MITRATECH

ClusterSeven Health Check

Trust is good. Transparency is better.

Many of your enterprise's most important business processes rely on spreadsheets, but they also can create *serious risk*.

Nearly 90%

of all spreadsheets have errors

1 in 5 large businesses

have suffered financial losses due to spreadsheet errors

43% of CFOs

do not know which spreadsheets in their enterprise are high risk

Known as the "London Whale" incident, spreadsheet errors cost J.P. Morgan Chase

over $6.5bn in losses and fines

source 1: https://www.forbes.com/sites/salesforce/2014/09/13/sorry-spreadsheet-errors/#30203b3356ab
source 2: https://www.businessinsider.com/stupid-spreadsheet-mistakes-could-lead-to-corporate-disaster-2015-4
source 3: https://fsn.co.uk/blog/cfos-how-do-you-stop-the-spreadsheet-spiral/
source 4: https://www.businessinsider.com/excel-partly-to-blame-for-trading-loss-2013-2

What's "Shadow IT" – and how does it put you at risk?

Many of your enterprise's vital business processes likely depend on applications developed and maintained by your business users. **Shadow IT** - the key applications, files, and assets spread across your enterprise which are hidden, outside of IT's control - are models, tools, calculators, and spreadsheets - with spreadsheets typically making up **70-80% of your End User Computing (EUC) estate**. Other highly used application types include Python®, R®, MatLab®, SAS®, Access DB and RPAs, and more.

The number of Shadow IT assets stored on your network or shared drives can run into **millions of files**. Identifying key files is an exhaustive process and it's just a start. Once you find these key files you then have to effectively triage them for both technical and material risk. Additionally, understanding and managing the risk they present to your organization is critical for preventing fines and maintaining compliance with regulations including **CCPA, GDPR, SR11 -7, Solvency II, SOX, SS3/18, Operational Resilience, SMCR/ BEAR, BCBS 239** and many more.

Gain control of your spreadsheets with a Health Check

By running a comprehensive Health Check using the ClusterSeven Shadow IT Manager, you can automate the discovery of those assets, learn how to risk-assess them, and then store them in an active inventory as part of your ongoing business-as-usual continuity process.

While it's good to trust in everyone's hard work and good intentions, it's better to control risk by having transparency for all the assets your enterprise depends upon.

An impossible task – *when done manually*

Uncovering the full extent and risk associated with these key EUCs within an organization is practically impossible if done manually, consuming huge amounts of labor and time. With our Health Check, you'll:

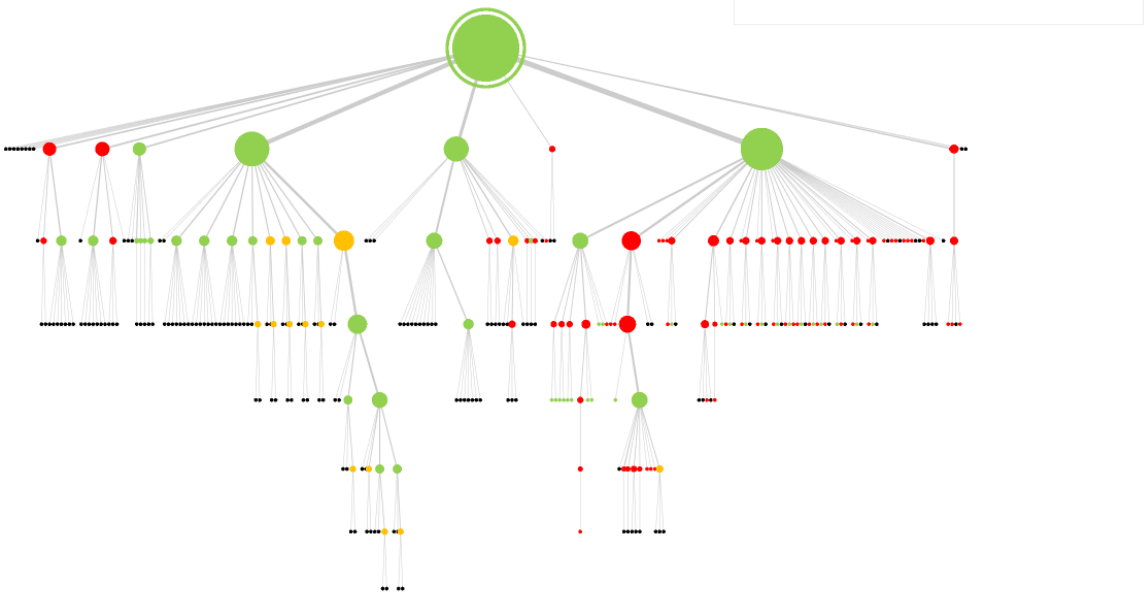
- **Automate** the discovery process to quickly uncover the "shadow IT" assets across your enterprise.
- **Risk assess** the spreadsheets and other file types for technical complexity and identify those to monitor as part of your Operational Resilience or CCPA program, for example.
- **Discover** how your EUCs connect with other EUCs and IT applications.
- **Rank and sort** the high-risk files for further triage in your initial inventory.
- **Automate** the version control processes over key EUC applications.
- **Prepare** your initial inventory for BAU (Business as Usual) where the business can decide which assets to archive, remediate, monitor or replace, going forward.

