International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

# Identification and Governance of End User Computing Applications Impacting the Integrity of CCAR/DFAST Stress Testing Reporting in Banks

**Samej Wakode**

Department of Management Studies, Jamnalal Bajaj Institute of Management Studies, Mumbai, India
Email: *samej20wakode[at]gmail.com*

**Abstract:** ***EUC (End-User Computing) applications are an integral part in complementing various critical processes in financial institutions. One of the vital section where it has presence is to support compliance-driven reports related to stress testing; Comprehensive Capital Analysis and Review (CCAR) and Dodd-Frank Act Stress Testing (DFAST). Although End-User Computing tools contribute to improve operational efficiency and adaptability, their inherent lack of standardization, insufficient controls, and reliance on manual processes pose considerable exposures to the integrity, accuracy, and compliance-driven compliance of stress testing submissions. This research paper investigates the identification, exposure assessment, and governance of End-User Computing tools that influence CCAR/DFAST reporting. The study emphasizes: 1) Challenges in End-User Computing tools management and remediation such as undocumented logic, issues with version control, and exposures to information integrity 2) Regulatory implications such as potential for non-compliance with CCAR, DFAST [1], SR 11-7 (Model Risk Management)[2], and BCBS 239 (Risk Data Aggregation) standards due to unregulated End-User Computing tools 3) A Structured governance framework suggesting best practices for managing inventories, assessing exposures, validating controls, and automating processes to reduce End-User Computing applications related exposures. Methodologically, the paper integrates research related to End-User Computing tools in CCAR/DFAST reporting, compliance-driven guidelines from the Federal Reserve, OCC, and Basel Committee, Industry best practices from financial institutions that have effectively established End-User Computing tools governance programs. Key findings indicate that financial institutions should maintain a centralized inventory of End-User Computing tools [3] with exposure-based classifications, implement automated controls (such as formula checks and input validation), enforce diligent Change management and independent model validation, Utilize End-User Computing tools remediation and management tools (like Xceptor, Appian, ClusterSeven and Apparity) for effective automation and monitoring. The paper concludes with actionable recommendations for financial institutions to enhance End-User Computing tools governance, thereby ensuring information accuracy, auditability, and compliance with regulations in CCAR/DFAST submissions.***

**Keywords:** EUC (End-User Computing), Stress testing, Comprehensive Capital Analysis and Review (CCAR), Dodd-Frank Act Stress Testing (DFAST, EUC identification and classification

## 1. Introduction

EUC (End-User Computing) applications/tools—including spreadsheets, access databases, macros, and customized scripts—are now fundamental for financial institutions to satisfy compliance-driven requirements for stress testing. Within frameworks of the Comprehensive Capital Analysis and Review (CCAR) and Dodd-Frank Act Stress Testing (DFAST), there is significant presence of End-User Computing tools in several vital processes. Few of them are:

- Data Aggregation and Processing: Gathering financial information from different sources.
- Model Input Preparation: Structuring and verifying inputs for stress testing models.
- Interim Computations: Conducting complex calculations between platforms.
- Reporting and Visualization: Creating reports for compliance-driven submission and internal management.

According to a Federal Reserve survey conducted in 2023, 78% of Category I-IV financial institutions utilize spreadsheets for certain aspects of the CCAR/DFAST workflow, with 43% using spreadsheets for calculations. This extensive use introduces operational and compliance-driven exposures that must be carefully managed.

### 1.1 Increasing Regulatory Oversight of End-User Computing tools

In recent years, regulators have intensified their attention on End-User Computing tools management as a part of comprehensive model exposure management. Such as-

- Federal Reserve SR 11-7: Identifies End-User Computing tools as models requiring formal oversight.
- OCC Bulletin 2020-75 [4]: Recognizes spreadsheet-related exposures within operational exposure management.
- Basel Committee BCBS 239: Calls for stringent controls over exposure information and its reporting.
- Dodd-Frank Section 165: Imposes strong control requirements for stress testing practices.

