Engage ESM 4 Pillar Operational Resilience Methodology

> "Engage ESM and ServiceNow have been transformational. The ServiceNow platform now plays a key part in managing our operational risk and means we have a best practice approach centered around governance, risk and compliance."
>
> *- Key stakeholder in Financial Services*

Engage ESM's Operational Resilience Methodology operates across 4 main pillars, People, IT, Assets and Suppliers. Our methodology is based around a three-step process, we identify gaps, reduce risks of critical processes, and then measure and continually refine these based on outcomes.

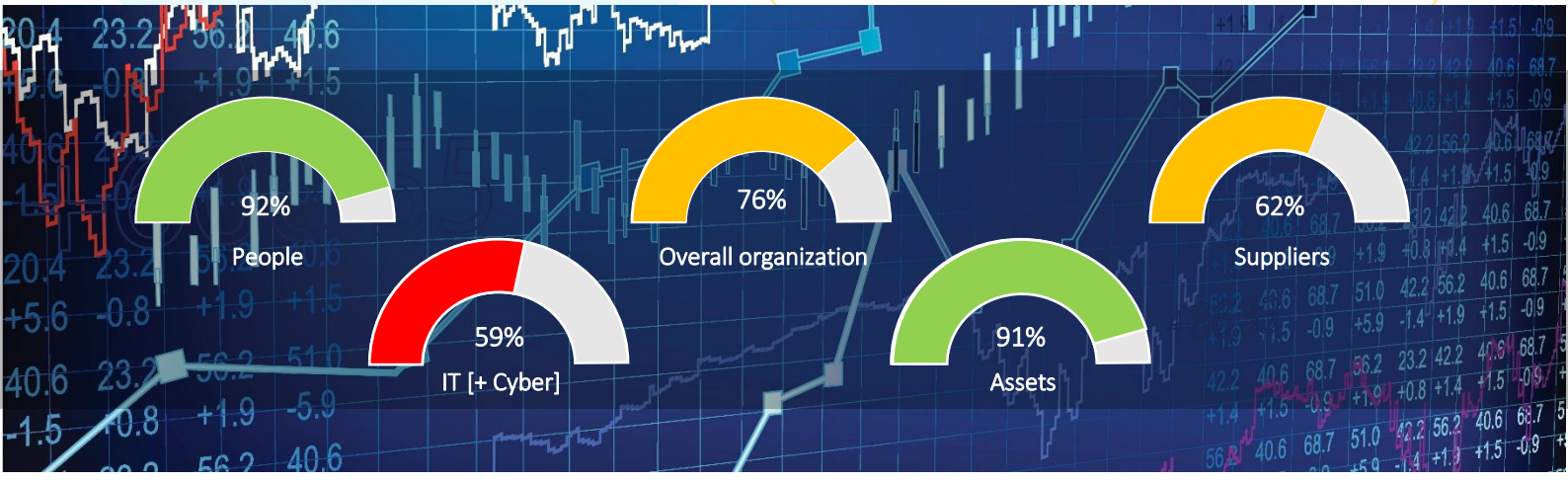
To achieve this, we leverage ServiceNow®, including the leading Governance, Risk and Compliance capabilities within the platform. Performance Analytics then provides the real time and predictive intelligence you need for enhanced metrics and increased visibility of your organization's performance and security.

Benefits

- Data-driven model that anticipates future demands, trends and threats
- Clear view of operational resiliency across lines of business
- Actionable insights are brought together in a single easy to understand dashboard
- Improved visibility allows you to be more strategic and respond more quickly
- Maintain sustainable competitive advantage
- Enables your organization to take a more proactive approach

What can you expect?

