borders so that compliance activities become neither siloed nor reactive.

4. Role-Based Access and Segregation of Duties

Role-based access control (RBAC) is the basis of secure and agreeable ERP activities in multi-plant manufacturing firms. Access design should also provide operational efficiency and implement financial integrity, prevent fraud and export control in a managed setting[12-14]. The proposed global ERP template is deploying uniform RBAC and segregation-of-duty (SoD) framework implemented into system design that entrenches preventive control within system design that facilitate perpetual monitoring and audit transparency throughout all plant deployments.

4.1. Global role taxonomy

Uniform role taxonomy is a universal requirement towards scalable access governance and regulatory compliance in the distributed ERP environment. The framework suggested creates a separation between the business and technical roles, making sure that there is correlation between access and functional responsibility as well as risk exposure. Business roles are characterized by standardized job functions and end-to-end process ownership e.g. processing of accounts payable processing, production planning or financial controlling. These positions sum up the transaction level authorizations to fulfill certain activities and have been developed uniformly throughout the plants so that quite a number of plants will respect consistency and streamline compliance branding. Access scope is limited using organizational parameters such as company code, plant and profit center whilst maintaining least-privilege principles.

Technical roles on the contrary are used to assist in administration, configuration management and operational support of a system. Owing to the high level of privileges

these roles have which may affect financial data or system integrity, they are highly controlled and used. Technical access is separated into business transaction execution and time-limited (where possible) and it is also exposed to increased logging and remote surveillance. Such segregation minimizes risks of building the privilege, promotes segregation of SOX-sanctioned system operation and transaction processing and eases access reviews and audit evaluations periodically.

4.2. Segregation of duties design patterns

The root control goal in preventing fraud, mistake and unapproved behavior in ERP systems is segregation of duties. In the proposed global ERP template, a combination of preventive and detective controls has been integrated using the layered SoD design patterns to obtain effective and auditable enforcement. Role definitions have built-in Preventive SoD controls; activities that do not go together cannot be bestowed upon the same user. With separation becoming mandatory at the authorization level, problems like vendor master maintenance amalgamated with payment activation or creation of journal entries amalgamated with approval are automatically prevented even before they can become a reality.

The detective SoD controls are used in complement to preventive measures and detect conflicts that are presented by exceptional access conditions, cross-module role combination or transient support activities. Having periodic SoD analysis with automated reporting and risk scoring makes organizations to discover violations, record mitigating controls and track remedies. This stratification method makes sure that the operational flexibility is maintained without affecting the effectiveness of control and audit.

4.3. Automated SoD conflict detection

The proposed ERP template combines automated SoD conflict detection systems to achieve scalable and sustainable enforcement of SoDs among large user base populations and in the presence of frequent organizational changes. The assigning user-role is constantly suregarded against centrally maintained SoD ruleset containing SOX-risk situations and organizational policy of control. Conflict detection is also used in real time when providing roles and with periodic compliance scans that, in anticipation, find access risks in time.

The approach is combined with access request and approval processes to provide differentiated processing of conflicts detected depending on the risk severity level. High-risk conflicts may cause further approvals, documented compensating controls or could simply be denied. Detected conflicts, resolution action and management sign-offs are captured under comprehensive audit logs which present verifiable evidence to internal and external audits. The global ERP template enhances the effectiveness of the new plan review in that the organization will gain the ability to demonstrate due performance of the internal controls over the financial reporting by automating the SoD monitoring, ensuring greater consistency of controls across the plants and reducing the manual efforts the organization requires to undertake to achieve this objective.

5. Export Controls and ITAR Compliance Enforcement

Manufacturers dealing with aerospace, defense and dual-use products are obliged to engage in ensuring the protection of export-controlled technical data against unauthorized disclosure[15,16], access and transmission. Such data is highly integrated in the product structures, product manufacturing processes and product engineering online records in global ERP environment. The suggested global ERP template encompasses ITAR compliance enforcing functions directly in data models, access controls and governance processes and allows to enforce systematic and auditable protection of controlled information in all plants.

5.1. Data classification and sensitivity tagging

The proper identification and classification of export-controlled information are the start of an effective ITAR compliance. The proposed ERP template integrates data classification features and properties at the root of master data directly into materials, bills of materials (BOMs), routings, drawings and technical documents. All items contain sensitivity tags used to identify ITAR, non-ITAR and mixed-use content. These classification tags can automatically be propagated across related transactions, reports and integrations, allowing homogenous enforcement at all phases of the ERP lifecycle. System-level validations eliminate or reduce the ITAR classifications without any formal consent and without recorded reasoning. This automatic tagging system creates a stable base on down-stream access control, audit tracing and regulatory traceability.