There have been several notable enforcement cases underscoring the effects of inadequate End-User Computing tools controls:

**Table 1:** Past use cases

| Bank | Year | Penalty | Primary EUC Issue |
|---|---|---|---|
| Citibank | 2020 | $400M | Spreadsheet errors in risk reporting |
| Goldman Sachs | 2023 | $7M | Miscalculating its risk weighted assets (RWAs) |
| Wells Fargo | 2021 | Consent Order | Material deficiencies in stress testing controls |

### 1.2 The Unique Challenges of End-User Computing tools Governance

End-User Computing tools governance poses specific issues that differentiate it from traditional IT governance [5]:

- Expansion: Spreadsheets often proliferate informally across departments
- Obscurity: Business rules may be hidden within complicated formulas
- Vulnerability: Files can become corrupted or fall victim to version mishaps
- Reliance: Key operations may depend heavily on a few expert users
- Changeability: Tools are updated frequently, often without following change management practices.

Deloitte's 2022 research revealed that only 32% of financial institutions maintained a complete inventory of End-User Computing tools for compliance-driven purposes, and only 18% conducted regular independent validations of these applications [6].

### 1.3 Research Objectives and Purpose

This study seeks to create a framework for pinpointing End-User Computing tools that significantly influence CCAR/DFAST information integrity, identification of EUCs, examine current compliance-driven requirements and enforcement trends for End-User Computing tools oversight, and suggest a governance model with controls standard.

The methodology integrates compliance-driven guidelines, disciplinary actions, compliance-driven frameworks and analysis of End-User Computing tools remediation and management tools. The research aims to help financial institutions align with compliance-driven expectations while enhancing the reliability of stress testing processes.

## 2. Methodology

The methodology is mainly classified into three categories: Identification of Critical End-User Computing tools in CCAR/DFAST Reporting, which includes methods of identification, Risk assessment by quantification of risk scores and Governance Framework for End-User Computing tools in Stress Testing.

### 2.1 Identification of Critical End-User Computing tools in CCAR/DFAST Reporting

#### 2.1.1 Methods for End-User Computing tools Identification

Banks are required to adopt structured techniques to identify EUC (End-User Computing) applications throughout the organization. Below are a few methods with which End-User Computing applications can be identified:

a) Automated Scanning Tools: File System Crawlers, like ClusterSeven and Apparity, can be used to locate financial spreadsheets within the organization. Network Drive Analysis can help to pinpoint collective repositories used by multiple users and metadata information evaluation can help to highlight files that are either highly complex or subject to frequent changes [7].

b) Business Process Mapping: Process walkthroughs can engage subject matter experts in process reviews and help to uncover End-User Computing tools used at critical junctures, Diagramming the information movement involved in compliance-driven reporting like CCAR/DFAST identifies potential End-User Computing touchpoints, Manual handoff identification where information is manually transferred, or interim calculations are made exposes additional exposure areas.

*c)* User Self-Reporting: Instituting processes that require reporting of compliance-driven tools ensures transparency, Business units need to periodically ask to confirm the End-User Computing tools in use, providing channels for anonymous reporting encourages the revelation of critical, previously unreported End-User Computing tools.

**Table 2:** Comparison of End-User Computing tools identification Approaches

| Method | Coverage | Effort | Limitations |
|---|---|---|---|
| Automated Scanning | High | Low | False positives, cloud storage gaps |
| Process Mapping | Medium | High | Dependent on SME availability |
| Self-Reporting | Low | Medium | Under-reporting risk |

#### 2.1.2 Inventory System Requirements

A robust centralized End-User Computing tools inventory should be maintained with the following details:

- Basic Metadata information: Details such as owner, storage location, and last edit date
- Functional Attributes: Information on the tool's objectives, information sources and outputs, and downstream effects
- Technical Specifications: Size, complexity indicators, and dependency mapping
- Risk Flags: Sensitivity indicators and compliance-driven significance.

### 2.2 Risk Assessment Framework for Critical End-User Computing tools

#### 2.2.1 Risk Scoring Methodology

A weighted evaluation model should be used as below:

**Table 3:** Evaluation model

| | |
|---|---|
| Impact (50%) | Having regulatory significance, especially with direct implications for CCAR/DFAST. |
| | EUCs having financial relevance, such as potential errors in capital reporting. |
| | And operational importance indicated by business process reliance. |
| Vulnerability (30%) | EUCs having degrees of complexity (e.g., embedded macros, external links). |
| | Also, the frequency of changes to the EUC. |
| Controls (20%) | Extent and accuracy of documentation. |
| | Access management. |

*Risk% and factors can be changed and updated.

