Engage, Educate, Empower

Privacy Risks In Your Supply Chain and Identifying Hidden Vulnerabilities
(not just the technical ones!)

Mark Logsdon - CISO NHS England
Ray Stanton – CISO/CRO/NED & CISO/CRO Redwood Technologies Group

Purpose of our session today

1 Our view of challenges for Information Security & Data Protection in Supply Chains

2 Share recent global trends & perspectives, dynamics

3 Give insight into case study of how NHS handles this area

4 Share anecdotes and experience(s)

5 Give our top tips & questions to go ‘home’ and ask

6 Have a few laughs, smile and make new friends ☺

First a little about Mark

1 Chief Information Security Officer at NHS England. Responsible for 9 CNI systems

2 Previously held senior, global roles, in the City, Barclays and the Prudential

3 Leads & creates risk and delivery focussed teams that are diverse. Pragmatic, timely, expert, actionable advice.

4 I take great pride in seeing my team grow and develop collectively and as individuals.

5 Formally Royal Navy, (Submarine Service) and Army (missionary work!!)

6 A member and former chair of the White Hat Ball Committee, raised close to £3m for NSPCC Childline

A little about Ray

1 Held/holds roles as NED, Board Advisor, Charity Board founder & fundraiser (White Hat Ball)

2 Nine years in British Armed Forces (Army)

3 Held CSO, CiSO, CRO & senior security roles Airbus, BT, National Grid, TDC Group

4 Married and 24-year-old daughter

5 Previous ISF Advisory Board member, WEF advisory, BoE advisor, among others

6 New golf enthusiast, lapsed rugby player (yes!), health nut, wine collector & cat lover

The problem we face and see, are challenges everywhere!

Too much to do

- □ Managing stakeholders
- □ Nail third-party risk
- □ Manage privacy office
- □ Respond to legislators & external auditors
- □ Updating CEO & board
- □ Budget management
- □ Input security content for vendor's contracts
- □ Make progress on your never-ending identity project
- □ Deliver your project list
- □ Communication calendar
- □ Manage the risk rankings & security roadmaps
- □ Provide SLDC testing protocol
- □ Encryption direction
- □ Provide data handling best practices
- □ Help with Mergers & Acquisitions
- □ Share best practice
- □ Review logs for fraud & ongoing investigations
- □ Help with insider threat discovery
- □ Determine location of sensitive data in the cloud
- □ Investigate possible infection on legacy system
- □ Continue pen testing of new business mobile apps
- □ Help architects understand zero-trust
- □ Answer security policy emails indiscretions
- □ Work with recruiters on staffing
- □ Deliver test plan requirements for new products
- □ And everything else under the sun…..

