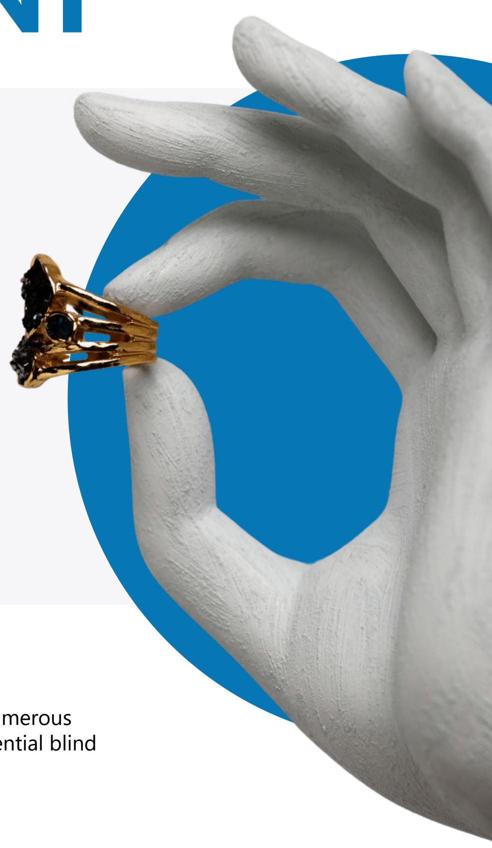
FACTSHEET

CROWN JEWELS ANALYSIS ENGAGEMENT

What Would Your Crown Jewels Analysis Reveal?



Most organisations have a good idea of what's important. Far fewer know exactly what would happen if those systems, services, or processes suddenly became unavailable.

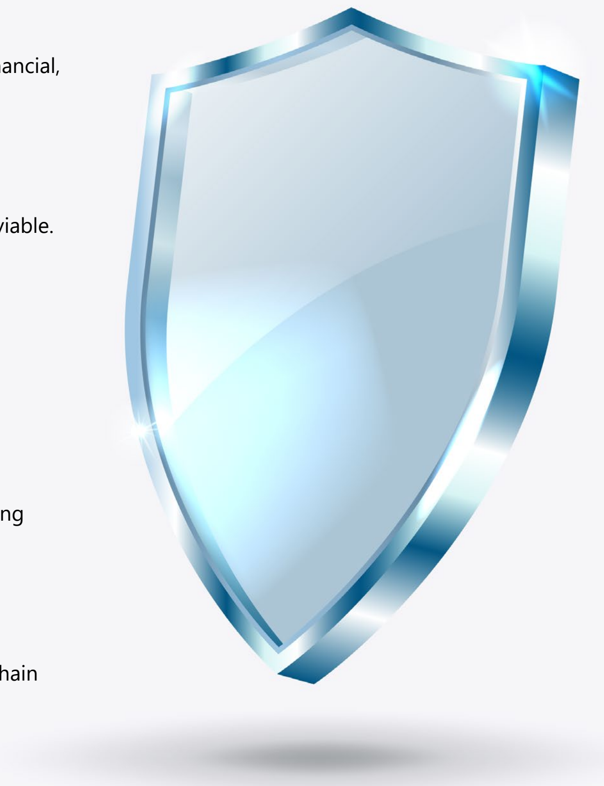
A Crown Jewels Analysis cuts through assumptions. It identifies the functions that keep your organisation running, measures the impact of disruption, and reveals how long the business can realistically operate without them.

The outcome is a practical framework for prioritising protection, recovery, and investment. Organisations gain the insight needed to focus recovery efforts where they'll have the greatest impact, build resilience into critical services, and get back to business faster when disruption occurs.

Conducting a Crown Jewels Analysis

Conducting a Crown Jewels Analysis involves several key steps and usually requires the involvement of numerous stakeholders across the business. Consulting with experts can provide valuable insights, help identify potential blind spots, and ensure that your analysis aligns with industry best practices and regulatory requirements.

The following steps outline the process:



1 Identify Critical Business Functions
Determine which processes are essential for operations and revenue generation. Examples include customer service, IT infrastructure, and supply chain management.

2 Assess the Impact of Disruptions
For each critical function, evaluate the potential effects of downtime, considering financial, operational, and reputational consequences.

3 Establish Maximum Tolerable Outage (MTO)
Confirm the maximum time allowed for an outage before the business becomes unviable. Knowing the MTO helps in setting realistic recovery objectives.

4 Establish Recovery Time Objectives (RTOs)
Set targets for how quickly business functions should be restored after a disruption.

5 Evaluate Resource Dependencies
Identify key personnel, IT systems, suppliers, and equipment necessary for maintaining operations. Understanding dependencies allows for contingency planning.

6 Develop Mitigation Strategies
Once risks and impacts are assessed, develop strategies such as alternative supply chain options, data backups, or emergency staffing plans.

7 Document and Update the Crown Jewels Analysis Regularly
A Crown Jewels Analysis is not a one-time process. Regular reviews ensure that new threats and changes in operations are considered.

How Littlefish can help

Littlefish offers comprehensive support to help enhance your resilience. Our approach includes:

Engagement with Key Stakeholders
Conduct workshops and interviews with executives, department heads, and technical leads to identify critical assets and gather input on what would disrupt business continuity the most.

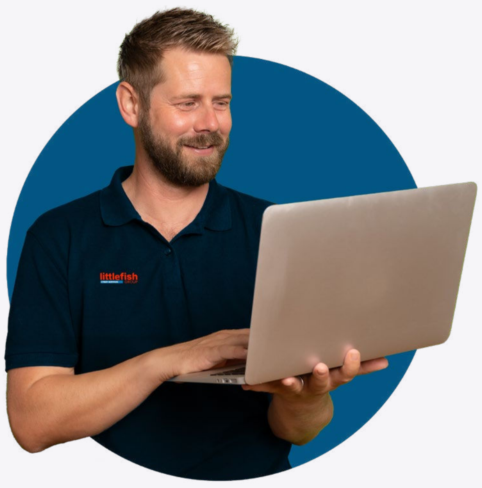
Determining Essential Business Functions
We work closely with your team to determine which processes are essential for operations and revenue generation, ensuring that all critical functions are identified.

Leveraging Industry Insight
Our experts bring industry knowledge and best practices to the table, helping you understand potential threats and vulnerabilities specific to your sector.

Identifying Specific Controls for Crown Jewels
We help you implement stronger security controls around your most critical assets, including end-to-end encryption, role-based access control, and multi-factor authentication.

Developing a Protection Strategy
We assist in establishing a comprehensive plan to protect your crown jewels, including updating your Incident Response Plan (IRP) and implementing continuous monitoring mechanisms.

Regular Reviews and Updates
We ensure that your Crown Jewels Analysis is regularly reviewed and updated to account for new threats and changes in operations.



The Littlefish Group difference

**Cyber security is often treated as a technology problem.
We see it as a business challenge.**

Littlefish combines deep cyber expertise with a practical understanding of business operations, helping organisations make better decisions about risk, resilience, and investment. We identify vulnerabilities, strengthen defences, and help teams prepare for disruption.

The result is a cyber strategy that aligns with business priorities, protects critical services, and gives leaders greater confidence in their ability to recover from the unexpected.