#### 2.2.2 End-User Computing tools Tiered Classification Approach

End-User Computing tools should be sorted by their exposure score:


**Figure 1:** End-User Computing tools Risk Map

Tier 1 (Critical): Includes End-User Computing tools directly affecting CCAR/DFAST, characterized by high complexity (e.g., capital calculation workbooks); require comprehensive model governance.

Tier 2 (Material): Covers End-User Computing tools with indirect but meaningful impacts, such as information preprocessing tools; needs formal controls and scheduled reviews.

Tier 3 (Standard): Consists of lower-impact tools, like reporting templates; basic control measures suffice.

### 2.2.3 Assessment of End-User Computing tools functionalities

a) Structural Analysis
With the help of SME input or automated assessment, analyze below details:
Formula Complexity: Depth of formula nesting and use of advanced array logic
Linkages: Presence of external links and references
Stability: Detection of unstable elements like volatile functions or circular references
Performance: Evaluation of calculation times and resource demands

b) Data Flow Mapping
Crucial for understanding each End-User Computing tools reporting impact by information flow mapping:

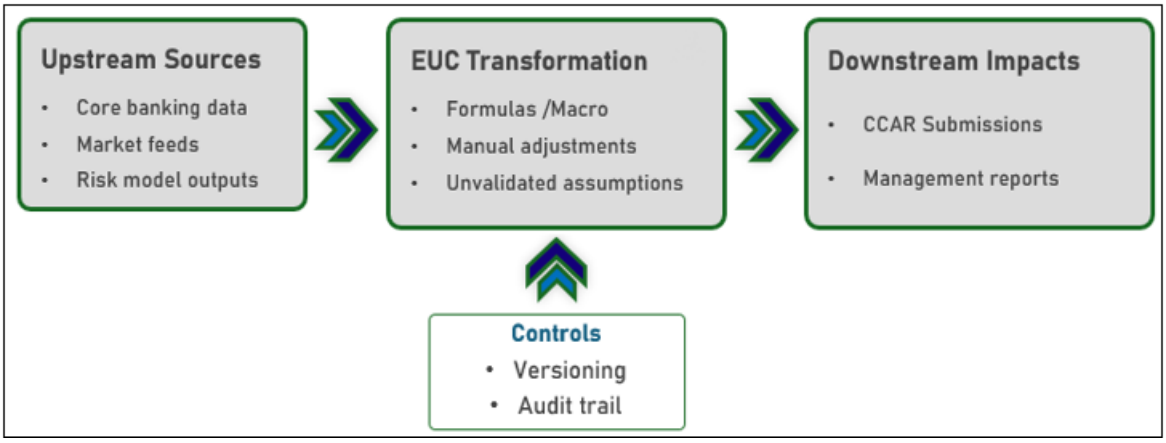


**Figure 2:** End-User Computing tools Data Lineage Diagram

Upstream Sources: Includes internal reporting systems, capital calculative models, & market data feeds
Transformation Processes: Documenting embedded business rules and assumptions, as well as manual interventions.
Downstream Outputs: Regulatory report generation, management summaries, capital planning steps.

### 2.2.4 Continuous Monitoring Mechanisms

Proactive monitoring is good to have but recommended to uphold the integrity of EUC (End-User Computing tools) throughout the Comprehensive Capital Analysis and Review (CCAR) and Dodd-Frank Act Stress Test (DFAST) processes. This can be achieved through the implementation of Automated Change Detection Systems aimed at identifying unauthorized or high-exposure alterations to critical End-User Computing tools. The integration of Additionally, a sample structured workflow for exceptional handling is necessary:

specialized tools such as ClusterSeven, Apparity, ControlPoint, is essential for real-time monitoring of file changes, tracking user access and modifications, and flagging any deviations from established change management protocols.

