



Cyber Risk Audit Local Authorities

UK Councils are a target for ransomware attacks, with more than a quarter (27%) having fallen victim.

Source – Information Age

Demand for Cyber Risk Insurance is on the increase and driving the need for X-Ray vision across enterprise cyber risks.

Without a tested Audit framework, the people know-how, or the discovery and monitoring tools in place to identify and track these risks, most organisations don't know where to start or how to satisfy their insurer's diligence requirements.

This often results in the terms and cost of cover being mis-aligned and, as a result, some insurance claims being rejected. Equally without expert guidance, the level of effort needed to satisfy the insurer's diligence requirements can often result in the process being abandoned, leaving the organisation at risk.

As a trusted Cybersecurity Professional Services partner to many sector-leading organisations, Trustify has been working with insurers and brokers to deliver a Cyber Risk Scoring model designed to:



1

Map and rate every Cyber Risk using a simple Cyber Risk Index.



2

Align those findings to insurance industry underwriting requirements in line with ISO 31111:2018 – Cyber Risk Insurance Framework (CRIF).



3

Produce a fully costed and prioritised Cybersecurity Improvement Programme, addressing Critical Risks first.



4

Implement all improvements with the appropriate risk and security controls using a virtual or on-premise Managed Security Service – Cyber Risk Manager.



5

Centralise the Governance, Risk and Compliance reporting tasks in dedicated portal.



6

Roll-out a Cyber Awareness & Training program to every staff member via the same portal.



7

Install a Red Team testing regime to regularly test these improvements and update the security and risk controls proactively.



8

Deploy Advanced Monitoring to preserve and optimise the organisation's Cybersecurity status time.

Organisations who have already deployed this model:

1. Know who you are dealing with all the time, every time
2. Recall errant emails
3. See who has read what and prevent onward forwarding issues
4. Invite your clients into a circle of trust to avoid risk of scamming

Without this clarity of vision and action, organisations will continue to struggle with the demands and challenges of safe Digital Transformation in 2020.

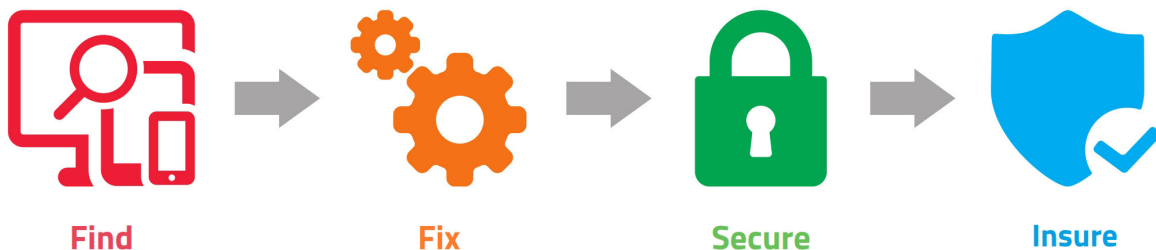
For Local Authorities this can be an especially difficult task in a budget-constrained environment.

That is why Trustify has modelled sector-specific commercial terms to suit this financial requirement.

We provide all LGA members with a fixed-price Cyber Risk Audit based upon the number of employees – c. £5/employee.

We can also offset the Year-1 cost of the audit against the cost of the recommended Cyber Improvement Programme should the service be provided by Trustify.

If you need complete transparency over Cyber risk why not contact our Cyber Risk Audit Team now to book a free half-day Workshop and we will help Find, Fix, Secure & Insure your organisation against Cyber Risk.



Cyber Risk Audit – Case Study

A UK Local Authority needed assurance that its sensitive information was protected against hackers and other Internet threats. Local Authority management was concerned about compliance related issues and wanted assurance its systems were protected against external threats.

Trustify's Solution

Trustify provided an External Network Security Audit and a comprehensive Penetration Test. Our services included a variety of hacker type tools and techniques that identified and evaluated the Local Authority's external risks:

1. **Firewall** - reviewed and analysed configuration.
2. **External** - penetration evaluated vulnerabilities.
3. **Social engineering** - determined employee & supply chain risks.
4. **Phishing** - used fake emails and USB devices to elicit behavioural anomalies.
5. **Fake sites** - determined risks.
6. **Policies** - evaluated Cybersecurity related policies.

Trustify compared the county with industry benchmarks and determined the type of security infrastructure in place. We tailored our attacks to take advantage of the gaps.

Trustify provided an External Network Security Audit Report, a Risk Assessment Report, and a prioritised Action Plan Report of Information Security and Risk Management related recommendations.



Client Benefit

Trustify's external network security audit documented several areas that placed the organisation at risk to external threats. The prioritised Action Plan helped the organisation increase security while increasing protection of its information assets and citizen relationships.

Figures 1. & 2. Council 'X' before and after our Audit recommendations were implemented.



How can I find out more?

Let us find out how we can help you deliver real value from the investment you make in your people.

Visit us at www.trustifyexperts.com

Call us on **+44 (0) 808 196 4200**

Trustify
experts

The home of World Class cyber talent

London

1 Ropemaker Street, London, EC2Y 9HT, United Kingdom