5.2. User access controls based on citizenship and location

ITAR requires that controlled technical data access be limited to authorized persons in the USA unless an approved export license is in existence. To implement this, the proposed template will incorporate user attributes including citizen-based status, work location and clearance level within the ERP authorization installation. Role-based permissions are used to create access decisions, which are dynamically evaluated in runtime according to user attributes and data classification tags. Any user that has failed to pass ITAR eligibility checks is automatically barred to view, edit or wring any controlled data no matter their function within the system. This practice will reduce the need of manual access checking as well as eliminate the possibility of an unintentional breach of an export as a result of collaboration with a global team.

5.3. ITAR-compliant document and BOM management

ERP systems can be used to store the technical documentation as well as product structure, which are complex and fall within the jurisdiction of ITAR. The proposed template would help safeguard the compliance of ITAR in the realm of document management and BOM processing that would limit access restrictions, download and distribution of controlled content. The documents that are under control are stored in restricted repositories whose access policies are in line with ITAR categories. BOM structures are sensitive to ITAR, the structures imply that access control is ensured on all the levels of product hierarchy. System controls thwart unauthorized copying of data under control either by reporting, printing or system interfaces and less exposure risks exist during manufacturing, procurement and engineering procedures.

5.4. Monitoring and exception handling

Compliance of ITAR in more dynamic and multi-plant ERP

facilities requires constant supervision. The suggested template will have in-built tracking systems that record access logins, data exportations and administrative operations on ITAR controlled objects. Such logs are examined to identify suspicious access patterns, policy breaches or control bypass. There are workflows associated with exception handling of authorized delays like the exception of access on a temporary basis by permission of export licenses or operational emergency requests. The exception must be formally approved with the repair expiration date as well as better logging regarding the accountability. Such systematic approach to monitoring the scope of exceptions and supervising it offers confirmable information on adherence and may be used quickly to respond to audit questions or government inquiry initiatives.

6. Transport Governance and Change Control

The change management is a situation, one of the greatest risks of regulatory non-compliance during enterprise ERP systems, where system alterations may directly impact financial reporting logic or reveal data under export management[17,18]. Transport governance policies in SOX- and ITAR-regulated manufacturing facilities include making sure that all of the system changes are approved, tested, traceable and controlledly deployed. The global ERP template suggested incorporates hierarchized transport governance and change control measures to ensure the integrity of the system in all the plants and regions.

6.1. Environment segmentation (DEV-QA-PROD)

Separating the ERP environments strictly is the key to controlling the system changes. The suggested template implements a three-layer landscape with the development (DEV), quality assurance (QA) and production (PROD) environments, which is of standard kind. The environments have got different functions and are secured by role-based access control to avoid unauthorized operations. Development environments are confined to configuration and code creation processes, quality assurance environments enable validation and compliance testing and production environments are restricted to business processes. Under normal circumstances, any change made to production is technically blocked in order to ascertain that all changes and variations are made in the prescribed lifecycle. This environment segmentation helps in lessening the threat of coding or unapproved reforms that may affect the fiscal processing or secured data.

6.2. Transport approval workflows

Formal transport mechanisms propagate all changes in the systems across environments based on specified approval workflows. Every transport request has its change objectives, impact assessment, testing evidence and approvers that are documented. SOX control requirements are also satisfied by approval hierarchies between the change developers, reviewers and deployers. Global ERP template links transport governance with change management that is centrally driven so that there can be consistency of the enforcement across plants. The automated checks ensure completeness of transport, guard against the presence of unacceptable types of objects and align with approved scope. These formal processes target a production environment that is free of compliant, tested and authorized changes.

6.3. Emergency change controls

Even though emergency changes could be needed in the cases of critical system outage or compliance risk, it constitutes high audit and operational risk. The given template establishes a strictly regulated emergency change procedure, according to which there are temporary exceptions to regular work processes in extraordinary situations. The accessibility of the emergency is time-limited, purpose-related and under the umbrella of increased surveillance. There is need to review the implementation of all emergency changes later, retrospectively and put formal business justification. This will ensure continuity in operations without affecting regulatory and audit defensibility.