- Transform previously siloed and inefficient business processes into automated end-to-end workflows
- Performance analytics provides real time and predictive intelligence
- An approach centred around governance, risk and compliance
- Engage ESM 4 Pillar Methodology drives best-practice approach which aligns to current market drivers, frameworks and regulations



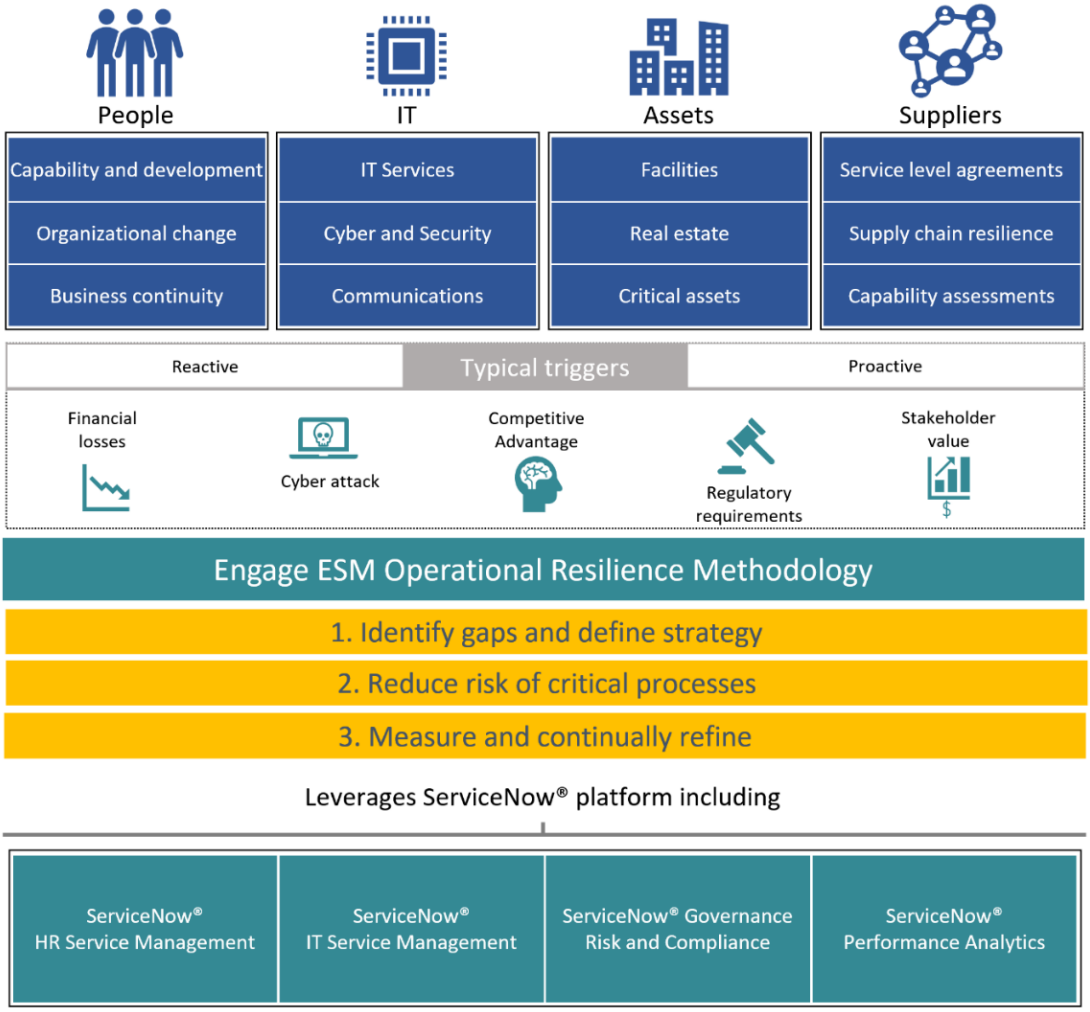
servicenow Partner Elite

www.engage-esm.com | info@engage-esm.com

servicenow Partner Elite

Engage ESM 4 Pillar Operational Resilience Methodology

Operational Resiliency is critical for maintaining stability and confidence across enterprise scale organizations globally. More than business continuity and disaster recovery, firms must have plans in place to deliver essential services, no matter what the cause of disruption is. These can range from man-made threats such as physical and cyber-attacks, to hazards such as fire, flood, severe weather and pandemic flu. Recent cyber-attacks have had global reach and caused significant collateral damage across numerous sectors, including financial services, entertainment and public services.



> "Firms and FMIs [need] to develop and improve response capabilities so that any wider impact of disruptive events is contained. The speed and effectiveness of communication with the people and institutions most affected, in particular customers, should be at the forefront of every firm's response."

-Building the UK financial sector's operational resilience, Bank of England. July 2018