**Table 4:** Trigger type analysis.

| Trigger Type | Example | Alert Severity |
|---|---|---|
| Access Anomalies | Unapproved users modifying files | Very High |
| Structural Changes | Formula edits, macro modifications | High |
| Data Source Shifts | Broken links, new external connections | Medium |

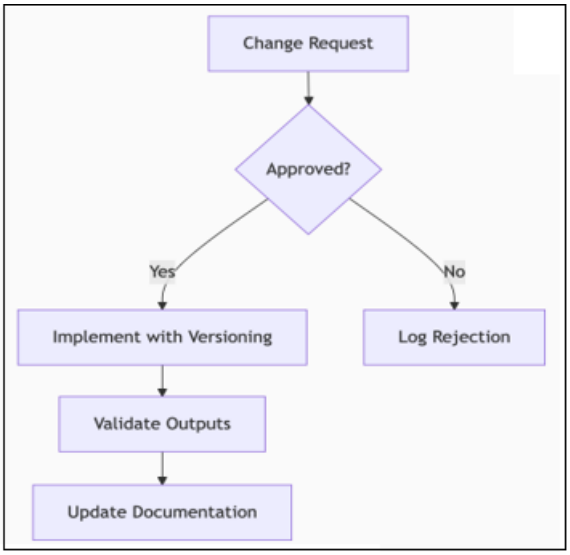


**Figure 3:** Exception flow

### 2.3 Governance Framework for End-User Computing tools in Stress Testing

This section presents a comprehensive governance framework designed to mitigate exposures associated with EUC (End-User Computing) applications in CCAR/DFAST processes. The framework addresses policy development, control implementation, and oversight mechanisms necessary to ensure information integrity and compliance-driven compliance [9].

#### 2.3.1 Policy Architecture

The foundation of effective End-User Computing tools governance lies in establishing robust policies that define acceptable use and management standards [9]. These policies must delineate scope parameters to encompass all End-User Computing tools involved in capital planning and stress testing workflows, Implement a tiered classification system based on materiality and exposure impact, Incorporate explicit prohibitions against high-exposure practices, particularly in Tier 1 applications, The policy framework should align with existing compliance-driven guidance, including: Federal Reserve SR 11-7 provisions for model exposure management, OCC Bulletin 2020-75 requirements for spreadsheet controls and Basel Committee BCBS 239 principles for exposure information aggregation.

#### 2.3.2 Control Matrix Implementation

An exposure-based control matrix ensures appropriate safeguards for each End-User Computing tools classification tier:

**Table 5:** Minimum Control Requirements by End-User Computing tools Classification Tier

| Control Category | Tier 1 Requirements | Tier 2 Requirements | Tier 3 Requirements |
|---|---|---|---|
| Change Management | Pre-approval by MRM team, Impact assessment for all modifications | Post-implementation review | Version tracking |
| Validation | Quarterly independent testing, Full replication by validation team | Annual owner attestation with sample testing | Ad hoc sampling |
| Access Controls | Dual (maker-checker) authentication, Role-based permissions with segregation of duties | Department-level restrictions | Basic user authentication |
| Documentation | Complete model documentation package including business rationale, technical specifications, Data lineage | Process flow diagrams with input/output mapping | Basic description |

#### 2.3.3 Organizational Governance Structure

The framework employs a three-lines-of-defense model to ensure comprehensive oversight:

**First Line**: Business unit owners responsible for:
- Daily operational controls
- Initial validation testing
- Change documentation

**Second Line**: Risk management functions performing:
- Quarterly challenge testing
- Control effectiveness assessments.
- Issue remediation tracking.

**Third Line**: Internal audit conducting:
- Annual independent reviews
- Policy compliance verification
- Regulatory examination support

#### 2.3.4 Compliance Documentation Standards

Banks must maintain comprehensive documentation demonstrating End-User Computing tools controls:
- Centralized Inventory System: Maintains metadata information for all stress testing End-User Computing tools including Ownership and responsibility assignments, Criticality classifications (Tier 1-3), Data lineage and system interdependencies.
- Validation Artifacts: For Tier 1 End-User Computing tools, financial institutions should preserve test methodologies and scenarios, Input/output verification

Furthermore, the integration with Model Risk Management (MRM) involves cross-functional collaboration for Tier 1 End-user Computing tools with the following processes: MRM review cycles occurring monthly for critical End-User Computing tools that affect capital ratios and quarterly for material End-User Computing tools that have indirect effects on CCAR, Validation protocols include independent testing by the MRM team on 10-15% of high-exposure End-User Computing applications and a review of assumptions to challenge manual inputs and Regulatory reporting must incorporate End-User Computing tools monitoring results in CCAR attestation packages and requests from the Office of the Comptroller of the Currency (OCC) and the Federal Reserve.

