ALLOut Security

The Future of Controls

Pursuing an Auditable Compliance Model in JD Edwards

WHITEPAPER

Contents

About ALLOut

Who we are

ALLOut is the market-leading security solution for JD Edwards, bringing you the enhanced functionality you need, directly in your E1 or World environment. It's easy to install! There's no need to work with your data outside of JD Edwards, reducing risk & allowing you to maximize existing ERP resource without the need for your team to learn a new system.

Our mission

Our mission is to deliver simple security, streamlined processes & auditable reporting. We believe in providing cost-effective solutions to simply secure and protect organizations against emerging risks. We're the market-leading security, audit & compliance toolset for JD Edwards.

Abstract & Scope

Abstract

In the digital age where data is your organization’s most valuable asset, using an ERP system like JD Edwards to keep this vital resource in the right hands is essential. With compliance and best practices on the cusp of further change, AllOut Security is passionate about providing organizations with strong security controls that focalize accountability and protection through safeguarding strategies.

In light of existing and forthcoming changes regarding the increasing threat that fraud poses on a global scale, this whitepaper aims to inform and advise you on how to proceed securely at a time when efficient and auditable security controls have never been more crucial.

Section one outlines how new complexities and rules characterize the regulatory landscape in terms of emergent personal data protection laws such as Sarbanes-Oxley (SOX) and similar regulations across the globe. This review will address why fraud and employee error pose an increasing risk to an organizations’ data under these conditions and make a case for why effective risk mitigation is essential.

We're dedicated to security and compliance, making protecting your business our only mission.

Abstract Continued

Section two provides a roadmap for the necessary actions that organizations should consider in light of these changes by recommending simple steps an organization can take to make a big difference. These include controls focusing on Segregation of Duties (SOD), User Access Reviews (UARs), Change Management (CM), Data Protection, and other Audit Readiness procedures. Each step will proceed with an 'ALLOut Tip' on implementing these safeguards based on our industry-leading research and expertise.

Scope

This whitepaper frames its scope of inquiry around the inherent and emerging risks that an organization faces when failing to protect their JD Edwards system adequately and recommends ways of mitigating them through the application of strong security control solutions. Keeping you protected and up-to-date with the changing conditions of compliance and best practices takes precedence in our eyes.

Note: This document is intended for general information purposes only, NOT as either legal advice or as a guide for the planning and implementation of security. While we endeavour to ensure that the information is correct at the time of writing, no warranty is given as to its accuracy, and we do not accept any liability for error or omission.

Introduction

Are you adequately prepared to identify and prevent an inaccurate or criminal transaction from taking place within your organization?

Although JD Edwards (JDE) conveniently unifies information facilitating core business operations, including financials, human resources and customer relations, this still leaves data vulnerable to users with excessive authority. Primary risks include fraud, employee error, and compliance violations in such instances.

To mitigate the likelihood of these risks, no individual should have more system access than is strictly required to fulfill their role (principle of least privilege).

Relatedly, no individual should have system access that permits them to execute transactions without checks and balances across an entire business process (principle of segregation of duties). An example of such risks is when one individual can create a supplier, issue an invoice, and issue a payment freely without any internal controls.

The adverse effects of fraud and employee error on an inadequately protected system, even to an organization without specific compliance requirements are real. As section one outlines, emerging personal data protection laws, such as GDPR or HIPAA, continue to significantly impact system security and an organization’s need to protect data.

Additional compliance requirements brought about by SOX, and similar legislation are growing worldwide, making the management of publicly listed companies responsible for internal controls on financial reporting.

The issue is clear, but addressing it can be difficult, disrupting business and consuming valuable resources in the process.

Although JDE has its own security, using this correctly requires in-house expertise that few companies have. According to Gartner, 80% of organizations struggle to hire experienced security practitioners. Furthermore, even with this expertise in place, the process is complex and time-consuming due to multiple programs, menus, users, and role permissions. Thus, it is essential to maintain appropriate controls that restrict access and reduce risk via robust reporting processes that identify vulnerabilities and deliver compliance, which is our forte.

Whether you are complying with SOX, JSOX, GDPR, HIPAA, Oracle Licensing, other regulations or simply your own internal Policies, Allout tools can provide the information you need.

Part 1
What are the risks of weak security in JD Edwards?

Importance of Controls

The importance of a control environment is key, even without compliance requirements!

Few organizations are free of compliance considerations relating to the planning and implementation of their system security, and even then, comprehending legislation is critical. Organizations must act to mitigate the risks of fraud or employee mistakes impacting sensitive operations, leaking personal information or misappropriating money or assets. In PwC's 2020 Global Economic Crime and Fraud Survey[1], 47% of 5,000 organizations across ninety-nine territories reported being victims of fraud between 2018-2020. Of this 47%, more than half involved at least one internal perpetrator. The true scale may be higher still when taking into account those organizations operating without adequate tools to monitor and identify fraudulent activity. As recorded by PwC, the total cost of fraud was $42 billion USD, with 13% of organizations reporting a loss of more than $50 million USD.

