A single view of Operational Resilience.
Now, wouldn’t that be nice?
See how connecting your teams on one platform will strengthen your response to disruption.
These are demanding times for Financial Institutions

1. Regulatory pressures
As a business, you need to satisfy the regulators that you are proactively identifying and managing risk—and are fully prepared to respond to potential incidents.
2. Customer expectations

Customers expect your services to be available 24/7, and their data to be securely managed at all times.
Today’s challenge for Operational Resilience

What we hear from Chief Operating Officers:

Our teams are facing different pressures around Operational Resilience—and they manage them in their own way using different processes and data.

Without a single clear picture, the business as a whole is reactive to failure, rather than proactive.
Today's challenge for Operational Resilience

Each business function plays an important role in Operational Resilience. But working in silos and reporting via spreadsheets means key information and actions can get lost in the gaps. Follow the links below to explore some of the different pressures and perspectives facing the C-suite today.

- Click to see the **Risk** perspective
- Click to see the **IT** perspective
- Click to see the **Finance** perspective
- Click to see the **HR** perspective
- Click to see the **Security** perspective
- Click to see the **Facilities** perspective
Chief Risk Officers are saying:

There’s GDPR and other legal duties to evidence, and we need to have the right governance in place so that we can quickly identify and respond to risks like supplier fraud.

Risk teams need to share resilience data points internally with the business and externally with regulators, including:

- Business service disruption
- External fraud and GDPR compliance
- Legal and regulatory obligations
Along with Financial Resilience, Finance teams can contribute to Operational Resilience by reporting on:

- Ability to get upfront funding
- Ongoing contractual issues
- Potential impact on finance systems

Chief Finance Officers are saying:

**Revenue and cashflow are critical to Operational Resilience. We need to keep a constant eye on ‘problem’ contracts and make sure that the business can access funding for new projects.**

Along with Financial Resilience, Finance teams can contribute to Operational Resilience by reporting on:
Chief Security Officers are saying:

We need clear visibility and consistent reporting from multiple systems, so that we can proactively respond to emerging threats.

Security teams play a critical role in Operational Resilience, providing data on:

- Supplier health and reliability
- Contract management
- Physical security exposure
- Infrastructure vulnerabilities and threats
- Onboarding and compliance
Chief Information Officers are saying:

There are new risks to manage as we move to the cloud and digitize via DevOps. But we also need to identify and address threats to existing services.

To help keep essential business services and systems running, IT has to report on many resilience data points:

- Digital design and change
- Secure service operations
- Hybrid cloud management
- DevOps orchestration
Chief People Officers are saying:

As employees and contractors join or move teams, we need to collect, request and collate data to ensure that people have the appropriate access and identity rights.

HR contributes to Operational Resilience by tracking anything that threatens people’s productivity and wellbeing—or that could damage the reputation of the organization:

- Identity and access rights
- Joiners, movers, leavers
- Resourcing skills and expertise
Chief Facilities Officers are saying:

We want an instant view on the strengths and weaknesses of our global sites. But getting the right data together and navigating geopolitical nuances is a challenge.

The physical workplace is critical to business operations, and Facilities teams have a lot to keep on top of:

- Geographic and political issues
- The health of the physical infrastructure
How Operational Resilience should feel for Financial Institutions

Our teams are connected, our workflows are joined up, and we have a central approach to governance. So now we can respond quickly and confidently whenever disruptions occur.
Tomorrow’s vision for Operational Resilience

When teams are working in a unified way, via joined-up workflows on one central platform, they can contribute far more effectively and proactively to Operational Resilience—as described below.

- **Risk** can be proactive in mitigating potential service impacts and compliance risks.
- **IT** can see the resilience of their applications and customer data.
- **HR** has good visibility on resourcing and retention risks, especially for niche skills.
- **Finance** can manage contractual issues and supply chain risk more effectively.
- **Security** can address both physical vulnerabilities and cyber threats, quickly.
- **Facilities** can focus on priority improvements to help maintain operations.
- **Chief Operating Officers** can see the health of all services and systems in one place.
Find out more about solutions by ServiceNow™ for the financial services industry by visiting: servicenow.com/solutions