BPA Policy 230-5

Internal Controls for End User Computing Tools

Table of Contents

1. Purpose & Background

This policy establishes internal control guidelines for computing tools developed by end users to support business processes at BPA.

While the need to develop process controls is always considered for tools developed under the IT Software Lifecycle (IT SLC) model, End User Computing Tools (EUCT) are implemented ad hoc by the general employee population, outside of the IT SLC. Examples of EUCTs include:

- Excel spreadsheets and Access databases;
- Enhancements to Microsoft products through Visual Basic for Applications;
- Code developed using scripting languages like R, or using numerical analysis packages like Matlab;
- Standalone or add-in risk analysis tools like @Risk; and
- Any non-IT developed tool, solution or application that is approved for use consistent with the BPA Approved Software List.

Law requires implementation of internal controls for business processes and data that affect BPA's financial reporting; notably, as implemented according to guidance given in OMB Circular A-123.

This policy requires implementation of internal controls for Critical EUCTs – those that materially affect business operational or compliance decisions, financial reporting, or the controls around financial reporting. Controls are instituted with the goal of preserving the quality of data used in, and produced by, these activities.

2. Policy Owner

The Executive Vice President of Compliance, Audit and Risk (EVP CAR) owns this policy. Agency Compliance and Governance (CG) has overall responsibility for monitoring, reporting, deploying, evaluating, interpreting, and proposing revisions to this policy.

3. Applicability

This policy applies when Critical End User Computing Tools are developed, deployed or used.

4. Terms & Definitions

A. **Controls:** Procedural monitoring and review tasks that help to minimize the risk of errors within an EUCT. *See section 2.4 of the procedure document for detailed types of controls.*

B. **Critical EUCT:** An End User Computing Tool used to produce data or other quantified information that have a significant or major influence on operational or compliance decisions, financial reporting, or the controls around financial reporting.

C. **End User Computing Tool (EUCT):** Computing applications developed outside of the IT SLC standard that allow users to directly manage, control, or manipulate data, inputs or outputs.

D. **IT System Lifecycle (IT SLC):** A formal process for planning, creating, testing, and deploying an information system. IT SLC processes and standards are developed by the Chief Technology Officer (CTO) and are maintained on the CTO's organizational intranet site.

E. **Federal Managers Financial Information Act (FMFIA) Attestation:** Annual attestation by the Administrator as to the state of internal controls over reporting, efficiency and effectiveness of operations and compliance with laws and regulations.

5. Policy

A. BPA management ensures Controls are in place for Critical End User Computing Tools.

B. Critical EUCTs are developed, deployed and used in accordance with standards and procedures contained in *BPA Procedure 230-4-1 Controls over Critical End User Computing Tools*.

6. Policy Exceptions

None

7. Responsibilities

A. **Managers and supervisors**

1. Implement controls for Critical EUCTs they, or their organizations, own that are used to inform operational decisions, and to report on operational, compliance and financial results.
2. Maintain an inventory of Critical EUCTs used within the business processes they own, and ensure appropriate controls are in place to mitigate identified risks surrounding their use.
3. Attest that controls are in place to mitigate risks surrounding the use of Critical EUCTs through the annual FMFIA process.

B. **Governance and Internal Controls (CGC)**

1. Sets standards and procedures for implementing this policy.
2. Gives advice on whether an EUCT is a Critical EUCT.

8. Standards & Procedures

See *BPA Procedure 230-4-1: Controls over Critical End User Computing Tools,* which lists and describes types of control and types of risk.

9. Performance & Monitoring

A. CGC manages Control requirements for Critical EUCTs related to financial reporting through annual certification of OMB Circular A-123, Appendix A processes.

B. Management protects the integrity of data developed in business processes they own, and used in determining financial statement transactions amounts, balances, or disclosures, by ensuring controls are in place, and are compliant with OMB Circular A-123, Appendix A.

C. The annual FMFIA attestation process monitors manager's areas of concern in efficiency and effectiveness of operations, compliance with laws, regulations and reporting, including Critical EUC tools.

10. Authorities & References

A. OMB Circular A-123, Appendix A

B. Federal Information Security Act (FISMA), https://www.dhs.gov/federal-information-security-management-act-fisma

C. NIST Cybersecurity Framework (National Institute of Standards and Technology), http://www.nist.gov/

D. BITA (BPA Information Technology Architecture)

E. InfoSec Program (BPA Information Security Program)

F. BPA Policy 230-5, Internal Controls Protocols and Actions

11. Review

Under Policy Program standards, this policy is scheduled for cross-agency review in 2022.

12. Revision History

Version Number	Issue Date	Brief Description of Change or Review
1.0	12 June 2017	Initial publication