[1] Price Waterhouse Coopers. *PWC's Global Economic Crime and Fraud Survey 2020*. PwC. Retrieved March 16, 2022, from https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.

Importance of Controls

It is also important to consider the further consequential costs that could arise as a result of reputational damage, such as:

- Depreciation of the organization's shareholder and investor value resulting from a loss in market confidence.
- Missed business opportunities due to an organization's change in credit rating and financing becoming more costly as a result.

Besides the risk of fraud, the dangers to system data integrity resulting from employee error are often underestimated. This is highlighted in IBM/ObserveIT's 2020 study of 4,716 incidents involving employees (or contractors). The report states that 63% of incidents were due to negligence, 23% attributable to malicious behaviour and 14% to credential theft.[2]

If an individual can create a supplier and enter an invoice, a Segregation of Duties breach has likely gone undetected in the process, which would allow the creation of a fraudulent payment. This is why, when it comes to developing a secure control environment, four eyes are certainly better than two. Without operating within a secure control environment or implementing the Segregation of Duties process effectively, some actions an individual may be able to carry out include:

- Inappropriately access personal data held by the organization.
- Set-up a fictitious or an inappropriate supplier through which to process payments.
- Create fictitious sales orders and direct incoming payments from other customers to them, thereby misappropriating goods.
- Create a "customer" and return goods from them for a refund.
- Change the sourcing of a product to favor a particular supplier.
- Create false employee records and initiate payments to them.

[2] *2020 Cost of Insider Threats Global Report*. Retrieved March 16, 2022, from https://www.proofpoint.com/sites/default/files/observeit/2020/02/2020-Global-Cost-of-Insider-Threats-Ponemon-Report_UTD.pdf.

Data Protection Compliance

Many large economies impose some obligation on organizations to protect the personal data that they store, use or transfer. Any JDE system is likely to hold large amounts of personal information relating to employees or customers. Hence organizations must implement strong security to prevent data loss, information leaks, or other unauthorized data processing operations. Failure to do so could lead to severe civil or criminal penalties and reputational damage. For example, an organization in violation of the EU’s General Data Protection Regulation (GDPR) risks a fine of up to €20 million or 4% of its annual worldwide turnover. Below are key examples of Data Compliance Regulations that impact businesses around the world.

Data Compliance Regulations

Regulation	Country	How this applies to you
General Data Protection Regulation, 2018 (GDPR)	EU	• Applies to any entity in the world, regardless of location, that processes the personal information of individuals inside the EU or EEA. • Applies to information relating to identifiable living individuals within the EU/EEA. • Requires a risk-based approach to implementing 'appropriate technical and organizational measures'[3]. This includes ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services; and a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures.
California Consumer Privacy Act, 2020 (CCPA) California (See also: Virginia Consumer Data Privacy Act and Colorado Privacy Act, 2023)	US	• Applies to for-profit entities doing business in California and which have a gross annual revenue exceeding $25 million or which process information about more than 50,000 California residents.

[3] *GDPR Compliance Guide*. Retrieved March 16, 2022 from https://www.gdpreu.org/compliance/#:~:text=The%20phrase%20‘%EE%80%80appropriate%20technical%20and%20organizational%20measures%EE%80%81’%20are,data%20encryption%2C%20anonymizing%2C%20or%20the%20pseudeonymization%20of%20information.

Data Compliance Regulations Cont.

Regulation	Country	How this applies to you
California Consumer Privacy Act Continued.	US	• Protects information relating to an identifiable California resident only. However, few large US businesses can be certain they do not process information about California residents. • Requires implementation and maintenance of reasonable security procedures and practices.
Health Insurance Portability and Accountability Act, 2003 (HIPAA) - US federal law	US	• Applies to any US entity related to healthcare or having access to patient information (e.g. a law firm dealing with clinical negligence claims). • Protects information relating to the health of an identifiable individual only. • Requires administrative, technical and physical safeguards.
Data Protection Act, 2018 – UK Data Protection, Privacy and Electronic Communications (Amendment Etc.) (EU Exit)) Regulations 2019 (UK GDPR)	UK	• Post-Brexit retains GDPR in essentially identical form. • Applies to any entity that processes the personal information of individuals in the UK.

Data Compliance Regulations Cont.