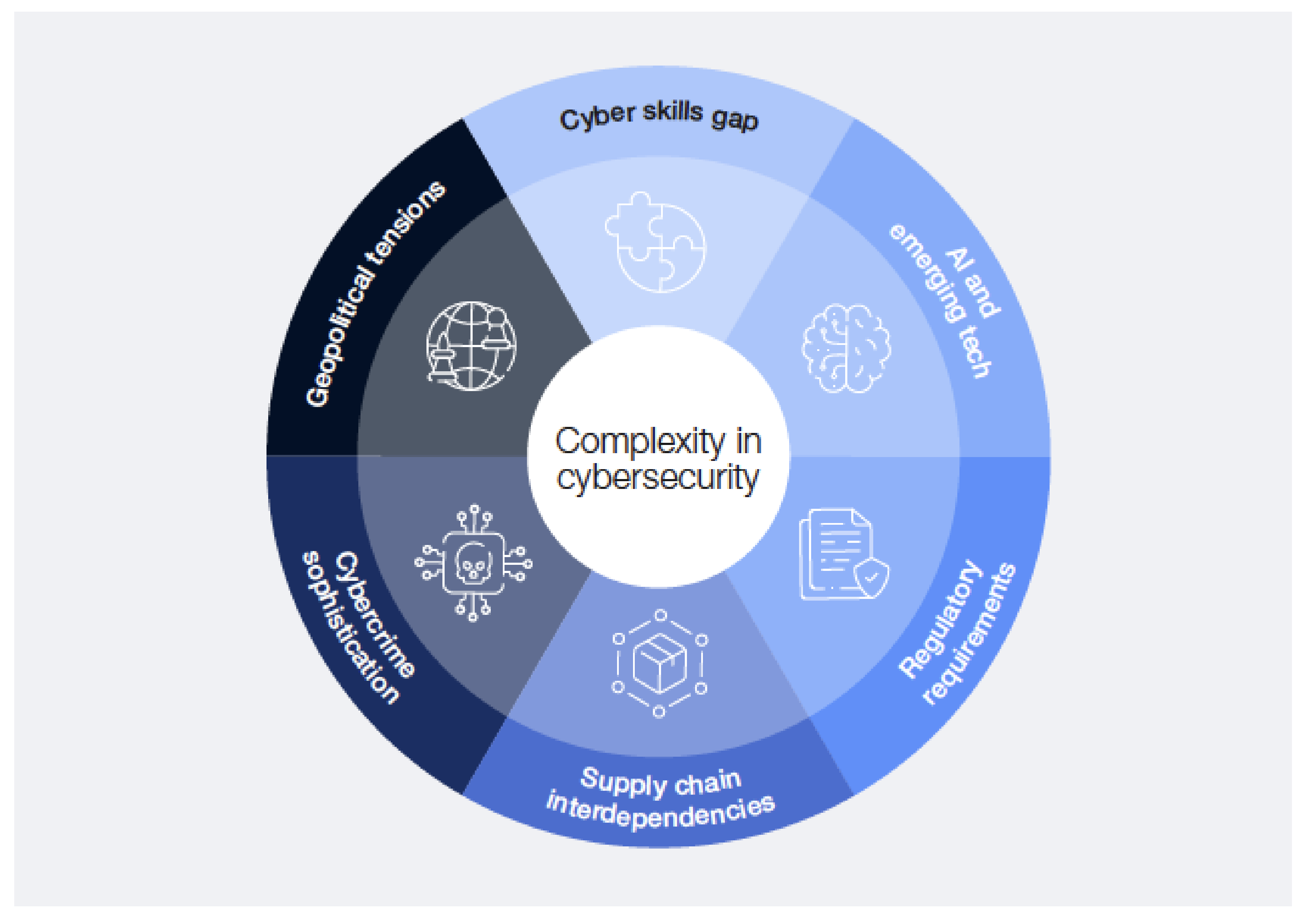
Too many vendors

Too much complexity

Too many regulations

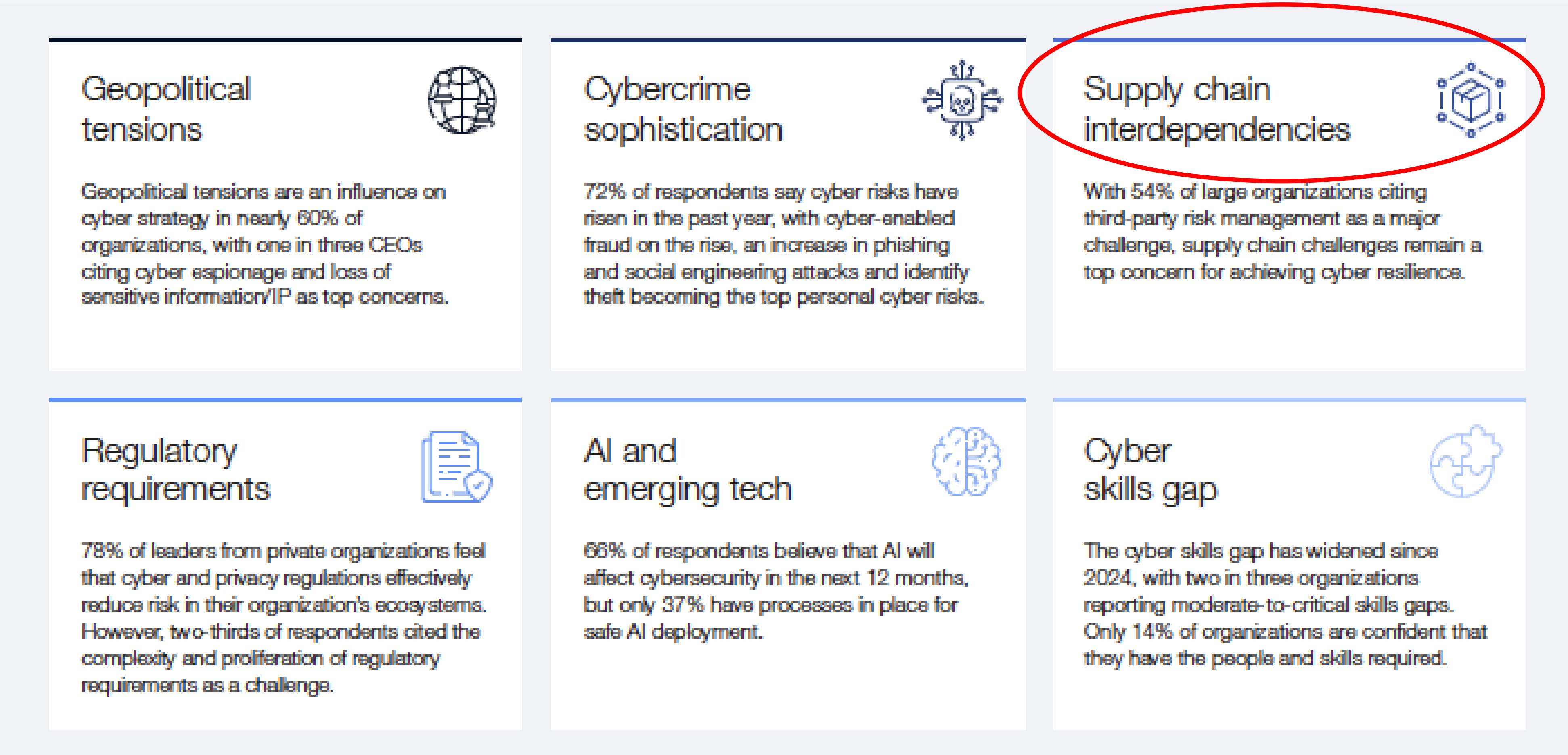
© 2025 RJMS Services Ltd

Factors compounding the complex nature of cybersecurity


Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions
Complexity in cybersecurity

WEF Global Cybersecurity Outlook 2025

Cybersecurity is (becoming) increasingly complex



Geopolitical tensions

Geopolitical tensions are an influence on cyber strategy in nearly 60% of organizations, with one in three CEOs citing cyber espionage and loss of sensitive information/IP as top concerns.

Cybercrime sophistication

72% of respondents say cyber risks have risen in the past year, with cyber-enabled fraud on the rise, an increase in phishing and social engineering attacks and identify theft becoming the top personal cyber risks.

Supply chain interdependencies

With 54% of large organizations citing third-party risk management as a major challenge, supply chain challenges remain a top concern for achieving cyber resilience.

Regulatory requirements

78% of leaders from private organizations feel that cyber and privacy regulations effectively reduce risk in their organization's ecosystems. However, two-thirds of respondents cited the complexity and proliferation of regulatory requirements as a challenge.

