# 6 KEY CONSIDERATIONS
## FOR GOOD INSIDER RISK MANAGEMENT

### 01. Define your objective and be disciplined in its pursuit.

IRM includes many possible use cases. Start small with a few, discrete objectives. Prove the value of IRM with wins from the first objectives before expanding to additional use cases.

### 02. When in doubt, prioritize response.

Insider risk functions do not exist to identify incidents, but to address and close them. Lag in closing cases means backlog, which is itself a risk.

### 03. Technology matters – especially your sources.

Garbage in, garbage out. If you employ substandard technology to detect events, your potential is limited. If you must choose, prioritize your spending (time or money) on obtaining and configuring the best data monitoring capabilities. Save the prioritization and collation (think SIEM, UEBA) spend for later.

### 04. Train your users and define “acceptable”.

We can’t assume that users know where and how they should share data. Define, publish, and train users on sanctioned collaboration tools, which you can point to during insider risk investigations.

### 05. Right-size IRM for your organization.

Not every organization can afford dedicated insider risk specialists and technology. That’s okay. Build an IRM program with the technology (an M365 E3 license can work) and people available. Set realistic objectives and escalation thresholds. Finally, gather metrics that demonstrate success. Successful programs become funded programs, so that shiny new IRM tool may come sooner than expected.

### 06. You don’t have to go it alone.

While building or evolving an IRM program is an eminently doable endeavor, it’s much easier when you have guidance and help from an expert partner.



info@kudelskisecurity.com | www.kudelskisecurity.com

KUDELSKI SECURITY