Regulation	Country	How this applies to you
Personal Information Protection and Electronic Documents Act, 2001 (PIPEDA) – Canada* *Alberta, British Columbia and Quebec have their own similar regimes	Canada	• Applies to private businesses that operate in Canada and handle personal information. While less stringent than GDPR and CCPA, it requires appropriate security in place. • In addition to generally protecting an individuals information, it was a response to GDPR in that it also reassures the European Union that Canadian law is able to protect the personal information of European citizens.
Protection of Personal Information Act, 2013	South Africa	• Restricted to organizations that are either based or process personal data in South Africa. • You must implement appropriate technical and organizational measures to protect personal data in your possession and give due regard to generally accepted security practices and procedures.
The Privacy Act & The Australian Privacy Principles (APPs), 1988 (as amended2000 - 2020)	Australia	• Applies to acts or practices engaged in by organizations outside of Australia that have an Australian link. GDPR The from: misuse, interference and loss; and unauthorized access, modification or disclosure.

Data Compliance Regulations Cont.

Regulation	Country	How this applies to you
The Privacy Act & The Australian Privacy Principles (APPs), 1988 (as amended2000 - 2020)	Australia	• You must 'take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities'[4]to ensure compliance with the APPs with respect to the security of personal information. The more personal information an APP entity has and/or the more sensitive it is, the greater this security obligation is.
Act on the Protection of Personal Information (APPI), amended 2003, 2017 and 2020	Japan	• Modelled on GDPR and applies to any business that handles the personal data of people who are in Japan. • The purpose of this Act is to protect the rights and interests of individuals while taking into consideration the usefulness of personal information by clarifying the responsibilities of state and local government. • The Act also defines the duties of a business handling personal information requiring them to obtain consent and limit use to a specified purpose. They must take necessary and proper measures for the prevention of leakage, loss, or damage, and of the personal data.

[4] *Australian Privacy Principles. Home. Retrieved March 16, 2022, from https://www.oaic.gov.au/privacy/australian-privacy-principles.*

Financial Regulation Compliance

The first key regulation came into effect in 2002 with the Sarbanes-Oxley Act (USA) aimed at improving the accuracy and reliability of financial reporting to protect investors. This came into effect following several high-profile corporate frauds (Enron and WorldCom) that undermined public trust and deterred investment in listed companies.[5]

The following sections of this act are most relevant to our theme of pursuing an auditable compliance model in JD Edwards:

- Section 404 (a) (1) states that management is responsible "for establishing and maintaining an adequate internal control structure and procedures for financial reporting."
- Section 404 (a) (2) requires an annual assessment of "the effectiveness of the internal control structure and procedures of the issuer for financial reporting."[6]

[5] *Public law 107–204 107th Congress an act. Retrieved March 16, 2022, from https://www.congress.gov/107/plaws/publ204/PLAW-107publ204.p.*

[6] *Ibid.*

Accordingly, companies must establish and comply with internal controls on financial reporting to protect the integrity of the data that builds financial records and the annual report. In addition to providing an assessment of financial statements, external auditors are also required to formally assess the adequacy of the company's internal control structure (section 302).[7]

These requirements render both CEOs and CFOs as liable for certifying the accuracy of the company's financial statements and annual reports as those who sign misleading or fraudulent reports can be prosecuted.

If found guilty, penalties include up to 20 years in prison and fines of up to five million dollars. Determining whether your JDE environment is compliant, in addition to considering the various regulations that your company needs to adhere to, you should also take into account any internal standards, practices and policies related to access requirements.

Since the implementation of SOX, similar circumstances and legislation followed in other countries thereafter. For instance, Japan's regulatory framework has altered in response to Japanese market scandals, including Seibu Railway, Oct. 2004, Kanebo, Sep. 2005, and Livedoor, Jan. 2006.

[7] *Ibid.*

Regulations Affecting Companies

Regulation	Country	How this applies to you
Sarbanes–Oxley Act, 2002	USA	Requires public companies to maintain internal controls over financial operations and reporting, attested by management certification and an external auditor. All organizations should limit access to financial data and keep sensitive data safe from insider threats, cyber-attacks, and security breaches. Accordingly, the pillars of SOX compliance are as follows: • Ensure financial data security and prevent malicious tampering of financial data. • Track data breach attempts and remediation efforts. • Keep event logs and make them readily available to auditors. • Ensure appropriate Change Management. • Administer defined processes to add and manage users, install new software, and make changes to databases or applications that manage your company's financials. • Demonstrate compliance in 90-day cycles.