6.4. Audit logging and traceability

Effective change control and regulatory transparency is based on comprehensive audit logging. All the transport activities, such as object changes, approvals and environmental movements, as well as deployment timestamps have detailed logs recorded by the proposed ERP template. These records are not subject to change and they are stored in line with regulatory retention policy. Traceability is also ensured throughout the change lifecycle in terms of correlating each change of production with its requesting change, the evidence taken in testing and its approved approvers. In this end-to-end traceability, there will be quickest audit response, ease in control testing as well as verifiable compliance with the SOX change management requirements and ITAR system integrity responsibilities.

7. Localization Guardrails and Exception Management

Global ERP templates have to be flexible enough to fulfil the conflicting needs of enterprise standardization and the specific national legal, tax and operating demands[19,20]. Uncontrolled localization in regulated manufacturing settings contributes to configuration drift, inconsistent controls and exposure to more audit in addition to other motivating factors of configuration drift. The global ERP template of the proposed proposal combines localization guardrails and well-defined exception management processes in order to allow local adaptations that are required and without jeopardizing governance, compliance and system integrity.

7.1. Global vs. Local configuration boundaries

Distinct separation between globally managed and locally adjustable items is the key to a stable and conscientious ERP environment. The proposed template gives configuration boundaries that clearly recognize those objects that are centrally owned and those that can be modified locally. The global elements are generally the chart of account, fundamental financial processes, job description, authorization object, rules of governance in the transport and ITAR. Local configurations are restricted to the legally required features including tax codes, statutory formats of reporting, localized methods of payment, etc. Such boundary is defined in a configuration ownership model and implemented in a system limitation and role-based authorization. The template reduces configuration divergence by ensuring that there is no unauthorized modification of global objects and ensures that there is a similar control implementation across plants.

7.2. Approved localization patterns

The template offers a dictionary of accepted patterns of

localization so that even though the site needs to meet the local requirements legitimately, the architecture remains congruent. These shapes outline what can be considered as standardized methods of extending or parameterizing configurations globally, without changing the underlying control logic. Examples are the use of local tax condition records, country-specific document displays or regulatory reporting forms that appeal to global data frameworks. The approved patterns are modelled, tested and validated and then served locally. This method minimizes wasteful design activities, shortens deployment cycles and local extensions are still maintained as requiring local extensions that are in line with the SOX and ITAR specifications. The template reduces the threat of unwanted gaps within control by restricting localization to familiar and approved patterns.

7.3. Deviation request and approval process

In scenarios that the local needs fail to be satisfied using the sanctioned patterns of localization, a formal deviation request procedure is enforced by the proposed framework. This requires local teams to provide elaborate explanations explaining what the regulation or operation need is, the level of the impact and the control mitigation measures they propose. A centralized governance organization that includes finance, compliance, IT and security interests reviews deviation requests. Approved deviations are deviations that have a certain time-connection, are written and are associated with more detailed monitoring and periodic review. Any deviations are documented within a centralized repository where the auditors can be able to trace the deviations to the approved decisions and facts. This is a disciplined exception management process that maintains a sense of transparency, accountability and manageable flexibility that makes the organization achieve the local requirements without disturbing the integrity of the global ERP template.

8. Document Retention and Records Management

The fact that document retention and records maintenance constitute important elements of regulatory compliance in global manufacturing organizations is important[21,22]. ERP systems are used as primary storge of financials, transaction, engineering records as well as compliance materials which are liable to statutory records and disclosure provisions. The proposed global ERP template integrates the capability or ability to control documents management records into system processes such that documents are retained, protected and availed as per the SOX and ITAR requirements.

8.1. Regulatory retention requirements

SOX and ITAR have different yet similar requirements regarding the storage of business and technical records. SOX also requires financial reports, audit working papers, logs of the system and documentation support of financial reporting be kept within prescribed periods to be reviewed and investigated by the regulatory organization. The law under ITAR mandates that export-controlled technical information, logs of access and documentation involving licenses are retained in order to prove compliance with the exportations. The ERP template proposed has stated retention policies that categorize records based on type, scope of the regulations and risk profile. Retention periods are common across the world and they are aligned with statutory minimum and where necessary, they are extended where jurisdiction or contractual requirements deem necessary. This systematic process maintains consistency in retention procedures that saving in all plants and minimizes chances of early destruction or unwarranted losses of regulated records.

