Technology implications of Operational Resilience Briefing

Presented by Justin Ward, Interim CIO Premia Group and
ICSR Talent Pool Member

Hosted by Kenneth Underhill, Implement Compliance Solutions & Resources

16th July 2020

Contents

What Is Operational Resilience?

ICSR
Implement Compliance Solutions & Resources

" The ability of firms and financial sector as whole to prevent, adapt, respond to, recover and learn from ops disruptions"

Important Business Services:
"All resources required to deliver that critical activity are then required to be operationally resilient."

(Kenneth Underhill: 4th June 2020 webinar – available on YouTube)

Resources……..?

Why is it so important to consider technology in your planning?

ICSR
Implement Compliance Solutions & Resources

July 2018 – Building the UK financial sector's operation resilience

FCA, PRA and Bank of England publish a Joint Discussion Paper (DP 01/18 or DP18/04). It is a response to an increasingly cyber-hostile environment and an increasing reliance on technology.

The stated aim of the regulators in 2018 was require senior management to build more resilience into their businesses by setting, monitoring and testing specific impact tolerances for key business services.

6 Key Ingredients of your Technology Operational Framework

ICSR
Implement Compliance Solutions & Resources

Know your IT estate (inside-out)

Create your technology framework

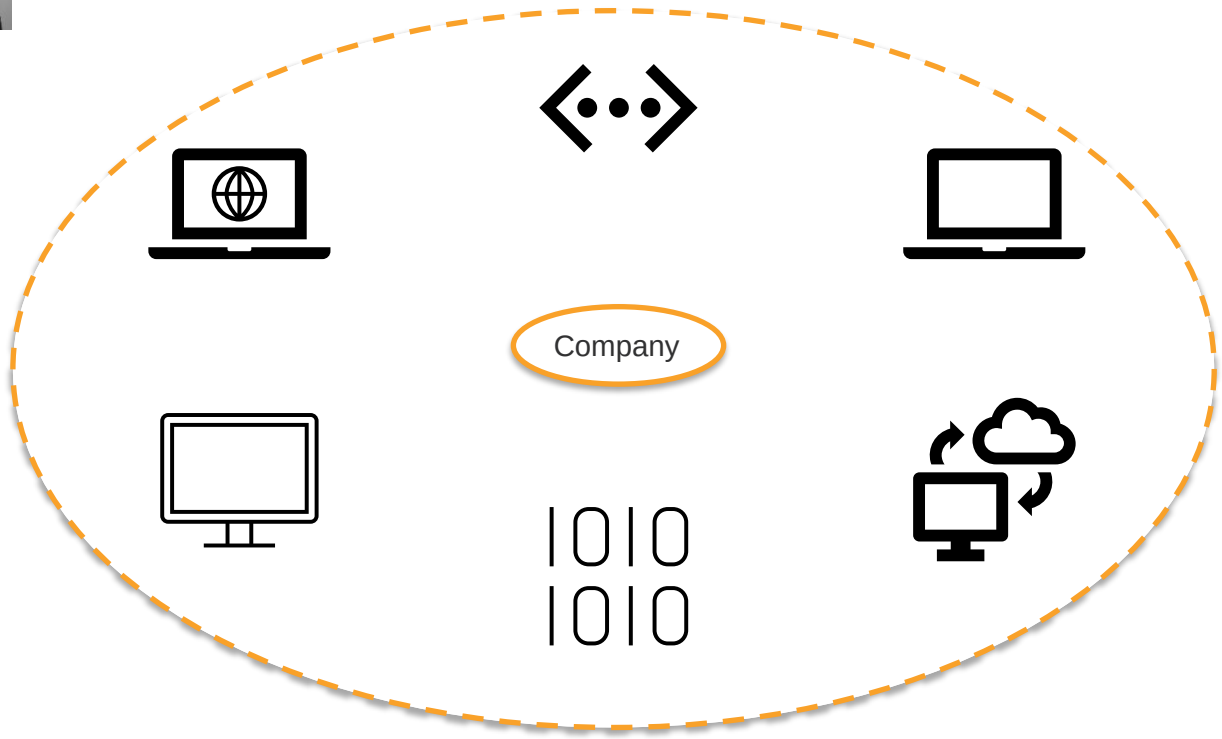
Have a tried & tested DR plan

Security is everything

Remote doesn't mean splendid isolation

Ensure everyone is involved

1. Knowing your IT estate inside out



- Which applications require support or upgrading to remain safe, simple and current is key
- Consider ‘end of life’ applications