Regulations Affecting Companies

Regulation	Country	How this applies to you
C-SOX (Bill 198), 2003	Canada	• Comparable to SOX without requiring external auditor attestation. • The CSA requires Canadian companies to deliver a "reasonable assurance" to prevent risk of material misstatement.
J-SOX, Financial Instruments and Exchange (FIE) Act, 2006 Evaluation and Auditing Standards for Internal Control for Financial Reports and Implementation Standards , 2007	Japan	• Applies to listed companies in Japan, including their significant subsidiaries and affiliates. • Resembling SOX without, however, requiring an external examiner to management's evaluation of the effectiveness of internal controls, not the internal controls directly.
Code Tabaksblat, 2003	The Netherlands	• Dutch governance code, based on 'comply or explain'. • Dutch code states that this risk management structure applies to all types of risks, such as operational risks and compliance risks. The US Act only applies to risks related to the reliability of financial statements. • More limited auditor review than above laws.

Regulations Affecting Companies

Regulation	Country	How this applies to you
Financial Security Law of France ("Loi sur la Sécurité Financière"), 2003	France	• The French equivalent of Sarbanes–Oxley Act. • All French corps (whether private or public) requires the president of the board of directors or supervisory board to prepare a report on internal control procedures. In addition to their general report on the company's accounts, the statutory auditors are required to prepare a separate report presenting their comments on the company's internal control procedures. • Extend the scope of the chairman's report on internal control and risk management procedures implemented by companies making public offerings to include details about "procedures relating to financial reporting for the parent company, financial statements and, where appropriate, the consolidated financial statements".[8] • The chief executive is responsible for the preparation and content of the company's annual report, containing an "internal control report," which must: ○ Affirm the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting. ○ Contain an assessment, as of the end of the company's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

Regulations Affecting Companies

Regulation	Country	How this applies to you
King Report on Corporate Governance, 2002. South African corporate governance code, King II Report, non-legislative.	South Africa	• Compliance with the King Reports is a requirement for companies listed on the Johannesburg Stock Exchange. • Significantly, however, and unlike the King Report 2002, the Sarbanes-Oxley Act will require the external auditor in 2005 to attest to, and report on, management`s assessment.
UK SOX – date forthcoming	UK	• As part of the government’s sweeping plans to reform audit in the UK, it is looking to bring in a UK version of the US Sarbanes-Oxley Act to regulate directors and improve accountability.

[8] *Retrieved March 16, 2022, from LAW No. 2003-706 of 1 August 2003 on financial security (1) - Légifrance (legifrance.gouv.fr).*

Taking a Risk Based Approach

In light of the above global legislative changes, auditors and executives are spotlighting system controls. Many of these laws show how vital it is that you create a compliance management framework that:

- Considers all regulations, which your organization is required to comply with.
- Includes elements that are preventative, detective and responsive.
- Takes a risk-based approach to prioritizing efforts.
- Is conversant with changes in regulation and of organizational risk according to the evolving legislative landscape.

Accordingly, establishing a compliant environment relies on you knowing and adhering to specific best practices as well as regulations and upholding the internal standards, practices and policies related to access management. Without a robust framework, the organization is in danger of failing to manage risk and meet regulatory and compliance requirements, with the cost of fraud and other internal control failures being well documented.

As the list of regulations continues to grow, compliance initiatives are broadening out to consume more corporate resources. While there is no failsafe plan that can eliminate these risks, adopting a risk-based approach can significantly mitigate them in a balanced and efficient way that reflects the value that is being protected.

ALLOut Security

Part 2
How to achieve a Best Practice Compliance Model

Segregation of Duties (SoD)

The essential starting point is to review your Segregation of Duties!

Segregation of Duties (SoD) is a basic building block of any internal control environment, which attempts to ensure that no single individual has the authority to execute two or more conflicting, sensitive transactions that can impact financial statements or create fraudulent transactions.

At present, there is a heightened interest in SoD, which is partly due to control-driven regulations worldwide and the executive-level accountability for their successful implementation (outlined in section two). However, the underlying reason for these regulations is more important and predates any of these regulations. No individual should have excessive system access that enables them to execute transactions across an entire business process without checks and balances, highlighting the need for integrated IT and financial controls.

According to KPMG, 36% of all material weaknesses reported by US companies in 2020 involved Segregation of Duties issues.[9]

[9] *2021 IPO Material Weakness Study. Retrieved from March 16, 2022 from https://advisory.kpmg.us/articles/2020/material-weakness-study-2020-ipo.html.*

SoD Continued.

As clear as the need for SoD is, there are a variety of reasons why many companies struggle to achieve it:

- Defining and applying appropriate SOD can be difficult due to the increasing complexity and automation of key business processes.
- As businesses grow, additional access is typically granted to more users, which over time may result in the initially designed security controls becoming less effective or misapplied.
- As employees change jobs, it is not unusual for access that is no longer needed to be left available, resulting in unintended access to sensitive processes across many functional areas, including the potential to carry out a complete process from start to finish.
- In order to ensure business continuity with backups in place for processes, lack of additional resources with the required availability and training can limit options.

