**IT 482 Project One**

**IT-482 Ops/Systems Planning**

**Tatiana Epps**

**April 6, 2025**

**Project One**

**Introduction**

Intelligent Computer Services (ICS), a global leader in AI solutions for the finance and retail sectors, is embarking on a transformative journey to migrate 75% of its critical technology infrastructure to the cloud within the next three years. This strategic initiative, driven by significant revenue growth and a strong financial position, aims to enhance agility, scalability, and cost-effectiveness. As the lead solution architect, this strategic plan outlines the proposed migration of ICS’s on-premises Oracle PeopleSoft Human Capital Management (HCM) enterprise solution to Oracle HCM Cloud, a Software as a Service (SaaS) offering. This plan will detail the new client-server architecture, its organizational fit, security considerations, business impact (including cost), compliance requirements (including SOX), and data privacy implications (with a focus on breach notifications and GDPR), providing a roadmap for a successful and secure cloud migration.

**Client-Server Architecture**

* **Current Components:** ICS currently operates a traditional client-server architecture for its Oracle PeopleSoft HCM, hosted across its five global data centers. The key components of this architecture include:
  + Application Servers
  + Database Servers
  + Web Servers
  + Network Infrastructure
  + Client Machines
  + Load Balancers
  + Storage Systems
* **Future Components (Post-Migration to Oracle HCM Cloud):** The migration to Oracle HCM Cloud will fundamentally shift the client-server architecture. The future state will primarily consist of:
  + Client Machines
  + Internet Connectivity
  + Identity and Access Management (IAM) System
  + Network Infrastructure (optimized for cloud connectivity)
  + Potential Integration Services (iPaaS)
* **Lowering Total Cost of Ownership (TCO) with SaaS:** Migrating to Oracle HCM Cloud as a SaaS solution offers potential TCO reductions compared to the current on-premises model. Generally, SaaS can lead to lower infrastructure costs, reduced IT staffing needs for maintenance, predictable subscription fees, and the elimination of upgrade expenses (Armbrust et al., 2010).
* **Cloud Scalability for Future Growth:** Leveraging Oracle HCM Cloud provides inherent scalability to accommodate ICS’s future growth. Cloud platforms are designed to handle fluctuating demands without significant upfront investment in hardware (Armbrust et al., 2010).

**Organizational Fit**

Benefits and Drawbacks of IaaS and SaaS:

* **Infrastructure as a Service (IaaS):** Offers greater control over infrastructure but requires more IT management.
* **Software as a Service (SaaS):** Provides a fully managed application with lower overhead but less customization.

The decision to adopt SaaS aligns with common industry trends, where organizations are increasingly leveraging cloud-based HCM solutions for their scalability and efficiency. By offloading HCM infrastructure management, ICS can refocus resources on its core AI innovation and client services. A modern, cloud-based HCM system can enhance agility, support global growth, and potentially offer advanced HR capabilities. This aligns with ICS’s mission to be a global technology innovator and its vision of delivering first-class client services. The choice of Oracle HCM Cloud as the information system directly supports ICS’s strategic goals, and the organizational design will need to adapt to leverage the new system effectively.

**Security Considerations and Needs**

Migrating ICS’s critical HCM data to the cloud necessitates a robust security strategy. Key considerations include:

* **User Connectivity:** Mandatory Multi-Factor Authentication (MFA) and exploration of Zero Trust Architecture (Forrester, 2025) for secure access over the internet.
* **Data Encryption:** Encryption of data at rest and in transit using industry-standard protocols.
* **Identity Management:** A centralized IAM system integrated with Oracle HCM Cloud.
* **Additional Security Solutions:** Consideration of CASB, SIEM, and DLP tools.
* **Managing Security Deployments and Streamlining Policy Updates:** Leveraging cloud platform management consoles and Infrastructure-as-Code (IaC) principles.

