protiviti®
Global Business Consulting

Managing EUDA Risks in Financial Institutions

Introduction

End-user developed applications (EUDAs) — applications developed and maintained by an organisation's users rather than its information technology (IT) department — are a significant source of risk in financial institutions (FIs), as they are increasingly relied on to provide critical data for financial, management and regulatory modelling and reporting. The applications — also known as end-user computing applications (EUCAs), user-developed applications (UDAs) or shadow IT applications — include spreadsheets, user databases, robotic process automation (RPA) tools and reporting applications that leverage code such as SQL, Python or ACL. The introduction of low-code applications, like Microsoft Power Platform (e.g., Power BI, Power Apps and Power Automate), has simplified the creation of EUDAs and caused an uptick in their usage across organisations.

Though they drive efficiencies, EUDAs are not subject to established software development life cycle processes and are often developed without considering the risks they expose and the necessary mitigating controls. This governance shortcoming has been highlighted by the global shift to fully remote and hybrid work models, which have created environments that enable employees to create and store EUDAs on private servers, outside of institutions' control. Decentralisation has increased the risk of reporting errors and access breaches.

Given the implications of such governance failures and the potential for the availability, integrity and confidentiality of data used by EUDAs to be compromised, global regulators and external auditors have heightened scrutiny of the privacy and protection of the data processed within EUDAs and specific focus on applications that support financial or regulatory reporting processes. Recent regulatory guidance includes the U.S. Office of the Comptroller of the Currency's (OCC) 2021 *Model Risk Management* handbook and the U.K. Prudential Regulation Authority's (PRA) 2021 letter on thematic findings on the reliability of regulatory reporting. The increased focus on these applications, in addition to the existing laws and regulatory expectations impacting their use, builds urgency for institutions to proactively address deficiencies in EUDA oversight and risk management practices.

Below, we outline the impact of insufficient EUDA governance on enterprise risk, provide an overview of the global regulatory standards for EUDA use and risk management, and walk through a governance framework that institutions can adopt to mature their EUDA controls.

Enterprise risk impact

EUDA governance is a critical risk management concern given the breadth and sensitivity of data that EUDAs are able to access. If unchecked, EUDAs may weaken operational sustainability and compliance efforts. Poor EUDA governance can impact enterprise risk across several dimensions, including the following:

- **Financial risk:** Inadequate governance of EUDAs can result in regulatory fines, reputational damage and customer loss, among other costs. A study by Chartis Research calculated that the annual value at risk from losses due to errors in EUDAs totalled USD $12.1 billion across the 50 largest financial institutions.1 However, errors from EUDAs are common and often underreported or not captured, meaning organisations may not fully realise the possible costs of poor EUDA governance.
- **Data governance/protection risk:** Customer and company data breaches may occur in EUDAs, as the applications may have access to several data sources but lack essential IT security controls for protection against inappropriate access. Institutions must consider their data privacy and data usage obligations. EUDAs that are not stored in an access-restricted drive or that are not encrypted or password-protected may be shared freely, compromising the security of critical data for the organisation, leading to regulatory fines2 and reputational losses. Chief information officers (CIOs) and chief data officers (CDOs) are responsible for the data within the organisation and must attest to its control and accuracy. Inadequate governance and oversight of this data may lead to a lack of ownership and control.
- **Financial misstatement risk:** EUDAs may not be reviewed periodically for the availability, integrity and confidentiality of data inputs and outputs. When combined with inadequate access or change management controls, incorrect calculations or user data manipulation may occur, leading to incomplete, inaccurate or fraudulent management,

1 "Quantification of End User Computing Risk in Financial Services," Chartis Research Staff, Chartis Research, June 2, 2016, www.chartis-research.com/operational-risk-and-grc/operational-risk/quantification-end-user-computing-risk-financial-services-1142.

2 As an example, see "OCC Assesses $400 Million Civil Money Penalty Against Citibank," October 7, 2020, Office of the Comptroller of the Currency, https://occ.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html.

regulatory or financial reporting. These potential points of failure may require restatements of financial reports and result in the incurrence of subsequent fines, share price reduction and loss of public trust.