Following a best practice, SoD design would mitigate these risks as actions are divided amongst multiple individuals. Companies do not need to create undo complexity in their processes. By focusing on the transactions that pose the most significant risk to the business, a company can quickly identify the issues related to access and ensure that appropriate steps are being taken to remedy their root causes at a level that satisfies management and audit parties. In those situations where an SoD conflict cannot be avoided, ensure that you have mitigating controls in place.

ALLOut Tip

When defining your JDE security roles, ensure that each role is free of SoD conflicts. This will simplify your resolution of user issues later. Ensure that your SoD information includes documentation around what controls you are relying on. Involve business process owners or functional management in the SoD review process so that they understand the implication of access requests and the importance of processes that support mitigating controls. Understand that the information needs will include both summary reports for management and actionable information for administrators. Start your SoD process by focussing on those SoD conflicts that create the most risk and move on once those have been addressed.

SoD – Identify Risk

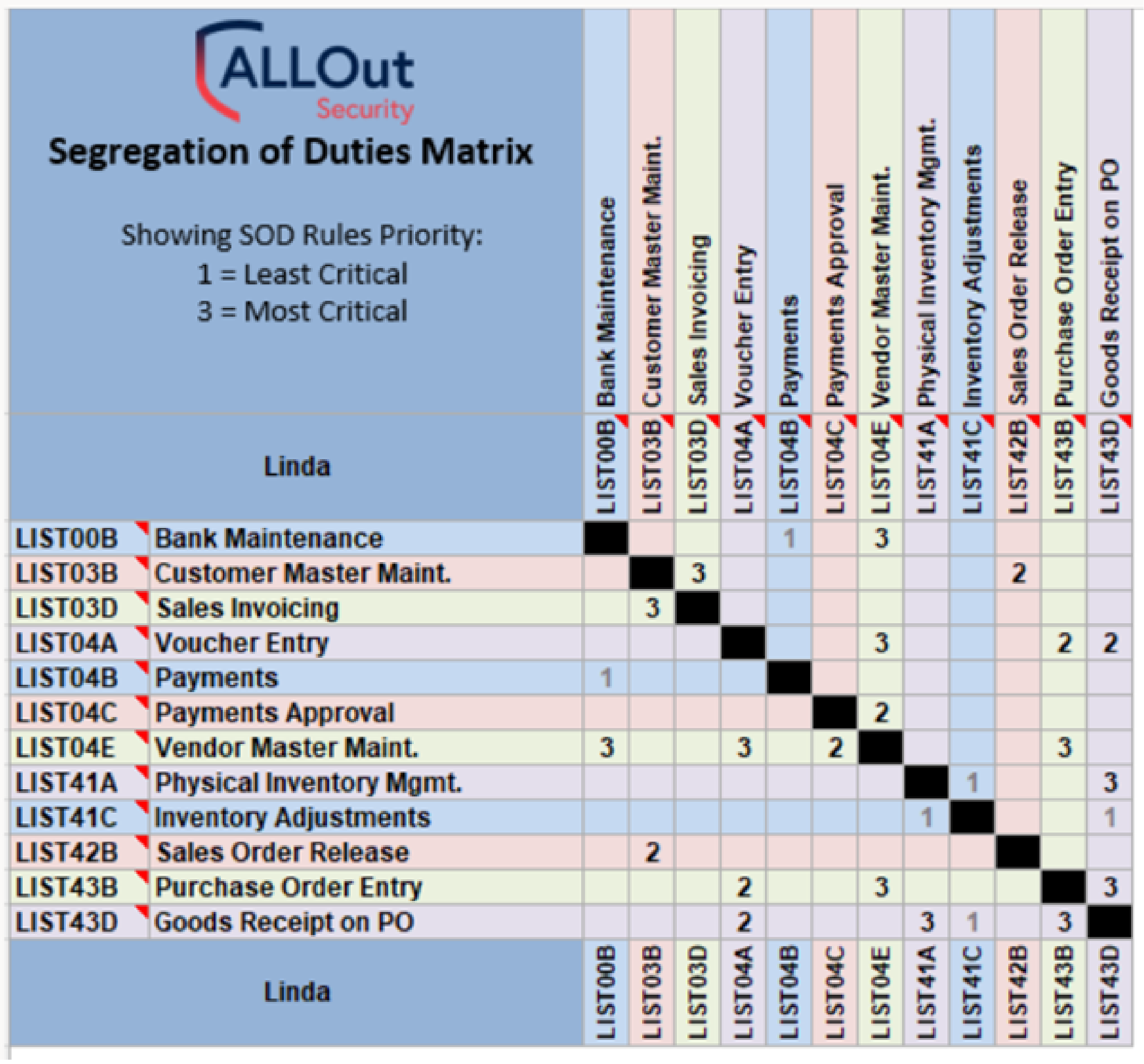
Each complete process within your business should be analyzed individually to determine which steps give rise to potential risk, i.e. where fraud or error could occur. Collaborate with business process owners to divide each process into component parts and allocate them to multiple individuals accordingly. For example, an E1 ‘Procure-to-pay’ transaction should be divided into the following sub-processes to determine where risk occurs: Supply Management, Requisitioning, Purchase Order Entry, Purchase Order Approval, Receiving, Payment, Payment Approval and Invoice Reconciliation.