**Business Impact**

A thorough Business Impact Analysis (BIA) will be conducted to identify critical business processes reliant on the HCM system, assess the potential impact of disruptions, and determine recovery objectives. This analysis will consider financial, operational, and reputational impacts of events such as security breaches or system outages.

**Impacts to Costs:** The migration to Oracle HCM Cloud will have significant cost implications that require careful analysis as part of the BIA. While SaaS offers the potential for long-term TCO reduction, the initial migration and ongoing operational costs need detailed consideration. These include:

* **Subscription Costs:** Oracle HCM Cloud's pricing varies based on the modules selected (e.g., Workforce Rewards, Workforce Management, Talent Management) and the number of users. A detailed analysis of ICS's current and projected usage of these functionalities is crucial to accurately estimate subscription expenses.
* **Implementation Costs:** The migration process itself will involve costs related to data migration, system integration with other ICS platforms, configuration, testing, and project management. These costs can be substantial and require careful planning and budgeting.
* **Training Costs:** Training ICS's 150,000+ global workforce on the new Oracle HCM Cloud system will be a significant expense. A comprehensive training plan, considering different user roles and global locations, is necessary.
* **Potential Integration Costs:** Integrating Oracle HCM Cloud with other existing ICS systems (e.g., finance, payroll, talent development platforms) may incur additional costs depending on the complexity and the need for middleware or custom integrations.
* **Ongoing Operational Costs:** While infrastructure costs will decrease, ongoing operational costs will include the SaaS subscription fees, potential costs for data storage beyond the included limits, and the cost of managing integrations and user access.

The BIA will include a detailed cost-benefit analysis, comparing the current operational expenses of the on-premises Oracle PeopleSoft HCM with the projected costs of the Oracle HCM Cloud solution over a defined period (e.g., 5 years). This analysis will factor in both direct costs and indirect benefits such as increased efficiency and reduced IT overhead.

**Risks of Moving to the Cloud:** Several risks must be carefully managed during the cloud migration:

* Potential Breaches
* Cost Increases (as detailed above)
* Vendor Lock-in
* Internet Connectivity Dependence

**Compliance**

ICS must adhere to various IT policies, laws, regulations, and standards. Key frameworks include the NIST Cybersecurity Framework (CSF) (National Institute of Standards and Technology, 2018) and ISO 27001 (International Organization for Standardization, 2022).

The Sarbanes-Oxley Act (SOX) is particularly relevant as it impacts financial reporting and internal controls. The migration to Oracle HCM Cloud will necessitate a review and potential revision of ICS’s internal controls related to financial data managed within the HCM system. This includes access controls, audit trails, and data integrity measures within the cloud environment to ensure compliance with SOX requirements for financial data accuracy and security. Our plans and policies will need to be adapted to leverage the security features of Oracle HCM Cloud while maintaining the necessary controls for SOX compliance.

ICS must adhere to various IT policies, laws, regulations, and standards. Key frameworks include the NIST Cybersecurity Framework (CSF) (National Institute of Standards and Technology, 2018) for managing cybersecurity risk and ISO 27001 (International Organization for Standardization, 2022) for information security management. Leveraging the NIST CSF can provide a flexible framework. ICS will rely on Oracle’s patching schedule for the SaaS platform and maintain its own vulnerability management program.

**Data Privacy**

Adherence to the General Data Protection Regulation (GDPR) (European Union, 2016) is critical for European residents’ personal data, and compliance with other global data privacy laws is also necessary.

**Breach Notification Requirements:** A critical aspect of data privacy is the handling of data breaches. Regulations like GDPR impose strict breach notification requirements. Under GDPR, if a personal data breach is likely to result in a risk to the rights and freedoms of natural persons, ICS, as the data controller, is obligated to notify the relevant supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach. This notification must include specific information, such as the nature of the breach, the categories and approximate number of data subjects concerned, the categories and approximate number of personal data records concerned, the name and contact details of the data protection officer or other contact point, the likely consequences of the breach, and the measures taken or proposed to be taken to address the breach, including measures to mitigate its possible adverse effects.