This all-encompassing identification and evaluation structure enables financial institutions to focus governance resources on those End-User Computing tools with the greatest exposure potential for CCAR/DFAST compliance, ensuring alignment with current compliance-driven demands.

records, Sensitivity analysis documentation, independent validation approvals, Materiality thresholds must be explicitly documented.
- Change Management Records: Chronological audit trails capturing change rationales and business justifications, impact assessments, authorization evidence, and historical versions covering multiple reporting cycles.

This framework provides financial institutions with a comprehensive methodology for maintaining continuous compliance while ensuring operational efficiency in End-User Computing tools governance. The structured approach balances rigorous documentation requirements with practical implementation processes to meet supervisory expectations.

## 3. Illustrative Implementation Roadmap

This section offers practical suggestions for financial institutions aiming to improve their End-User Computing tools governance frameworks impacting stress testing reporting, based on the empirical findings discussed in this research. The implementation roadmap covers technical, organizational, and compliance-driven aspects while outlining measurable success criteria.

Though multiple factors need to be considered before the actual figures arrive, the below can be referenced as an initial high-level estimation.

Banks should adopt a structured approach to End-User Computing tools governance that aligns with the annual CCAR/DFAST cycle.

### 3.1 Phase 1: Foundation Establishment

The initial phase is dedicated to establish the essential components necessary for effective End-User Computing tools governance. Banks should initiate this phase by conducting a comprehensive inventory of all End-User Computing tools involved in stress testing processes, employing automated scanning tools alongside manual validation from business units. This inventory must encompass vital metadata information, including ownership information, system interdependencies, and information lineage mappings pertinent to CCAR/DFAST reporting requirements.

Upon completing the inventory, institutions are required to conduct a detailed exposure assessment of the identified End-User Computing tools, utilizing materiality scoring criteria that reflect each application's influence on capital ratios and other significant stress testing outputs. This assessment must explicitly address compliance-driven implications, particularly focusing on FR Y-14 reporting timelines and SR 11-7 validation standards. The phase concludes with the implementation of essential controls for Tier 1 End-User Computing tools, which include version control systems, access management protocols, and formal change approval workflows designed to comply with compliance requirements.

### 3.2 Phase 2: Control Expansion and Automation

Building upon the established foundation, the following phase are concentrated on improving and automating controls within the stress testing End-User Computing tools environment. Institutions should prioritize the implementation of automated validation checks for critical information inputs and calculation outputs, with a specific focus on PPNR (Pre-provision Net Revenue) projections and loss estimation models. These automated controls should integrate reconciliation mechanisms that identify discrepancies surpassing established materiality thresholds.

Simultaneously, institutions ought to implement sophisticated monitoring capabilities that encompass real-time modification notifications and user behavior analytics specifically aligned with CCAR/DFAST submission timelines. These monitoring frameworks should seamlessly integrate with current governance, Risk, and compliance (GRC) platforms to deliver consolidated dashboards that track the effectiveness of controls. A thorough training initiative should be established alongside these technical improvements, featuring role-specific educational content for End-User Computing tools creators, validators, and business line managers engaged in stress testing activities.

### 3.3 Phase 3: Optimization and Integration

The concluding phase redirects attention towards establishing sustainable governance using predictive analytics and comprehensive compliance-driven integration. Institutions are encouraged to adopt machine learning methodologies to detect potential control violations or calculation discrepancies prior to their influence on stress testing outcomes. These sophisticated analytics should enhance robust documentation systems that automatically produce examination-ready packages linking End-User Computing tools to compliance-driven obligations.