AI and emerging tech

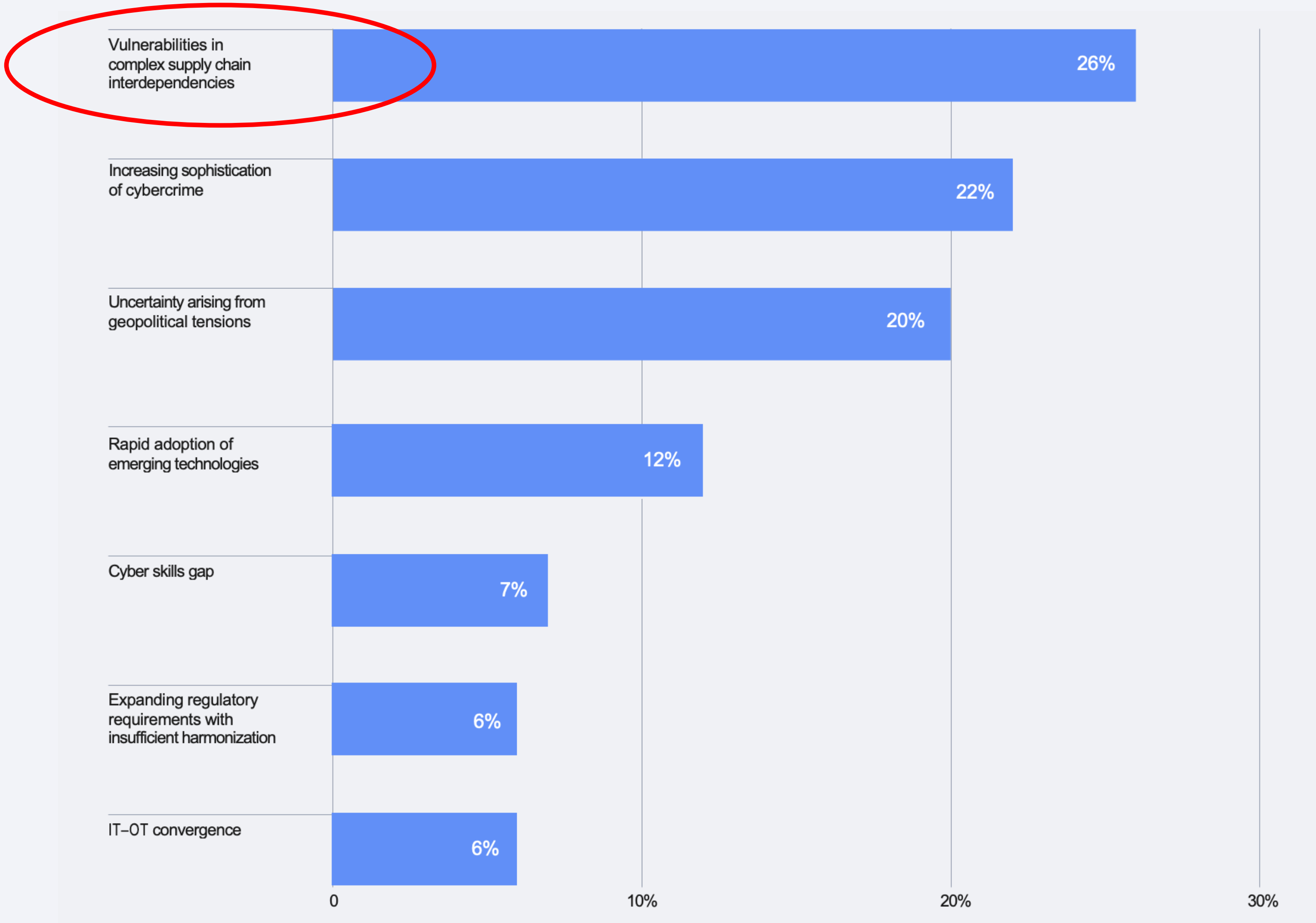
66% of respondents believe that AI will affect cybersecurity in the next 12 months, but only 37% have processes in place for safe AI deployment.

Cyber skills gap

The cyber skills gap has widened since 2024, with two in three organizations reporting moderate-to-critical skills gaps. Only 14% of organizations are confident that they have the people and skills required.

WEF Global Cybersecurity Outlook 2025

Challenges to organizations posed by cybersecurity threats – top remains supply chain risk



WEF Global Cybersecurity Outlook 2025

Now to Mark and how the NHS England deals with this/these challenge(s)

Third Party Risk Management (TPRM)

Presented by:
Mark Logsdon, Chief Information Security Officer, NHS England

National Cyber Services delivered by NHSE:

- **24/7 National Cyber Monitoring** (1.8m devices)
- **Secure Boundary**
  - Bitsight **risk measurement**
  - **Vulnerability Management Service**
- **Cyber Training** for Boards, and cyber training platform for all NHS Staff
- **Technical Support** (Backup reviews and tech remediation)
- **Cyber Assurance Service**
  - **Data Security Protection Toolkit**
- **Simulated Phishing** service
- **Cyber Associates Network**
- **Cyber Executive Network**
  - Critical **IT Vulnerability Alerts**

Cyber Operations in NHS England

Who we are

Cyber Operations purpose is to support safe care and build public trust by building NHS England's cyber resilience and enabling the wider health system to be cyber resilient, supporting the Transformation Directorates purpose of delivering the best care and outcomes for NHS England. Under the legal direction of the Secretary of State, the Data Security Centre is mandated to provide cyber services to the Health and Social Care System, regulated by the National CISO

