The Ultimate End-User Computing (EUC) Checklist

Questions to guide your framework for identifying, quantifying, and managing end-user computing (EUC) risk.
In a world where employees leverage user-centered applications (like Excel, Access, Python, and other democratized tools), IT departments worry about encroaching risks — and for good reason.

**End-user computing (EUC) refers to any application supporting a critical process that is developed or managed by end users rather than an IT department or professional software engineering team.** And though they can be wildly useful in helping teams boost efficiency in their everyday work, they are seldom managed with the same governance protocols or security checks that IT departments maintain in their custom applications.

In today’s environment, it’s highly likely you’ll be asked about your EUC management program. But which answers do you need to have at the ready to confidently say, “I have an effective EUC policy in place?”

Not having the right controls (and evidence of those controls) could leave you – and your organization – exposed. You need to have a framework that enables you to classify different types of EUC risk, and then mitigate and manage them through a combination of controls and business decisions. For example, if an EUC is high risk and central to your organization’s bottom line, your IT department may want to sunset the EUC and implement a more formal, IT-owned business application. Other EUCs, however, may never justify a full application and so should remain subject to the right controls and the continuous evidencing of those controls.

The right EUC risk management strategy gives you visibility and evidence of the risks you run, allowing you to make informed decisions as you navigate a complex and ever-changing technology landscape.
END-USER COMPUTING FRAMEWORK & CHECKLIST

1. DEFINE IT – Categorize your company’s end-user computing risk based on business impact

Do you keep track of all of the EUCs you’re in charge of managing, and can you easily categorize them based on organizational impact?

There are four main categories of EUC risk – have you evaluated your applications with these categories in mind?

☐ FINANCIAL RISK

- **Data Accuracy and Loss**: Inaccurate or incomplete EUC data can result in financial miscalculations, potentially leading to financial losses or regulatory compliance issues.

- **Resource Utilization**: Inefficient use of resources, including hardware, software licenses, and personnel, can result in unnecessary expenses and inefficiencies.

- **Vendor or Supplier Risks**: Dependence on specific vendors or suppliers for EUC solutions can expose the organization to financial risk if these entities fail to deliver or experience financial instability.

☐ OPERATIONAL RISK

- **Downtime**: EUC system downtime can disrupt business operations, causing productivity losses and revenue reduction. Downtime can result from technical issues, software glitches, or cyberattacks, and causes issues with business continuity.

- **Service Level Agreements (SLAs)**: Failure to meet SLAs can result in penalties, contractual breaches, and damage to customer relations.

☐ REGULATORY RISK

- **Non-Compliance**: Failure to adhere to regulatory requirements, such as BCBS 239, SR 11-7, Solvency II, or industry-specific standards, can lead to legal penalties, fines, and reputational damage.

☐ REPUTATIONAL RISK

- **Negative Public Perception**: Any issues related to EUC, such as data breaches, system failures, or regulatory violations, can tarnish the organization’s reputation, leading to crashing share prices, executive churn, and difficulty gaining and keeping customers.

- **Customer Confidence**: EUC-related problems can erode customer confidence and loyalty, and rebuilding trust will require significant effort and resources, if it is even possible.

**KEEP IN MIND**: While companies have paid off financial losses in years, the impact of reputational loss can last generations. Any and every EUC risk can result in reputational loss – from data breaches to downtime to non-compliance – so it is critical that you take the time to recognize your risks and take steps to keep them controlled.
2. CONTROL IT – Establish the controls you need to manage your EUCs

For any EUC falling under your department’s purview (especially those categorized as high risk), you’ll need to ensure the proper responsibilities and appropriate controls – based on the risk level – are in place to document changes, maintain quality control, ensure continuous updates, etc.

PwC produced an early list of requirements to demonstrate spreadsheet control to meet the need for compliance with Sarbanes-Oxley legislation. The objectives defined during this intensive period of controls implementation have now become standard elements for later spreadsheet control projects initiated under many later regimes, such as MIFID 1&2, Dodd Frank, CCAR, OCC Model Risk, COSO 2013, PCAOB Alert 11, UK PRA, Basel II, Solvency 2 and NAIC model audit rules.