Mopping up sins of the past and getting the basis right may be dull but is hugely important before moving onto the brilliance of the future.

2. Creating your technology framework

ICSR
Implement Compliance Solutions & Resources

Define your framework

- current, and understood
- Clearly defined
- Include levels of accountability

Important Business Services

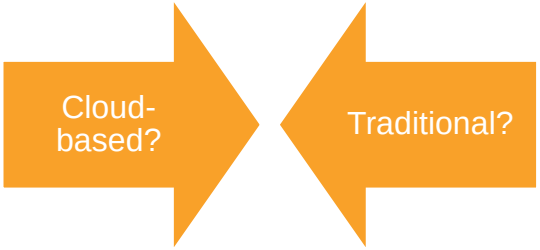
- Identify
- Impact tolerances
- Identify & document - people, processes, technology, facilities and information

3. Have a tried and tested Disaster Recovery Plan

ICSR
Implement Compliance Solutions & Resources

Technology keeps businesses running and ensures organisations return to a steady state once the disruption has ended.

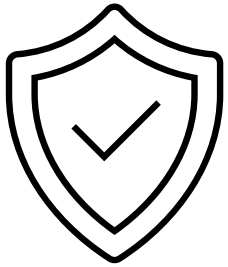
- Tools: BIA, Risk assessment and DR testing and even automated notifications as early warning systems

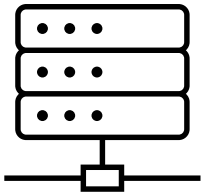


- Managed holistically- all staff should be involved. Everyone is in this together.

4. Ensure Security Is Everything

ICSR
Implement Compliance Solutions & Resources



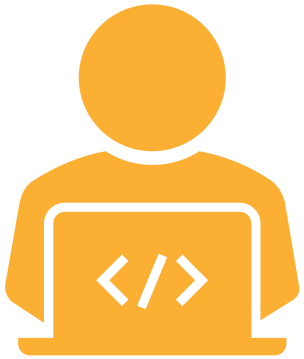


Crucial elements of your Cyber Security model should include:

- Data loss software
- Visibility and monitoring of the critical components of the ecosystem
- Privileged access management
- Patching and health checks and enhanced system monitoring
- Network containment
- Access and identity - leavers and joiners
- Service catalogue
- Security policy, governance and reporting