Our Mission

Cyber Operations **delivers consistent, efficient, proportionate security oversight and support to NHS England and supports the Health and Care System become cyber resilient**. We **provide centralised advice, controls and security services** and ensure individual security responsibilities across NHS England are discharged effectively in line with the Board's Risk Appetite. We support data, system and security risk owners in supporting and their services securely. Where it is logical to provide a service centrally for effectiveness or efficiency, we deliver centralised security services and fill the gaps where a secure by design approach fails to deliver effective security at a local level

Our Vision

In line with the National Strategy to deliver a cyber resilient Health and Care sector by 2030, we support a vision of a cyber resilient NHS England, where security choices are evidence based and business enabling aligned to the agreed risk appetite

Our Objectives

- **Manage the security risk within NHS England**
- **Continually and strategically improve services and overarching risk**
- **Run security services for NHS England and the system to continually improve security risk**
- **Lead and enable improved cyber outcomes in NHS England and the system**

Our Budget and Headcount

- It costs **£54 million** to run Cyber Operations in NHSE each year (Staff and Systems)
- **229 people** scheduled to work for us by the end of April 2024
- **£250 million Cyber Improvement Programme** for the NHS in England underway

Internal security

100
Security Champions

Across NHS Digital we have 100 security champions who are actively engaged. They act as ambassadors within their teams and regularly take part in security activities

Data Security and Protection Toolkit

55k
submissions

Over 41,000 organisations submitted a DSPT return; the online self-assessment tool that allows organisations to measure their performance against the National Data Guardians standards

Incident volumes

300%
rise in cyber incidents

Since 2019 there has been a 300% rise in incident volumes; requirement to scale-up and increase automation

Cyber Associates Network

2100
CAN members

Peer to peer network aimed at improving cyber security across health and social care. Giving opportunities to discuss key issues in a safe space and learn from each other

High severity alerts

15
High severity alerts

A 54% increase on the previous year's high severity alerts. These are cyber security alerts that require immediate action to prevent damage to the network

Protecting the NHS

23.2bn
transactions

Protection of 23.2 billion transactions over a five day period through NHS Secure Boundary

Protecting patients

6
Significant attacks

The cyber security operations centre prevented six significant ransomware attacks recently that could have severely impacted patient care and led to Trust level IT being unavailable for months

Security education

5k
downloads

Over 5000 downloads of security awareness materials from our Keep IT Confidential campaign. Topics include: social engineering, passwords, tailgating and be aware of what you share.

Devices protected

1.9m
devices enrolled

Devices enrolled onto Microsoft Defender for Endpoint which feeds directly into the cyber security operations centre enabling them to detect nefarious activity across the NHS network

Blocking malicious activity

21m
malicious items a month

On average CSOC blocks over 21 million items of malicious activity every month, Working directly with local team to respond to the cyber threats

Prevention

Multiple
Critical National Infrastructure

NHSE Exec are accountable for running multiple CNI systems, with Cyber Ops supporting work to ensure their resilience

Active defence

5m
transactions a week

We actively monitor and protect devices across the NHS and work directly with local teams in response to cyber threats

CISO Deliverables & Successes

GRC

Foundations

12 new Standards (& policy) on track for publication by March 25, with new processes for policy compliance & assurance to follow

Governance

Cyber Governance Board (CGB) & CISO Operational Group (COG) established, improving visibility & oversight, enabling engagement

Internal Audits

Established and embedded new, proactive processes to centrally coordinate cyber audits & related actions

Security Exposure Model

New methodology deployed to measure NHSE security posture and cyber risk position to enable a low-risk appetite

Secure

Programmes

FDP Live. PDM (Patient Data Manager) 1st in the UK to use AWS health lake.
One Digital Estate, New hospitals Programme & Digital heath check engaged. Single Patient Record initiated.

SbD

Principles embedding into Governance processes (TADA & DTAC)
On target for March 25

CCoE

Encryption on EDS & RDS data stores. S3 public buckets blocked, local IAM users blocked.

ECoE

Engineering Redlines adopted (e.g Immutable backups) & Cyber red lines agreed. IaC and SAST tools implemented.
CDDO Gen AI testing in flight (google Gemini & GitHub Co-pilot).

Threat Modelling

IriusRisk tool implemented

Modelling of Mission Critical Services underway (CIS2 & Spine Core)

Assure

c

Third Party Assurance

47 critical suppliers identified, 43 fully onboarded and 17 security reviews completed

Standardised Assurance Reviews

2 security reviews completed with 16 findings being remediated

Cabinet Office Departmental Security Health Check

First NHSE health check completed

Security Testing

92 tests completed

Business Partnering

100% of NHSE regions now covered in collaboration with cyber regional leads

Overseas Working Audit

121 investigations into working from red list countries

Risk Reduction

Accenture Sprint

- 11 aggregated risk themes established
- Remedial actions currently being prioritised
- Dashboards for centralised reporting being developed

CISO Resilience Programme

Strategy established; CRP absorbs Accenture outputs to build understanding of kdey risk themes and priority controls beyond the 15 Mission Critical Systems.