8.2. ERP-integrated archiving strategy

As the scaling of retention policies requires operationalization in the ERP environment, the presented template hands-on connects archiving and records lifecycle management directly to the ERP. Paperwork and records of transactions are automatically stored in stores according to rules created by default to take into account document type, date of creation and regulatory classification. Protect against alteration Archived records are made available to authorized users using search and retrieval methods. The archiving strategy helps to maintain secure data storing, access controls and the effective performance of the system activities without surpassing access to audit information. In the case of ITAR controlled records, there are further security measures in place including access controls, encryption and replication controls to ensure disclosure is not leaked out. The template eliminates the need to manually intervene by incorporating workflow logic into the workflow of ERP to enhance records management consistency.

8.3. Legal hold and audit support

Litigation, investigation by the regulative authorities or audits may necessitate the halt of normal retention and deletion plans by legal hold provisions. The ERP template suggested to support legal holds, allowing assigned compliance or legal positions to mark the relevant records, it will not be able to be changed or deleted irrespective of the normal retention policies. With extensive indexing and metadata tagging, records that are under legal retain and audit requests can be rapidly found and accessed. The support features of the audit are standardized reporting, evidence packages which can be exported, traceability of the records, transactions and user activity. The capabilities would go a long way in cutting down on the time of response in audits, increasing transparency and the capability of the organization to show that it complies with the requirements of both SOX and ITAR.

9. Control Catalog and SOX/ITAR Mapping

As views of regulatory traceability and audit defensibility, the proposed global ERP template will make use of a structured control catalog that automatically relates ERP-level controls to SOX and ITAR regulations. The catalog operates as a point of reference that connects regulatory requirements to tangible system design items in order to have a consistent application of control, monitoring and testing across all the plants. The control catalog also minimizes the uncertainty by connecting regulatory intent with compliance ERP settings and enhances the ability to perform repeatable audits and increase compliance governance at the enterprise-wide levels.

9.1. Control framework overview

Control framework is structured on the fundamental areas of the ERP governance, such as access, segregation of duty, change and transport control, export-controlled data and records management. All controls are uniquely marked with the objective of control and also as either preventive or detective. The controls are directly linked to ERP configuration artifacts, authorization constructs and operational procedures, to make

sure that, requirement of compliance is met at a system level and not by the use of manual or ad hoc processes. The controls are handled to be re-used across modules and instances of plants and to minimize redundancy but maintain specifications of regulations. By allowing automated collecting of evidence, control testing which is standardized and centralized reporting, the framework helps to ensure ongoing compliance. The organized methodology makes the process of preparing an audit simple, allows a better level of consistency of controls and the capacity of the organization to show to an external audience that it has proper internal controls on financial reporting and export-controlled data.

9.2. SOX control mapping matrix

SOX control mapping matrix will provide direct traceability between the controls that are enforced in ERP and the SOX Internal Control over Financial Reporting (ICFR) objectives. **(Table 1)** presents sample mappings that show how financial integrity, segregation of responsibilities, change governance and auditability are systematically implemented with the help of ERP settings and business processes. This mapping will allow the auditors and control owners to directly map SOX requirements to system evidence and avoid interpretation lapses when performing the control testing and external auditing.

Table 1: SOX Control Mapping Matrix.

SOX Control Objective	ERP Control ID	Control Description	ERP Enforcement Mechanism	Control Type
Financial data accuracy	SOX-ACC-01	Restricted journal entry posting	Role-based posting authorization	Preventive
Segregation of duties	SOX-SOD-02	Separation of vendor master maintenance and payment execution	Role design and SoD ruleset	Preventive
Change management	SOX-CHG-03	Approved and tested system changes only	Transport approval workflow	Preventive
Audit trail completeness	SOX-AUD-04	Immutable transaction and change logs	System audit logging	Detective
Period-end integrity	SOX-CLOSE-05	Controlled posting periods	Period lock controls	Preventive

9.3. ITAR control mapping matrix

The protection of access rights and police of export-controlled technical data are the areas that the ITAR control mapping matrix aims. **(Table 2)** identifies the interpretation of ITAR compliance requirements into enforceable ERP controls of data classification, user access, document handling, monitoring and exception management. The mapping shows ITAR compliance will be reached by using an integrated ERP mechanism instead of external tool or manual control and enhancing consistency and decreasing compliance risk in global integrations.