ALLOut Tip

Our recommendation is to make a list of processes that may be utilized and determine a clear set of guidelines through which processes can be assigned. When identifying these processes, identify all programs that enable updates, including any custom applications or processes that are integrated from outside of JDE. Determine which process should be segregated based on the level of associated risk. ALLOut has a best-practice set of ‘Rules’ and ‘Lists’ that can be used as a starting point to jump-start SoD reporting or as a self-audit tool to compare against how your company operates today.

*The image on the next page is an example of our SoDMaster Matrix.

The ALLOut SoD Matrix



Segregation of Duties Matrix

Showing SOD Rules Priority:
1 = Least Critical
3 = Most Critical

Linda		LIST00B Bank Maintenance	LIST03B Customer Master Maint.	LIST03D Sales Invoicing	LIST04A Voucher Entry	LIST04B Payments	LIST04C Payments Approval	LIST04E Vendor Master Maint.	LIST41A Physical Inventory Mgmt.	LIST41C Inventory Adjustments	LIST42B Sales Order Release	LIST43B Purchase Order Entry	LIST43D Goods Receipt on PO
LIST00B	Bank Maintenance	■				1		3					
LIST03B	Customer Master Maint.		■	3							2		
LIST03D	Sales Invoicing		3	■									
LIST04A	Voucher Entry				■			3				2	2
LIST04B	Payments	1				■							
LIST04C	Payments Approval						■	2					
LIST04E	Vendor Master Maint.	3			3		2	■				3	
LIST41A	Physical Inventory Mgmt.								■	1			3
LIST41C	Inventory Adjustments								1	■			1
LIST42B	Sales Order Release		2								■		
LIST43B	Purchase Order Entry				2			3				■	3
LIST43D	Goods Receipt on PO				2				3	1		3	■
Linda		LIST00B	LIST03B	LIST03D	LIST04A	LIST04B	LIST04C	LIST04E	LIST41A	LIST41C	LIST42B	LIST43B	LIST43D

SoD – Review Access

The complexity of E1 requires that you consider the following when determining which users have access to the programs that comprise your SoD rules/lists:

Security: There are multiple security types in E1, which can be applied to different profile levels to regulate what access users have to programs. Security Strategy in E1 can be employed using two distinct methods:

- ‘Open’: where users have the authority to carry out any activity until access is removed/revoked. With this model, SoD and at - risk access is very difficult to manage. Auditors will often take significantly more audit steps when this is the security model.
- ‘Closed’ (Deny All): where no user can carry out any activity until authority is specifically granted. This security model poses less risk.

Multiple Roles: E1 is designed to allow users to sign in with multiple roles as their responsibilities may lay in more than one capacity. In this case, security access can be assigned to each role. While this is a huge benefit for access management, depending on how you are generating access information, the interaction of these roles can make it slightly difficult to understand what security a user actually has.

Review Access Continued.

Menu and Exit Access: access to programs can also be controlled at the Solution Explorer menu level using ‘Menu Filtering (FineCut)’ and applied to roles to limit what users can access. This is most frequently utilized in an ‘Open” security environment but is not considered to be effective at blocking actual access because of exits and other ways to navigate to programs. An example is when programs can be called using form and row exits from within other programs. Access granted by exits is restricted when using a ‘Closed’ security strategy due to the fact that called programs must be explicitly granted to users. However, exits can give large amounts of unwanted access when employing an ‘Open’ security strategy, thus significantly increasing risk potential.

ALLOut Tip

We recommend a ‘Deny All’, or closed strategy. We also recommend small process - based roles that will be clear of SoD conflicts. This has the benefit of simplifying security maintenance as well. It is very common for user responsibilities to change but much less likely that the business process will, and therefore the required access to change. Layering these multiple roles together to grant an individual’s required access then makes it simpler to meet changing needs.