CISO PMDO Established

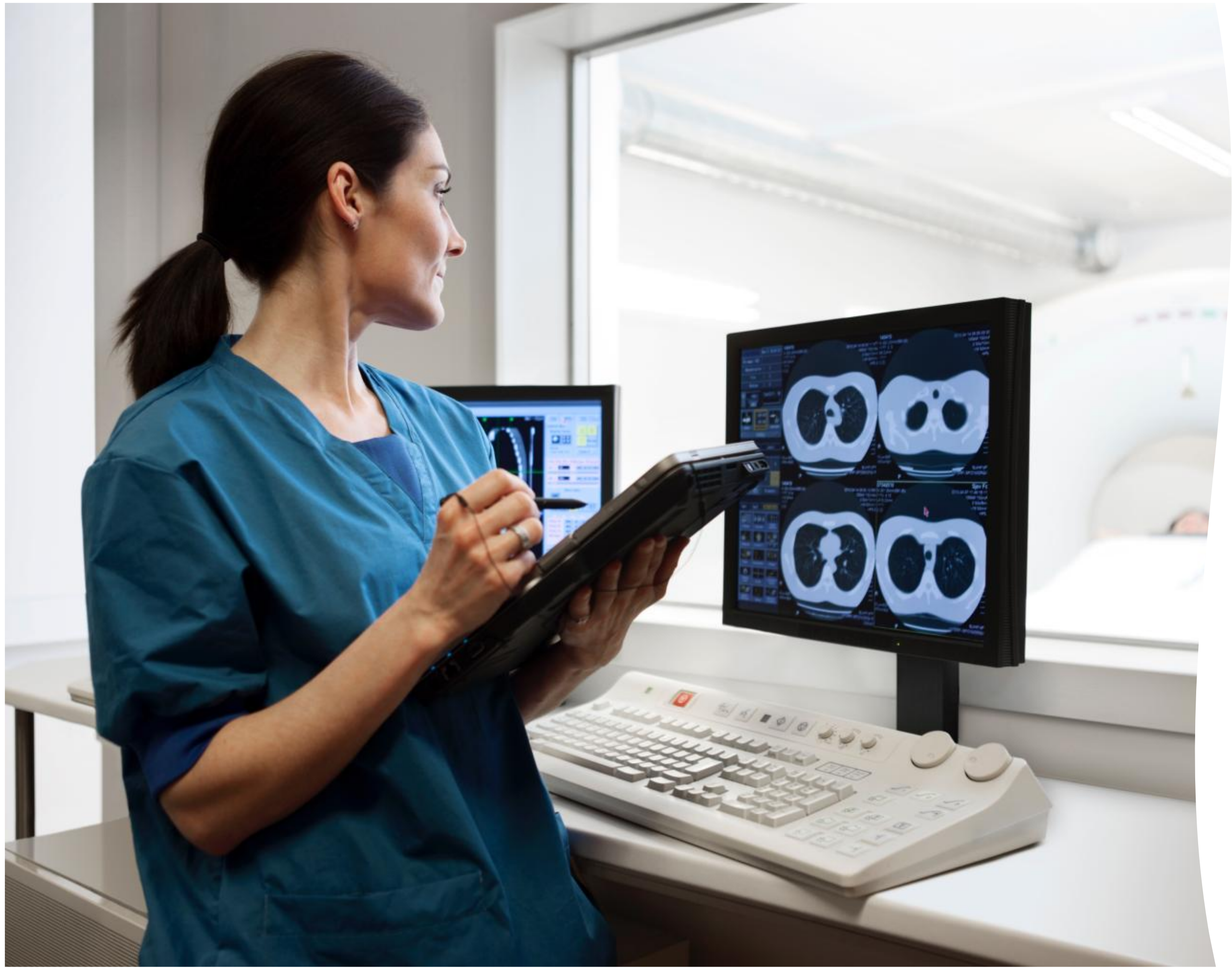
Project Management and Delivery Office formally transferred into the CISO area to support the CRP.

Emerging Risks

Quantum: NHSE enrolled in GCHQ-funded initiative to help understand how to discover and secure assets against the quantum threat.

Mission Critical Systems

- Driven the board commissioned work relating to a low cyber risk appetite, including:
- Completing **24** criticality assessments
- Identifying **15** Mission Critical systems
- Taking an active role in the current work to build a wider resilience programme and plan for remediations



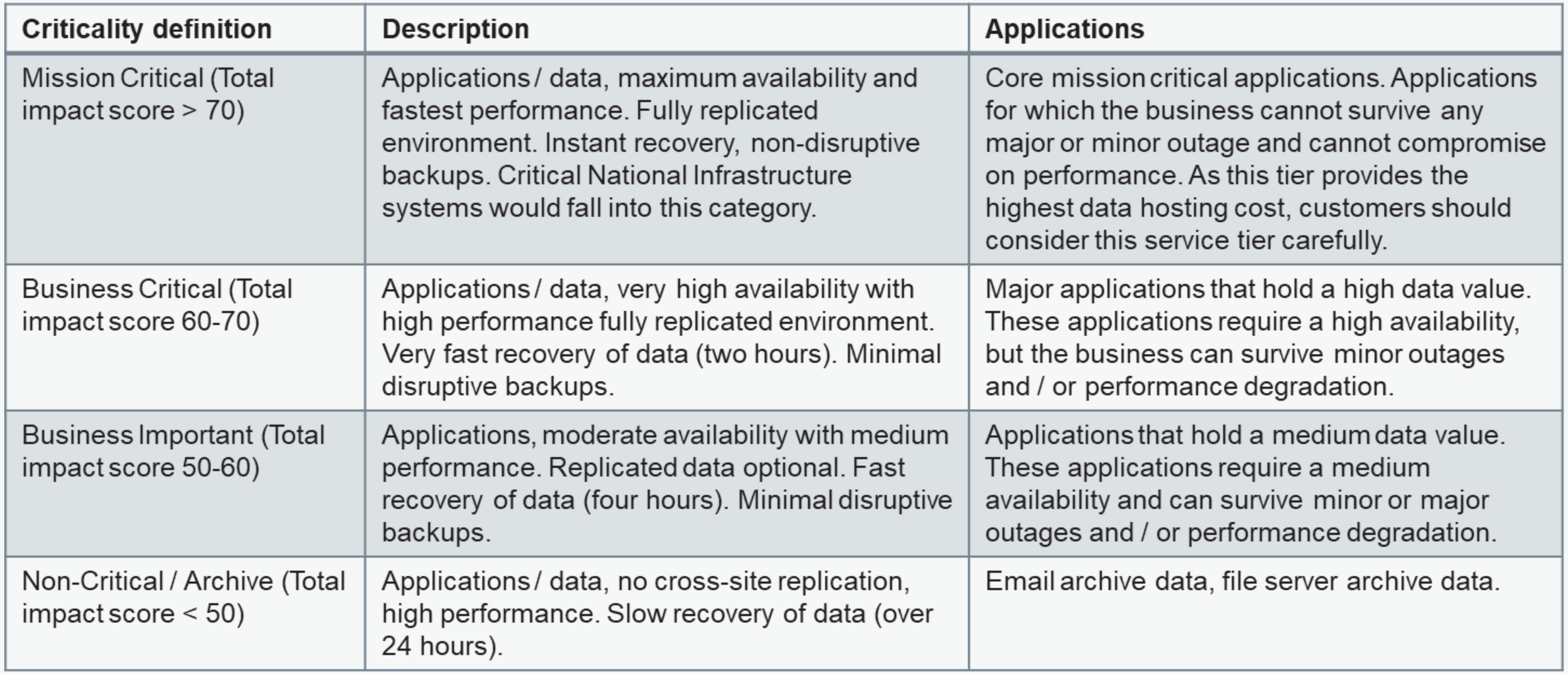
“A cyber attack on a supplier of pathology services to the NHS in south-east London led to the postponement of over 10,000 outpatient appointments and 1,700 elective procedures at King’s College Hospital NHS Foundation Trust and Guy’s and St Thomas’ NHS Foundation Trust”