Mechanisms for continuous improvement become ingrained within the institution during this phase, with ongoing benchmarking against peer practices and planned technology enhancements. The optimization initiatives should specifically target issues identified in earlier CCAR/DFAST cycles, with solutions aimed at minimizing manual interventions and enhancing information integrity.

### 3.4 Critical Success Factors

Three key elements are essential for successful implementation. Firstly, active executive sponsorship guarantees sufficient resources and organizational commitment. Secondly, proactive compliance-driven alignment, achieved through quarterly briefings and early remediation of potential findings, enhances supervisory confidence. Lastly, comprehensive change management strategies that involve all stakeholder groups—from senior leadership to frontline End-User Computing users to promote sustainable adoption of new governance practices.

This high-level roadmap offers financial institutions a clear strategy to evolve their End-User Computing tools governance from mere compliance to a strategic capability.

By adhering to this progressive approach, organizations can systematically tackle the distinct challenges presented by stress testing End-User Computing tools while fulfilling increased compliance-driven expectations. The implementation should remain adaptable to suit institution-specific conditions while keeping the primary objective of ensuring accurate and reliable CCAR/DFAST reporting.

## 4. Conclusion

Considering the thorough analysis provided throughout this study, financial institutions are encouraged to focus on three fundamental implementation principles for effective CCAR/DFAST stress testing reporting with minimizing exposure impact of End-User Computing tools. Firstly, it is essential to adopt an exposure-based strategy that focuses on the most impactful high exposure EUC (End-User Computing) applications impacting CCAR/DFAST compliance-driven reporting while ensuring adequate controls for those that are less critical. The tiered classification system outlined in Section 2.2 offers a validated approach for this prioritization. Secondly, it is important to invest in sustainable governance frameworks that persist beyond the initial implementation phase. This necessitates executive support, dedicated resources, and alignment with existing exposure management systems. The organizational models examined in Section 2.3 indicate that institutions with established governance committees tend to achieve more reliable outcomes. Thirdly, it is vital to cultivate a culture of compliance through ongoing training and well-defined accountability. The research indicates that institutions that integrate End-User Computing tools governance into performance metrics and job descriptions experience significantly higher compliance rates.

Financial institutions that adopt these recommendations can anticipate measurable advantages across three key areas. Regulatory compliance is expected to improve, with high-performing institutions achieving a significant reduction in manual errors, Operational efficiency improvements can be realized through process standardization and automation. Most notably, an exponential exposure reduction is feasible by addressing the frameworks mentioned in the paper.

Subsequent research should investigate the long-term effects of these practices and the changing function of EUC (End-User Computing) across different business units in progressively automated exposure management settings. Looking forward, emerging trends which are poised to influence future End-User Computing tools governance requirements are applications of artificial intelligence for automated monitoring demonstrate considerable potential based on pilot initiatives at leading institutions. Additionally, cross-border consistency in supervisory practices may simplify compliance with global financial institutions.

## References

[1] https://www.occ.treas.gov/publications-and-resources/forms/dodd-frank-act-stress-test/DFAST-14A-Template-Instructions.pdf
[2] https://www.federalreserve.gov/supervisionreg/srletters/sr1107a1.pdf
[3] Jamie Chambers, John Hamill, Controlling End User Computing Applications - a case study (2019)
[4] https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-132.html
[5] Naguib, H.M., Kassem, H.M. & Naem, A.EH.M.A. The impact of IT governance and data governance on financial and non-financial performance. Futur Bus J 10, 15 (2024). https://doi.org/10.1186/s43093-024-00300-0
[6] https://www2.deloitte.com/content/dam/insights/articles/US164678_CFS-banking-and-capital-markets-outlook/DI_CFS-banking-and-capital-markets-outlook.pdf
[7] Jamie Chambers and John Hamill, Controlling End User Computing Applications - a case study, ISBN: 978-905617 (2018)
[8] Dharmesh Dadbhawala, What Can Go Wrong with an EUCA? https://medium.com/@dharmesh_46873/what-can-go-wrong-with-an-euca-a50a1b5002ba
[9] Turner, Roger, Defining and Adopting an End User Computing Policy: A Case Study (2019)