SoD – Conflict Resolution

An SoD conflict is where a user has access and/or authority to more than one of the constituent parts of an SoD rule. Any conflicts that occur should be assessed and the appropriate action taken:

Remediation and mitigation:

- Remediation is the process of resolving conflicts so that they no longer exist by implementing the following:
    - If the review confirms that a user does not require access to anything in the role creating the conflict, then remove the role.
    - If they need some parts of the role, attempt to grant the required access with another role. If they still need the role, determine if you can remove the program creating the conflict from the role without negatively impacting another user.
    - Change individual user security to remove permission for the program in question.
- Mitigation is the process of implementing a documented control(s) to keep check of any unresolved SoD conflicts where remediation is not possible or appropriate and to change access to eliminate the conflict. This can be as simple as having someone review all vendor master changes for a user who can create vendors and enter invoices for payment. Often mitigating controls are detective controls to determine if something has occurred as opposed to preventative controls to keep them from happening, so only utilize these when necessary.

Conflict Resolution Continued.

ALLOut Tip

We recommend restricting access whenever possible as opposed to reducing risk with a mitigating control. This will decrease risk and time spent on audits. When making security changes to remediate an SoD conflict, avoid creating unnecessary similar security roles that can create confusion in future change requests. Ensure that individuals involved in performing a mitigating control understand that it is being relied on to reduce risk so that business process changes do not inadvertently drop controls unknowingly. One way to do this is to include the mitigating controls as a part of your SoD review. The ALLOut Segregation of Duties reporting can include these on the face of the reports or exclude mitigating conflicts from the reports when you want to just focus on what needs to be addressed. You will also want to have a process in place to review the requirement for and effectiveness of mitigating controls on a regular basis.

User Access Reviews

Managing Segregation of duties is not enough to implement an ethos of good practice and build a firm foundational control environment. Most organizations routinely perform access reviews. These verify whether users have appropriate access to the processes and programs necessary for their roles and responsibilities. Although the procedures used to monitor and verify user access will often vary, you must carry out an annual review to reduce organizational risk. It would be best if you addressed the following when conducting such a review:

- Inactive User Identification.
- Critical Process Access Validation
- Alignment of Business Process
- Access with Job Responsibilities.
- Confirmation of Appropriate Sensitive Data Access.
- Review of Segregation of Duties Conflicts and Implemented Mitigating Controls.
- Assess Change Management Processes and Ensure Compliance.

Failing to de-provision unnecessary or inappropriate access granted over time or for short-term needs is one significant factor contributing towards employees having unintended access. The responsibility for performing periodic verification of the appropriateness of access rests with the relevant system and/or business owners.

Access Reviews Continued.

These reviews should involve cooperation between individuals responsible for defining organizational risk appetite, those who understand current business processes and user job responsibilities as well as those who have system expertise. It is imperative to ensure that the individuals involved understand the significance of what they are involved in and are well-trained.

ALLOut Tip

Always start your user access review process by eliminating inactive users that no longer need to be in the system. With this approach you will not waste time unnecessarily in each of the next steps. Similarly, performing a critical process access validation before a Segregation of Duties review ensures that you do not spend time in remediation or mitigation for access that is not really needed. Critical process access reviews are most commonly completed based on a review of users with critical roles assigned or by utilizing the lists of programs that allow access to the critical process and reporting on users that have access to them. When determining what critical processes to include, do not forget to include access to inquiry or report over confidential or protected data such as employee personal information.

Change Control

Change Control is a term describing the process of managing how changes are introduced into a controlled system. Having a defined change management process firmly in place will go a long way in making sure that your company's security environment addresses risk and is compliant in the long run. Change control typically consists of at least the following five distinct phases:

- **Plan/Scope** what prospective change(s) are to be made. This stage should outline (document) what change(s) are required, who will make the change, how the change will occur, when it will be made and how success will be verified.
- **Assess/Analyze** what effects will the change(s) have. Risk assessment is a very important stage as making a change can potentially have a significant impact. All related areas should be accounted for.
- **The Review/Approval** of an approval process is usually required in any change control model. The impact of the change is considered in the context of the business and the appropriate 'owner' either rejects or authorizes the change(s).
- **Build/Test** those responsible for actioning the change(s) should execute the change in a controlled manner (or environment) where it can be validated to ensure that the defined requirements are met and that no unforeseen issues occur.
- **Implement the change(s)** and the relevant stakeholder(s) review the desired outcome results.

Change Control Continued.

When it comes to your security environment, these steps often include:

- Approving changes before they are made.
- Retaining documentation of approvals, including steps that involve self-monitoring and regular auditing of changes.
- Preventative controls to ensure that planned security changes are tested for the creation of SoD conflicts or unacceptable critical access **BEFORE** access is granted.