Top Tip #1 – Know your suppliers

- This can be much harder than it may first sound. Is the list up to date?
- Role of security in the procurement process. SbD.
- Do you know what they supply?
- What type of data do they hold
- Contractual – ‘right to audit’, inform of incidents etc

Top tip #2 – focus on the suppliers that matter

- Categorise your assets. Consistent, repeatable approach



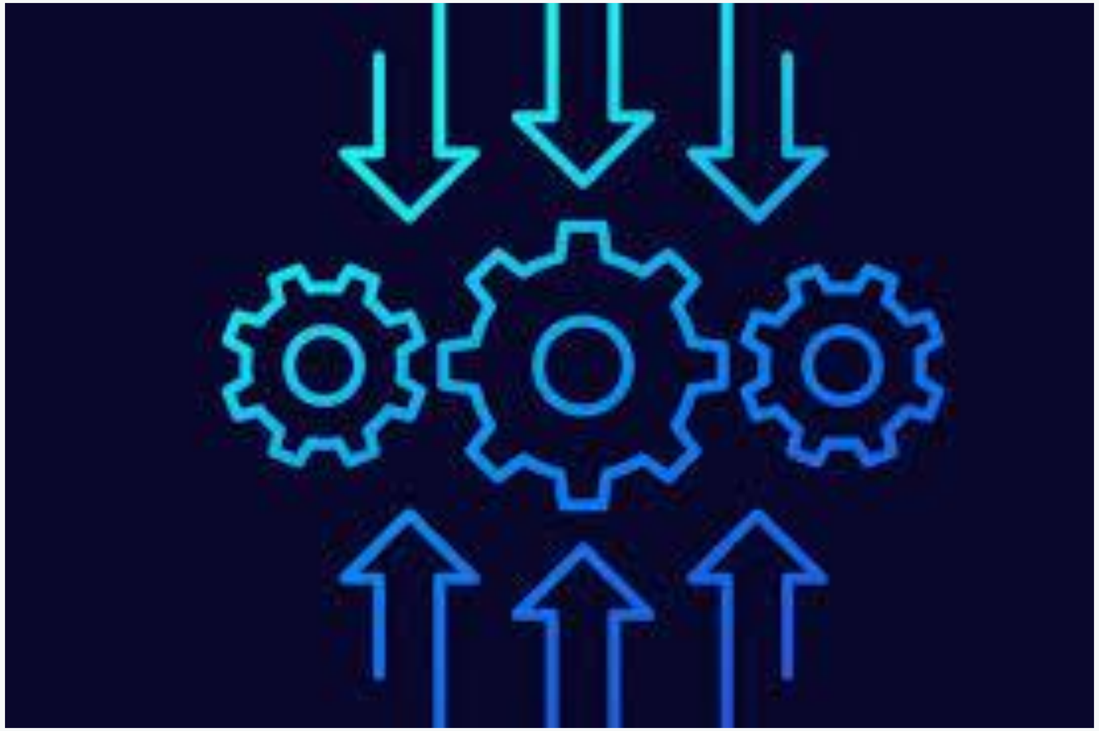
Criticality definition	Description	Applications
Mission Critical (Total impact score > 70)	Applications / data, maximum availability and fastest performance. Fully replicated environment. Instant recovery, non-disruptive backups. Critical National Infrastructure systems would fall into this category.	Core mission critical applications. Applications for which the business cannot survive any major or minor outage and cannot compromise on performance. As this tier provides the highest data hosting cost, customers should consider this service tier carefully.
Business Critical (Total impact score 60-70)	Applications / data, very high availability with high performance fully replicated environment. Very fast recovery of data (two hours). Minimal disruptive backups.	Major applications that hold a high data value. These applications require a high availability, but the business can survive minor outages and / or performance degradation.
Business Important (Total impact score 50-60)	Applications, moderate availability with medium performance. Replicated data optional. Fast recovery of data (four hours). Minimal disruptive backups.	Applications that hold a medium data value. These applications require a medium availability and can survive minor or major outages and / or performance degradation.
Non-Critical / Archive (Total impact score < 50)	Applications / data, no cross-site replication, high performance. Slow recovery of data (over 24 hours).	Email archive data, file server archive data.