Even better, a Health Check does this non-disruptively and non-invasively even while operating throughout the EUC lifecycle. Each EUC now behaves more like an IT application with controls, risk management, priorities, and decommissioning programs

We bring unparalleled experience and technology to building your EUC inventory. It's both an art and a science, requiring qualitative and quantitative insights:

- **Quantitative insights:** file type, date of last use, size & location, technical complexity.
- **Qualitative insights:** a file's purpose, development methodology, documentation, review and approval processes.

Our platform's use of configurable and integrated components enables you to capture *both.*



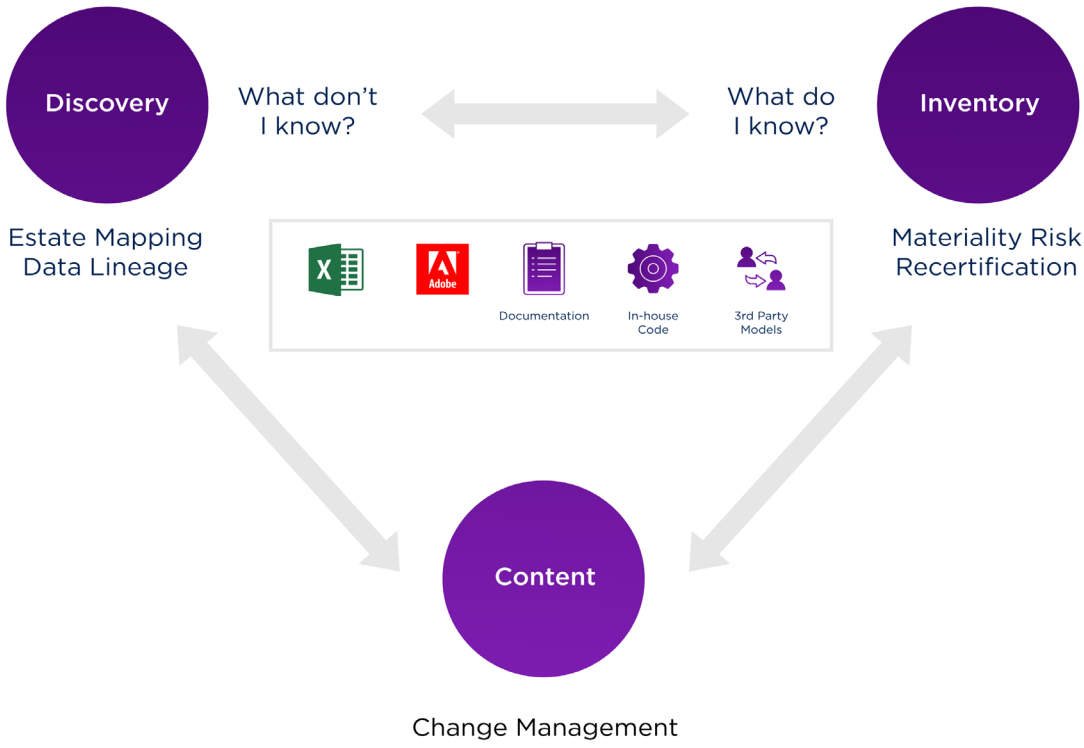
An intensive survey of your EUC risk landscape

Typical questions a Health Check will help you answer:

- How large and how complex is our Shadow IT / EUC estate?
- How many EUCs are being created per month? How many are being modified per month? How are they connected to other EUCs and IT applications?
- Which EUC is the highest risk to the business? Which one should I replace? Which ones should I monitor more closely for change? Which ones will the regulator review?
- How do we prioritize any required remediation effort?
- How can we confidently automate control and embed this in business-as-usual processes?

Satisfying the three key requirements of EUC Risk Management

Your Health Check will report tangible evidence about your EUC estate that can be shared with all stakeholders including management, IT, and risk & compliance teams while satisfying the three key requirements of EUC Risk Management:



The benefits of Health Check?

A Health Check is an investment in compliance and mitigation of potential risk arising from your "shadow IT" that will deliver an extensive range of benefits:

- The information governance value of obtaining an accurate EUC inventory.
- Visibility and risk analysis of the data supply chains and data lineage for key modeling, business, and financial processes.
- Improved efficiency and lower costs by reducing manual maintenance.
- Early insight into policy breaches including data access rights and data backup.
- Recognition if your unstructured shadow IT data assets present a GDPR, CCPA or PII data risk.
- Improvements in storage/retention costs and processes.
- Improvements to the reliability of spreadsheet-based ETL processes.
- Insights into where improved controls and further IT investment will provide longer-term benefits.

MITRATECH

Get in Touch

www.mitratech.com

info@mitratech.com