ALLOut Tip

The reporting used for critical access and user reviews touched on previously can support the monitoring and auditing steps required to identify risk and non-compliance. Security change reports can be used to put monitoring controls in place so as to ensure adherence to policies around access approvals. Additionally, using ALLOut tools to automate change control steps and manage information within our JDE system can reduce risk and simplify audits.

Data Protection

As discussed, data protection is a key component of many compliance regulations. Data protection is the process of securing digital information while keeping data usable for business purposes all the while ensuring appropriate data privacy. Data protection helps reduce risk and ensures compliance with the many regulations above and should include:

- **Reviewing data protection obligations:**
  - Document regulatory requirements.
  - Identify confidential information or information that provides a competitive advantage.
- **Data Protection Impact Assessment:**
  - Document data inventory.
  - Review data related security in JDE.
  - Review & document access to personal data.
  - Define data confidentiality, integrity & availability requirements.
  - Understand the consequences of non-compliance.
- **Data Breaches & Reporting.**
  - Design & document monitoring procedures:
  - Document process for personal data monitoring.
  - Document incident handling process and responsibilities.

Data Protection Continued.

- **Within standard JDE.**
  - Besides the consideration of application and action code security related to programs with critical data access, several more tools exist within standard JD Edwards's functionality to meet these data access requirements. Involving column security to protect key data fields on an application or table can provide targeted protection to ensure that data in key fields are not available to unauthorized users.
  - Address Book personal data security is an entire set of tools aimed at protecting critical information such as personal data, or identification numbers, from wherever it is accessed, including inquiry screens, reports or UBEs, as well as direct table access such as Data Browser and UTB access. This is much more powerful than simply protecting the data in only one screen where it might appear.

ALLOut Tip

When you are ensuring that protected data is appropriately controlled, do not forget to either manage that data as production data is written to test environments or limit access there as well. While accessing JDE with reporting tools can empower users with information, this allows another opportunity to access sensitive and protected data. Be aware of how this information could be accessed with reporting tools or at a table level. The ALLOut Critical Access Report can be used to provide quick reporting on who is able to access many types of protected data.

Pre-audit Review & Monitoring

Access compliance is never a “one and done” endeavor. Your users, businesses processes, and information are constantly changing. In light of this fact, there should be a defined process that includes steps to take throughout your year in order to avoid audit surprises and minimize risk. These are the primary best practice steps you should take to ensure your ongoing risk management and compliance:

- **Design & document processes proving access to authorized programs & data only.**
- **User provisioning & de-provisioning (including approval).**
- **Review role assignment procedures.**
- **Data vulnerability analysis:**
    - Perform periodic access reviews.
    - Perform critical programs & data access reviews.
    - Document any Segregation of Duties breaches.
    - Certify that privileged user accounts are limited to authorized personnel only.
    - Review users with advanced access, such as table level access.
    - Use encryption on key data.
    - Block access to critical data at a table level for *Public/*All.

Pre-Audit Continued.

- **Password policy:**
  - Make sure users create long & strong passwords.
  - Monitor password change frequency
  - Ensure adherence to password policies.
- **Audit logs:**
  - Utilize the Security Audit History table (F9312) to review changes.
  - Trace transaction history and monitor at-risk transactions.

ALLOut Tip

The over 100 out-of-box reports provided as a part of the ALLout tool set offers quick access to the information needed to support your ongoing compliance efforts. The simple to run delivery streamlines your monthly, quarterly and annual tasks, delivering repeatable and auditable business processes as well as monitoring activities. Utilize the history of changes in security and compliance so that review and audit activities can be targeted to just what has changed where appropriate.

Next Steps

While the vast number of regulations involved combined with the complexity of JDE security can make achieving compliance, effective risk management and a clean audit seem impossible, with targeted steps and the right tools, it can truly become just one more part of your business. The key elements to remember when striving to reduce risk and achieve a successful auditable compliance model are as follows:

- **It is a balancing act:** you can never achieve 100% protection, but you can make sure that business process owners are directly involved in achieving compliance without undue disturbance.
- **Avoid overcomplicating:** one way to ensure failure is to have a compliance process in place that is so complex that those involved cannot understand why they are performing procedures.
- **Managing material risks:** focus efforts on identifying where actual risk is present.
- **Continually adjust:** change is healthy. Achieving compliance relies on a continuous improvement process requiring regular updates that reflect internal and external threats and regulation changes.
- **Take responsibility:** align security control strategies with business processes to ensure Adherence.
- **Invest in network access and database security:** you can implement all of the JDE security to ensure compliance. However, if your data and information are available via external reporting tools or table level updates, your compliance framework is vulnerable.

Get in touch

Find us & Connect

sales@alloutsecurity.com

ALLOUT SECURITY ©2021

8400 E. Prentice Ave.
Suite 1500
Greenwood Village
CO 80111
United States4