Tip #3 Integrate the outcomes of 1 & 2

- Once this these crucial steps are complete, then one can start to embed an effective TPRM management programme.

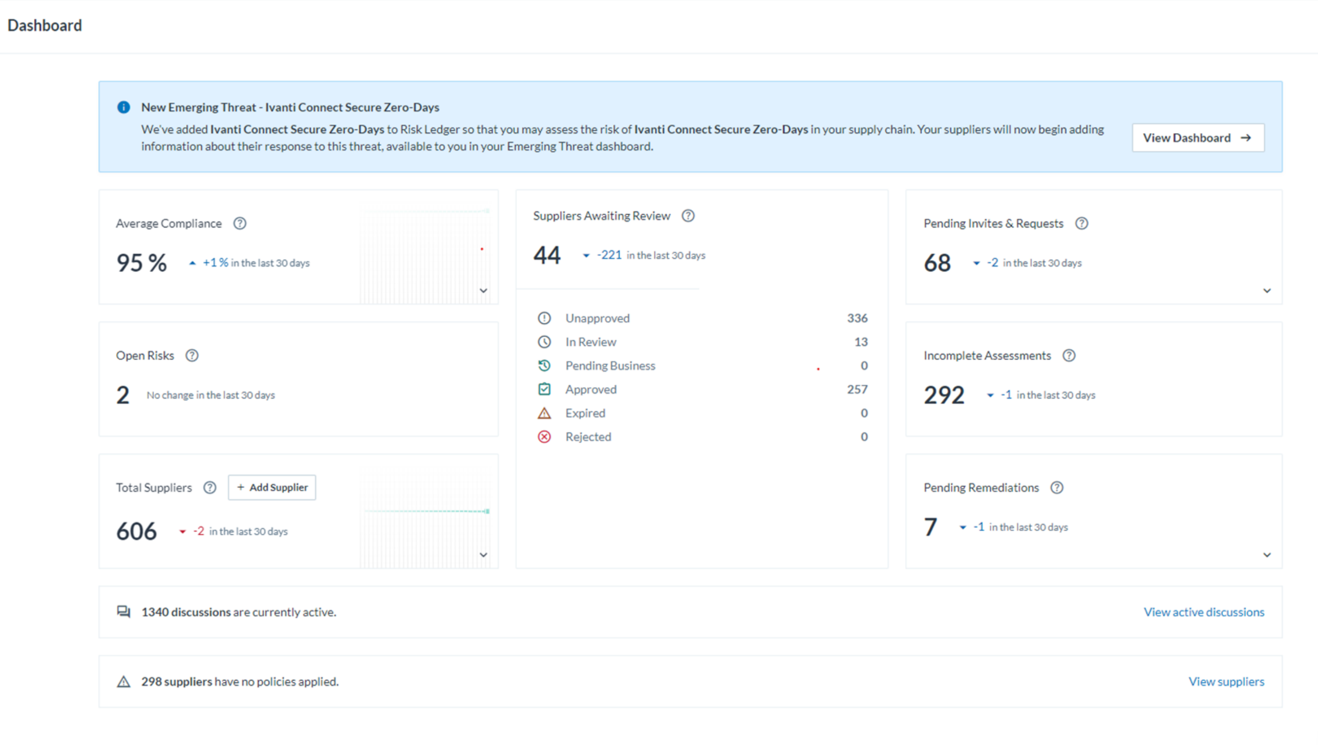
- Work closely with your suppliers. It’s a two-way relationship. Work closely with their security teams.

- They’re busy too. Consider what you are asking. “Do you have CISO?” Yes, then what? Where’s the value?



TPRM

Solution we use, Risk Ledger, allows us to have real time interaction with our suppliers and brings together information from across various domains, not just security, including artifacts e.g. pen test reports, to reach a risk determination.



Dashboard

New Emerging Threat - Ivanti Connect Secure Zero-Days

We've added **Ivanti Connect Secure Zero-Days** to Risk Ledger so that you may assess the risk of **Ivanti Connect Secure Zero-Days** in your supply chain. Your suppliers will now begin adding information about their response to this threat, available to you in your Emerging Threat dashboard.

Average Compliance
95 % +1 % in the last 30 days

Open Risks
2 No change in the last 30 days

Total Suppliers
606 -2 in the last 30 days

Suppliers Awaiting Review
44 -221 in the last 30 days

Unapproved	336
In Review	13
Pending Business	0
Approved	257
Expired	0
Rejected	0

Pending Invites & Requests
68 -2 in the last 30 days

Incomplete Assessments
292 -1 in the last 30 days

Pending Remediations
7 -1 in the last 30 days

1340 discussions are currently active.

298 suppliers have no policies applied.