5.Remote shouldn’t mean splendid isolation

ICSR
Implement Compliance Solutions & Resources



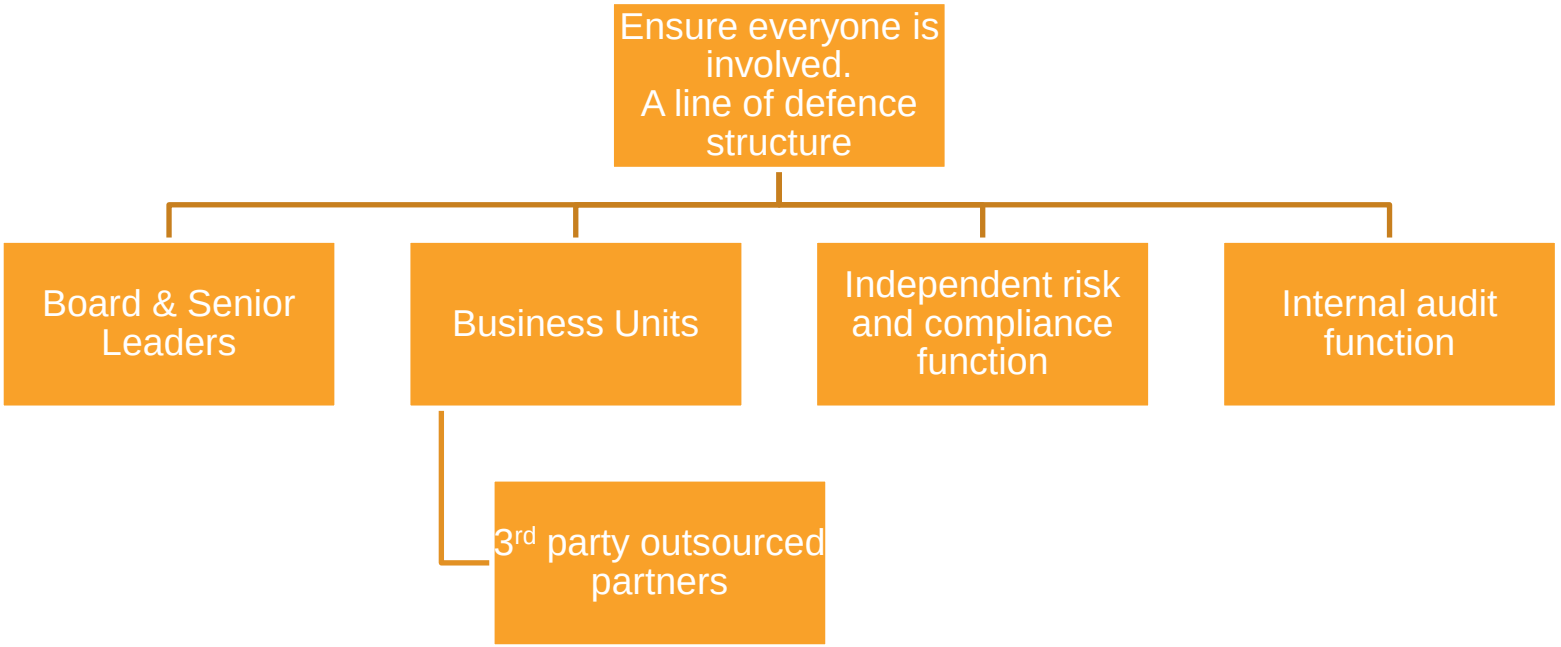
So having the right suite of collaboration tools is key:

- end point security
- encryption
- phishing
- version controlled
- audited as part of your planning
- Soft training: usability & security

Remote working will now be a long term option for most, with an 85% increase in overall productivity possible.

6. Everyone should be involved

ICSR
Implement Compliance Solutions & Resources



Summary

- Planning may sound daunting but making your business resilient shouldn't be daunting.
- Work incrementally- know what you can achieve and by when.
- Divide approach into manageable bite sized
- Your business continuity plan should be at the centre of your organisation
- Independent scrutiny and analysis is key

"understand your vulnerabilities, invest in protecting those and protecting yourselves, consumers and the market."

Megan Butler, FCA Executive Director of Supervision – Investment, Wholesale and Specialists
5th December 2019
https://www.fca.org.uk/news/speeches/view-regulator-operational-resilience

ICSR
Implement Compliance Solutions & Resources

Questions?

ICSR
Implement Compliance Solutions & Resources

About Justin Ward

Justin is a senior Technology and Operations consultant, having most recently operated as CIO for a major global Insurer. He has a background in Board Level strategy and delivery and has led a number of high profile global transformational change programmes. These include crisis management, modernising technology and claims estates and improving syndicate dealings with Lloyd's. A technology expert, his specialism is in building emerging and digital technology. He is passionate about delivering sustainable customer led propositions. Claims Transformation on a global scale is another area of expertise.

www.icsr.co.uk/our-team/justin-ward-consultant/

This presentation is the work of Justin Ward, ICSR Talent Pool Member. Please address any questions to Justin Ward or to Kenneth Underhill, Director of ICSR.