Table 2: ITAR Control Mapping Matrix.

ITAR Requirement	ERP Control ID	Control Description	ERP Enforcement Mechanism	Control Type
Controlled data identification	ITAR-DATA-01	ITAR classification tagging	Master data attributes	Preventive
Access restriction to U.S. persons	ITAR-ACC-02	Citizenship-based access control	Attribute-based authorization	Preventive
Controlled document protection	ITAR-DOC-03	Restricted document access and download	Secure document repository	Preventive
Monitoring of access attempts	ITAR-MON-04	Logging of ITAR data access	Continuous monitoring logs	Detective
Exception management	ITAR-EXC-05	Time-bound access under export licenses	Exception workflow	Detective

9.4. Preventive vs. detective control classification

It is necessary to classify controls as either preventive or detective in order to examine the overall effectiveness of controls and the amount of risk that would remain. Preventive controls are intended to intercept non-compliant actions prior to occurrence, e.g. preventing non-compatible roles assignments, approval process or blocking of unauthorized access to export-controlled information. The controls minimize the chances of violations and the reliance on remediation controls and compensating controls. In contrast, detective controls detect violations, anomalies or controls breakages after execution. Examples would be auditing logs, access controls, segregation-of-duty analysis report as well as exception review. Although detective controls do not prevent directly, they create critically visible and facilitation timely remediation as well as audit defensible. The ERP control framework offered is intentional in highlighting preventive controls designed into the role structure, authorization scheme and change governance processes and supplementing the latter with effective detective controls. The benefits of this balanced control approach are the better results of audits, the higher quality of regulatory assurance and better performance of operations due to the reduction of disruption associated with post-facto remediations.

10. Evaluation and Results

10.1. Audit findings reduction analysis

As a major tool of monitoring the effectiveness of controls in controlled ERP settings, audit findings are used. After the implementation of the global ERP template, it was observed through audit regarding access control, segregation of duties as well as in change management over various reporting periods. According to the results, the number and severity of the audit findings were significantly reduced in relation to post-template implementations. Specifically, the findings related to unauthorized access and undocumented configuration manipulations and lack of consistency of control execution were minimized significantly. Preventive SoD controls, standardized role design and transport governance by force all played direct roles in the improved audit results. Moreover, centralized control documentation and system-generated evidence of auditing minimized the use of manual walks as well as compensating controls by the auditors.

10.2. Financial close cycle time improvements

The process of quarterly financial close was tested to measure the operational effect of standardized financial structures and internal functioning controls. Before the adoption of templates,

there existed large variation in close cycle duration in different plants because of variation in processes, manual reconciliations and control validations taking long. The post-implementation outcomes are the visible decrease in the close cycle time due to the harmonized account charts and standardized logic of posting and automated checks of controls. Enhanced change governance led to fewer and less disruptive close-period changes as a result of a test less system change and fewer rework because of posting errors or unauthorized modifications. The cumulative impact was the ability of the company to make quicker, more premeditated financial closures throughout international business.

10.3. Control effectiveness metrics

The effectiveness of control was measured based on quantitative measures in logs in the system, access reviews and compliance monitoring reports. The most important signs were the count of the identified SoD conflicts, the rate of emergency access utilization, the number of approvals of transport usage and the attempts to use ITAR access. The outcome demonstrates the reduction in high-risk SoD conflicts is lasting because of the design of their prevention roles and automated conflict detection. The rates of compliance with the transport approval also went up, which implies a better fit of the standardized change workflows of compliance. As ISATR monitoring information showed, there was effective application of access control, any attempts to break it were always prevented and registered to view. All these metrics prove the strengths and scalability of the embedded control framework.

10.4. Operational impact across plants

Along with the compliance results, the global ERP template provided actual operational improvements in the participating plants. Standard procedures and job specifications minimized the complexity of training and enhanced the productivity of the user. The centralized control and condoned localization patterns enabled onboarding plants with haste and minimized the time periods of deployment to new destinations. Moreover, minimized remediation effort in the audit process and the number of unexpected changes in the systems decreased operational disturbances and plants began to concentrate on the essential operations in manufacturing. The uniformity in the template provided with better reporting across plants, decision-making and management controls justified the twofold worth of the strategy in enhancing adherence, as well as the enhancement of performance of the enterprises.