Top tip #4 Look at processes

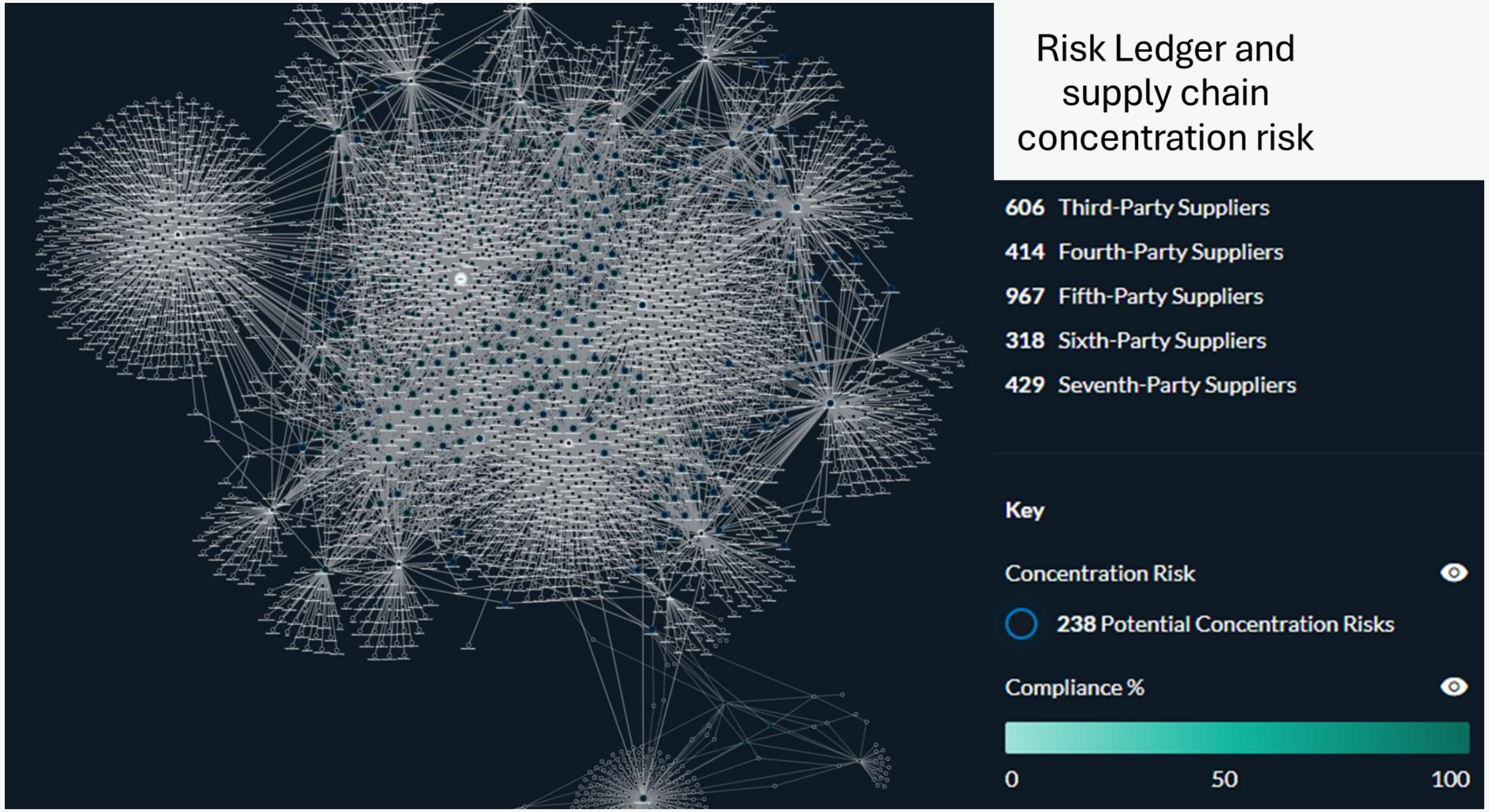
Once we had all the information it typically took us several days to analyse it.

Using AI, Co-pilot, we have taken the time down to on average 9 minutes.

We can use this saving to do other things and to better manage our risk.

TPRM

Risk Ledger and supply chain concentration risk



606	Third-Party Suppliers
414	Fourth-Party Suppliers
967	Fifth-Party Suppliers
318	Sixth-Party Suppliers
429	Seventh-Party Suppliers

Key

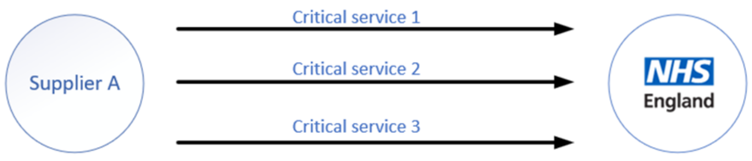
Concentration Risk

○ 238 Potential Concentration Risks

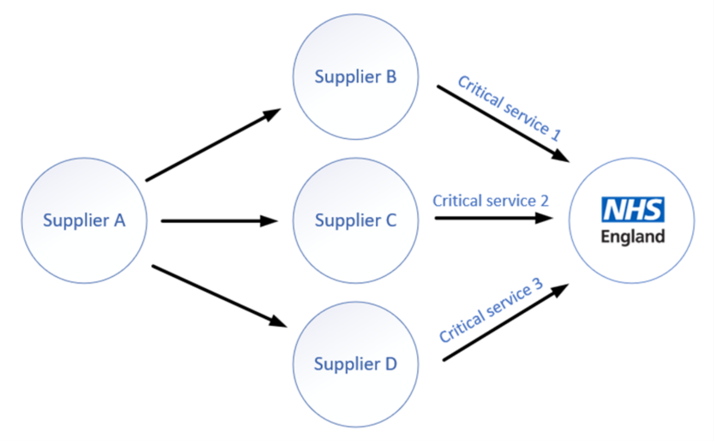
Compliance %

For Example, Concentration Risk

Two or more systems or services that depend on a single supplier:



Two or more third-party suppliers (Suppliers B, C and D) depending on the same fourth party (Supplier A):



In conclusion our top tips & takeaways

- You are helping organisations complete their fiduciary responsibilities
- They have a dependency on you
- Communicate wide and ASK QUESTIONS
- Be transparent
- Ask yourselves, are we represented in every project going on?
    - If not, why not and should we be???
- Again ask, is my team/I as close to Infosecurity team as we could be, or vice versa…

NHS England

Thank You

@nhsengland

company/nhsengland

england.nhs.uk