- **Business disruption risk:** Lack of access controls and IT support for EUDAs can compromise the integrity of the organisation's cybersecurity framework. Cybercriminals may gain access to the business data through insecure EUDAs, potentially causing business disruptions. Cyberattacks and the resulting operational impact will diminish customer trust and can lead to financial expenditures such as regulatory fines, ransomware payments, and marketing and public relations spend to alleviate reputational loss.
- **Internal fraud risk:** EUDAs may lack change management controls and be editable by any resource that gains access. Lack of an audit trail and password protection to access EUDAs and edit EUDA fields or calculations can allow users to manipulate data, resulting in simulated outputs that may be used to conceal fraudulent activity.
- **Model risk:** EUDAs are utilised across organisations, often for calculating forecasts and results. Inaccurate reporting due to lack of governance over EUDAs can impact strategic business decisions and affect planning for budgeting, headcount or other key business metrics
- **Documentation risk:** As shadow IT applications, EUDAs may not be fully identified, documented and managed by an organisation. Lack of governance and oversight of EUDAs can result in a complex network of independent applications, leaving management unaware of the number of EUDAs in place, how they are used in critical business processes, their link to other business systems and applications, the source of data inputs, and how data outputs are used.

Global regulatory standards

Regulators and external auditors have increased their focus and scrutiny on EUDAs that support regulatory or financial reporting processes. While the level of regulation varies between jurisdictions, regulators have published standards and guidance to help organisations comply with their reporting and risk management obligations. An overview of the standards affecting EUDAs in the United States, the United Kingdom, the European Union and Australia follows.

U.S.

The Sarbanes-Oxley Act (SOX): SOX applies to all public companies listed in the U.S. and aims to protect shareholders from accounting errors or fraudulent financial reporting. SOX Section 404: Management Assessment of Internal Controls requires management and external auditor attestation of the effectiveness of internal controls over financial reporting (ICFR), which includes control over end-user computing applications used for reporting purposes. It is

required that these applications have strict controls to give assurance of the accuracy and integrity of the data inputs and outputs.

The Federal Reserve Board (FRB) and OCC SR 11-7: This document provides extensive guidance on model risk management, including any EUDA models used for reporting within an organisation.

U.K.

The Senior Managers and Certification Regime (SM&CR): Applicable to all institutions regulated by the U.K. Financial Conduct Authority (FCA), the SM&CR aims to protect customers by applying accountability standards for the adequate conduct and competence of management in regulated financial institutions. These standards include being accountable for the accuracy and completeness of reporting, which may be derived from EUDA outputs. As such, EUDA governance will be key for accountable persons to meet their obligations under the SM&CR.

EU

The General Data Protection Regulation (GDPR): The GDPR applies to all EU member states and any company that conducts business with EU residents. It requires organisations that hold customers' personal data to oblige with data protection principles, including purpose limitation, data minimisation, data accuracy, storage limitation, integrity and confidentiality, and accountability, as well as lawfulness, fairness and transparency. Institutions that use EUDAs must therefore have strong controls for the data in the applications, ensuring accuracy, integrity and adequate record retention and deletion processes.

The Basel Committee on Banking Supervision (BCBS) standard 239 (BCBS 239): This standard outlines 14 principles for effective risk data aggregation and risk reporting, including governance, accuracy, integrity and completeness of data used for risk and regulatory reporting purposes. EUDAs that support the risk reporting process must have adequate controls to provide assurance that the data meets the requirements of the principle.

Australia

The Australian Prudential Regulation Authority CPG 235 — Managing Data Risk: This prudential practice guide provides guidance to APRA-regulated financial institutions for effective management of data risk through the assessment and management of data quality. This assessment includes accuracy, completeness, consistency, timeliness, availability and relevance of the data used across the organisation. Adequate EUDA governance includes assessment of the data used by the applications, helping ensure appropriate management of data risk.

The Banking Executive Accountability Regime (BEAR) and **the Financial Accountability Regime (FAR):** BEAR and FAR apply to APRA-regulated institutions and, similar to the SM&CR, aim to protect customers by applying accountability standards for the conduct and competence of management. FAR was introduced in 2022 and will replace BEAR. Designated "Accountable Persons" under BEAR and FAR must attest to the accuracy and completeness of financial reporting as part of their responsibilities, which may be derived from EUDA outputs.

EUDA governance framework

Institutions should prioritise building an adequate EUDA governance framework that enables them to identify, assess, manage and report on their EUDAs and corresponding risks. Leading EUDA governance practices observed in mature organisations, and in line with regulatory expectations, include the following key elements:

Development and implementation

- Align EUDA governance objectives with enterprise strategic objectives and risk appetite.
- Institute an EUDA policy that clearly communicates the institution's definition of an EUDA.
- Design a rating tool and questionnaire to categorise EUDAs based on criticality and risk for the business.
- Establish a risk-based EUDA control assessment from a standardised list of applicable controls to identify the controls already in place and any control gaps. Higher-risk EUDAs will require additional controls. All control gaps noted should be supported by an action plan to remediate the corresponding risk. Control areas to consider include:
  - Documentation and key person dependency
  - Version control
  - Access management
  - Data backup, recovery and retention
  - Data integrity
  - Calculations and output validation
  - Change management
- Conduct a periodic assessment of the criticality and control environment of EUDAs, with defined reassessment timelines using a risk-based approach (e.g., at least once every 18 months, and more frequently for high-risk or business-critical EUDAs).