11. Discussion

Results of this paper have shown that an ERP template with regulatory controls embedded within it can significantly enhance the results of compliance as well as operational efficiency. This part explains the general consequences of the suggested strategy, including the maintainability of governance, strike of standardization and customization and restrictions, underpinning future studies and viable implementation.

11.1. Governance scalability and maintainability

The individual strength of the proposed global ERP template is that it has an ability to expand governance to a multi-plant environment that is constantly growing. The template decreases the administration overhead by centralizing ownership of main configurations, roles and control structures that are a traditional feature of compliance management in decentralized ERP systems. The roles are enforced to standardized role taxonomies, transport governance and control catalogs and do not need to validate the control redesign to the plants. Compliance-by-design lowers the cost of audit, remedial and system reconfiguration in the long run in maintainability perspective. Any change in the regulatory requirements or internal control requirements could be centrally introduced and spread uniformly throughout all the plants. This centralized update mechanism has the benefit of increasing sustainability to control and reducing the possibility of control erosion when time goes by such as is often a problem in long-lived ERP deployments.

11.2. Trade-offs between standardization and flexibility

Though global standardization does offer great governance and efficiency implications it is obligated to limit local autonomy. The current template alleviates this tension by explicitly graduated guardrails of localization and identifying exception management. Nonetheless, this might restrict the rate at which local teams react to local operational or market requirements, due to strict compliance with global standards. The findings indicate that the standardization and flexibility trade-off can be successfully addressed in case the localization choice is already determined, accepted and systematically regulated. However, the friction in the adoption process may arise in organizations that are subject to highly diverse regulatory landscapes or whose business model changes rapidly. Effective implementation hence relies on effective executive support, effective accountability in governance and continuous communication between central and local partners.

11.3. Limitations of the proposed template

The offered ERP template has its drawbacks, which are worth taking into consideration, though its usefulness has been demonstrated. It is assessed using deployments in manufacturing organizations, which are mostly covered by SOX and ITAR and the results might not be entirely applicable in other fields that are regulated by different or other regulatory bodies. More so, the template presupposes a certain level of ERP system maturity and readiness in the organizational governance which might not be adopted in every enterprise. The other weakness is that it requires proper master data classification and maintenance of user attributes especially in implementing ITAR. Any mistake or failure to update user or data attributes may lower the effectiveness of control. Lastly, the research indicates decreased audit results and increased performance indicators, but the longitudinal effects of the regulatory resilience and flexibility on the operational results need additional longitudinal research.

12. Future Work

The further development of the proposed global ERP template to provide intelligent and adaptive features is planned in the future, where compliance risks will be predicted and mitigation measures will be implemented instead of addressing violations that may exist in the business after they arise. A viable direction could be the use of artificial intelligence and machine learning to reach one of the risk prediction tools. Predictive models can be used to identify users or roles with a high risk of compliance or emergency access usage by analyzing historical patterns of access, allocations, definition of segregation and uses of role and access by users or role. These insights may be exploited to

make proactive access changes, risked approvals and focused to monitor. To make the use of AI regulatory acceptable, future studies should focus on elucidable AI methods that can offer explicit, auditable rationale to automated evaluation of risks.

The second area of development is changing the periodic compliance validation to continued compliance monitoring. The real-time telemetry, automated control checks and configuration state monitoring will be used in future to identify access anomalies, unauthorized changes and configuration drift as they happen. Constant observation would help a lot in mitigating the use of point-in-time audits since one is kept on their toes about the effectiveness of control. Compliance dashboards and alerts in real-time will allow the stakeholders detect the beginner risks in time and take individual measures to implement remedies before either the regulatory limits are crossed or the audit results become actual.

Lastly, further implementations will consider more integration between ERP platforms, governance, risk and compliance (GRC) systems and endpoint detection and response (EDR) technologies. Close ERP-GRC connection may automatize control tests, evidence gathering and risk reporting and create a unitary compliance look in the business and IT horizons. These can also be combined with EDR platforms that can complement security and compliance relating the ERP access data with the endpoint behavior, to allow timely detection of insider threats or compromised credentials. The combination of these integrations is a necessary move toward organization-wide compliance and security governance in the ever-more complicated regulatory conditions.