Similar breach notification requirements exist under other data privacy laws globally, although the timelines and specific details may vary. ICS must develop a comprehensive Data Breach Response Plan that outlines the procedures for identifying, containing, investigating, and reporting data breaches in accordance with all applicable legal requirements. This plan will include:

* **Incident Response Team:** A designated team responsible for managing data breaches.
* **Detection and Escalation Procedures:** Processes for identifying potential breaches and escalating them to the response team.
* **Investigation and Assessment:** Procedures for determining the scope and impact of a breach, including the types and volume of PII affected.
* **Notification Procedures:** Clear protocols for notifying supervisory authorities and affected individuals within the legally mandated timelines. This will require understanding the specific notification requirements of GDPR and other relevant laws.
* **Remediation and Mitigation:** Steps to contain the breach, recover compromised data, and implement measures to prevent future occurrences.
* **Documentation and Reporting:** Maintaining detailed records of all breach incidents and the actions taken.

The migration to Oracle HCM Cloud will necessitate ensuring that Oracle’s security incident management processes align with ICS’s breach notification obligations. Clear lines of responsibility between ICS and Oracle regarding breach detection, investigation, and notification need to be established in the service level agreements.

**Impact of GDPR and SOX on Operations, Plans, and Policies:**

* **GDPR:** Significantly alters ICS’s operations, plans, and policies related to the personal data of EU residents. This includes:
* **Data Governance:** Implementing stricter data governance frameworks to ensure lawful processing, data minimization, and purpose limitation.
* **Consent Management:** Establishing clear and auditable consent mechanisms for processing personal data.
* **Data Subject Rights Procedures:** Developing and implementing processes to handle data subject requests (access, rectification, erasure, etc.).
* **Privacy by Design and Default:** Integrating data protection considerations into the design of systems and processes from the outset.
* **Cross-Border Data Transfer Mechanisms:** Implementing appropriate safeguards for transferring personal data outside the EU.
* **Vendor Management:** Ensuring that Oracle, as a data processor, provides sufficient guarantees of compliance with GDPR.
* **SOX:** Impacts ICS’s financial controls and reporting processes within the HCM system. This requires:
  + **Access Controls:** Implementing robust access controls to prevent unauthorized access to financial data within Oracle HCM Cloud.
  + **Audit Trails:** Ensuring comprehensive audit trails are in place to track changes to financial data.
  + **Segregation of Duties:** Implementing appropriate segregation of duties to prevent conflicts of interest.
  + **Change Management:** Establishing controlled processes for any changes to the HCM system that could impact financial data.
  + **Regular Audits:** Conducting regular audits of the HCM system’s controls to ensure ongoing compliance with SOX requirements.

These regulatory frameworks will be central to the planning and implementation of the Oracle HCM Cloud migration and will necessitate significant updates to ICS’s existing operational procedures, strategic plans, and internal policies.

**Conclusion**

In conclusion, this strategic plan outlines the crucial factors for migrating ICS's Oracle PeopleSoft HCM to Oracle HCM Cloud. It emphasizes the need for a secure, efficient, and compliant transition that addresses the complexities of global regulations. This technological evolution is strategically vital for enhancing ICS's agility and scalability in the modern digital landscape.

**Resources**

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM,* 53(4), 1 50-58. <https://doi.org/10.1145/1721654.1721672>

European Union. (2016). General Data Protection Regulation (GDPR) (EU) 2016/679. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. <https://www.iso.org/standard/77994.html>

Forrester. (2025, January 6). Zero Trust Security: the business benefits and Advantages. <https://www.forrester.com/zero-trust/>

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity. <https://www.nist.gov/cyberframework>

uCertify. (n.d.). Chapter & Lessons : IT-482-11432 [based on ITIL 4® Foundation] en-uCertify. uCertify. https://www.ucertify.com/app/?func=ebook&chapter\_no=0