Some of these controls and objectives include:

- **Change control**: All changes are highlighted and may be reported via dashboards, emails, or reports
- **Version control**: Automated version control for all files, even when they are updated by folder and name (e.g. /Jan/Report31.xls changing to /Feb/Report01/xls)
- **Access control**: Access to the file may be prevented at the file level
- **Input control**: All inputs can be monitored against definable tolerance levels; these may be absolute thresholds or relative to previous values
- **Security and Integrity of Data**: Cells/ranges/sheets and files may be protected to restrict access and thereby protect the data and formulas embedded in spreadsheets
- **Documentation**: Facilitates the preparation of documentation on the objectives and functions of the spreadsheet and ensures that it is maintained
- **Development lifecycle**: The full software development lifecycle is supported
- **Archiving**: Files may be archived according to corporate retention policies in a protected segregated location
- **Logic inspection**: Automated logic analysis on bulk inventories or individual files for both cell- and VBA-based content
- **Segregation of duties**: Ownership procedures, multi-level sign-off, and more can be automated and subject to control
- **Audit control**: A complete risk assessment should be applied automatically to bulk inventories or individual files to expose poor spreadsheet practices that would lead to error or fraud

**HOT TIP**: Managing EUC with controls is not just good practice – it is regulated. From the perspective of the financial services industry, three pieces of regulation in particular – BCBS 239, Supervisory Guidance on Model Risk Management (SR11-7), and Solvency II – have set the stage both for specific EUCs control issues and for the wider expectations on data quality.
2. EVIDENCE IT - Have evidence of your controls, monitoring, and reporting in place

You may have a great EUC policy, but can you provide evidence that it’s in place and effective? Do you have a strategy for continuously monitoring your EUCs and sunsetting them as needed?

By understanding all of your EUCs, their costs, risks, and benefits, employers can determine whether an EUC ought to be further centralized and transformed into an IT-owned core business application, or whether it ought to remain in the hands of your business users. In both cases, full visibility into an EUC is necessary.

If someone comes asking questions about your EUC management program, are you prepared to supply evidence of:

- A full list of your EUCs in one central repository
- An analysis of the kinds of risk that each EUC may pose
- A discovery process for new EUC risk detection to ensure inventory completeness
- Regular updates to RUC management according to new regulations or technology changes
- Proper control implementation according to risk level
- An end-of-life plan for an EUC (Need more support on this topic? See our Decommissioning EUCs Guide)

Once you have these pieces of evidence ready to go, you are also prepared to provide strategic and financial counsel to your IT team. By identifying risks and understanding the business impact of your EUCs, your department is prepared to determine which EUCs should be left alone (monitoring aside) and which should be transformed into new business applications.

**Embed automated monitoring and reporting into your tech stack DNA via integrated EUC risk management technology for a more comprehensive risk inventory. See last page for more information.**

It may be time to streamline your EUC management, response, and reporting

While strategizing around EUC risk management, the number of items to account for can feel overwhelming. Not to mention, auditing and monitoring your EUC risk is not a point-in-time exercise – it has to be continuous.

Flexible, customizable technology can help you automate governance, scan files according to your EUC risk criteria in near real-time, and give your executives and stakeholders greater insights simultaneously.
ABOUT MITRATECH

Mitratech is a proven global technology partner for corporate legal, risk & compliance, and HR professionals seeking to maximize productivity, control expense, and mitigate risk by deepening operational alignment, increasing visibility, and spurring collaboration across their organization.

With Mitratech’s proven portfolio of end-to-end solutions, organizations worldwide are able to implement best practices and standardize processes across all lines of business to manage risk and ensure business continuity.

Mitratech serves over 10,000 organizations worldwide, spanning more than 160 countries.

For more info, visit: www.mitratech.com