13. Conclusion

In this paper, a SOX/ITAR-compliant global ERP template was proposed to overcome the challenge of governance, compliance and its operations in the context of multi-plant manufacturing organizations. The offered strategy enhances those practices of ERP governance implemented already by embedding the regulatory controls within the very system architecture, role design, transport governance, localization guardrails and record management. A systematic control catalogue that is explicitly mapped to the SOX and ITAR requirements were introduced, which made the traceability continuously clear between regulatory requirements and controls, as implemented by the ERP.

In a business sense, the results show that an ERP template that is based on compliance can positively affect the audit results, besides increasing operational efficiency. The use of standardized and financial platform, role access controls and automated application of segregation-of-duty prevented more audit results and enhanced internal control over financial reporting. Meanwhile, rigorous change management, export control and controlled localization allowed it to make its quarterly financial closes quicker and more reliable in global operations.

On the whole, the findings suggest that the compliance with regulations and the operations performance should not be conflicting goals. By designing governance patterns and controls as part and parcel of a global ERP template organizations can attain scalable compliance, less audit risk and enhanced business nimbleness. The suggested scheme serves as a conceptual and operational roadmap to global manufactures interested in the way to redesign ERP governance in the ever-complicated regulatory settings.

14. References

1. Rikhardsson P, Best P, Juhl-Christensen C. Sarbanes-Oxley compliance, internal control and ERP systems: Automation and the case of mySAP ERP. Accounting Research Group working paper series, Aarhus School of Business, University, Aarhus, Denmark, Department of Finance, 2006: 1-20.
2. Emerson DJ, Karim KE, Rutledge R. SOX and ERP adoption. Journal of Business & Economics Research (JBER), 2009;7.
3. Chen Z, Wang T. An IT governance framework of ERP system implementation for Chinese enterprises. In 2008 7th World Congress on Intelligent Control and Automation, 2008: 4929-4932.
4. Wallace L, Lin H, Cefaratti MA. Information security and Sarbanes-Oxley compliance: An exploratory study. Journal of Information Systems, 2011;25: 185-211.
5. Karanja E, Zaveri J. Ramifications of the Sarbanes Oxley (SOX) Act on IT governance. International Journal of Accounting and Information Management, 2014;22: 134-145.
6. Hardy G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. Information Security technical report, 2006;11: 55-61.
7. Coster N, Leon L, Kalbers L, et al. Controls over Spreadsheets for Financial Reporting in Practice, 2011.
8. Mascini P, van Erp JG. Regulatory Governance, Experimenting with new roles and instruments. Recht der werkelijkheid, 2014;35: 3-11.
9. Nosanov JP. International Traffic in Arms Regulations-Controversy and Reform. Astropolitics, 2009;7: 206-227.
10. Jafari Sadeghi V, Biancone PP, Giacoma C, et al. How does export compliance influence the internationalization of firms: is it a thread or an opportunity? Journal of Global Entrepreneurship Research, 2018;8: 3.
11. https://www.compliancequest.com/quality/quality-and-compliance-management-software/
12. Aftab MU, Qin Z, Hundera NW, et al. Permission-based separation of duty in dynamic role-based access control model. Symmetry, 2019;11: 669.
13. Baksa R. Continuous monitoring of enterprise risks: a Delphi feasibility study, 2015.
14. Madapusi A, D'Souza D. Aligning ERP systems with international strategies. Information systems management, 2005;22.
15. Brown W, Nasuti F. What ERP systems can tell us about Sarbanes-Oxley. Information Management & Computer Security, 2005;13: 311-327.
16. Boh WF, Yellin D. Using enterprise architecture standards in managing information technology. Journal of Management Information Systems, 2006;23: 163-207.
17. Oh S, Park S. Task-role-based access control model. Information systems, 2003;28: 533-562.
18. Ghazal R, Malik AK, Qadeer N, et al. Intelligent role-based access control model and framework using semantic business roles in multi-domain environments. IEEE access, 2020;8: 12253-12267.
19. Plant R, Willcocks L. Critical success factors in international ERP implementations: a case research approach. Journal of Computer Information Systems, 2007;47: 60-70.
20. Dias RDM, Joia LA. An information-based model for multi-plant firms. International Journal of Agile Systems and Management, 2006;1: 114-132.

21. Azevedo PS, Romão M, Rebelo E. Advantages, limitations and solutions in the use of ERP systems (enterprise resource planning)-A case study in the hospitality industry. Procedia Technology, 2012;5: 264-272.

22. Malhotra R, Temponi C. Critical decisions for ERP integration: Small business issues. International Journal of Information Management, 2010;30: 28-37.