- Define a process for retiring EUDAs, including data transfer, retention or deletion requirements.
- Train stakeholders to use, assess and report on EUDAs, including low-code applications (i.e., Microsoft Power Platform). Training can help mitigate key person risk and create a controlled environment for end users to innovate.

Sustainability

- Define roles and responsibilities across people, processes and technology. Ownership of the EUDA framework should be delegated to application-development teams, which can provide support and guidance to end users as needed.
- Align the EUDA framework with the existing risk management framework by connecting EUDA risk management activities to existing operating risk management activities (e.g., risk and control self-assessments).
- Embed the EUDA framework in the institution's IT strategy, with a focus on how EUDAs can be used to increase effectiveness. Visibility of EUDAs can help develop and improve the IT strategy.
- Store EUDAs in designated locations within the network based on either business unit or type of process the EUDA supports. Control user access to the shared locations.
- Evaluate the institution's EUDA framework maturity and identify deficiencies. The maturity assessment can include discovery, assessment, reporting or ongoing monitoring of EUDAs.
- Apprise business stakeholders and EUDA owners of the benefits of effective EUDA governance to bridge the gap between responsibilities of senior management and other stakeholders. Business stakeholders should not see effective governance as a burden, as it can help optimise EUDAs so they are more efficient, easier to navigate and transferable across resources, and to identify obsolete or duplicate EUDAs that can be consolidated.

Reporting

- Categorise EUDAs according to business unit, application type, criticality, risk rating and purpose (e.g., management, financial or regulatory reporting). Business units that heavily use EUDAs may show underfunding or lack of support from an IT perspective.
- Clearly define data input sources and output destinations to identify connections and reliance between business units and applications.
- Catalogue, maintain and update EUDA inventory regularly, consistent with the established EUDA risk assessment timelines.

- Map critical data elements to EUDAs and include them in reporting, indicating how they are used in data inputs and outputs.

Technology

- Leverage existing technologies to improve EUDA governance based on the needs of the organisation, whether for initial identification of EUDAs or continuous monitoring and improvement.
- Implement a EUDA management system to help maintain a EUDA catalogue, visualise data inputs and outputs, identify interdependencies between business units, maintain the risk and control assessment schedules, report on risks, and provide alerts when key risk indicators are surpassed or control deficiencies are noted.
- Treat technology as a supplement to improve EUDA governance rather than a solution. Institutions should integrate the EUDA governance process into the enterprise and use systems to make the governance process more efficient and effective.

Conclusion

EUDA governance is a key aspect of risk management in financial institutions. The increase in usage of RPA and low-code reporting tools has resulted in an increase in EUDA risks, as the number of shadow IT applications increases and leads to less oversight. EUDA risks paired with regulatory scrutiny can have a severe financial and reputational impact. By developing an organised, sustainable and closely monitored EUDA environment, institutions can manage these risks, address regulators' concerns and minimise exposure to losses while reaping the benefits of EUDAs, including efficiencies in modelling and financial, management and regulatory reporting.

About Protiviti's Technology Consulting Solutions for Financial Services

Protiviti's Technology Consulting services include cloud and emerging technologies strategy, transformation and security, data strategy and governance, development, design and implementation of advanced analytics, enterprise application implementation, cybersecurity and data privacy assessment, development and implementation, risk management, and managed services. Protiviti's global financial services industry practice has served more than 75% of the world's largest banks and many of the largest and mid-sized brokerage and asset management firms, as well as a significant majority of life, property and casualty insurers. The FSI practice provides support to teams across Protiviti's portfolio of solutions, including regulatory compliance, risk management, internal audit, technology, cybersecurity, data privacy and sustainability.

Contacts

David Kissane
Managing Director
Technology Consulting
Protiviti – Sydney
david.kissane@protiviti.com.au

Mark Burgess
Managing Director
Risk & Compliance
Protiviti – Sydney
mark.burgess@protiviti.com.au

Acknowledgments: Protiviti Senior Manager Alejandro Pedroza contributed extensively to this paper.