Coalition®

Generated on 07 February 2025

Cyber Risk Assessment

PREPARED FOR

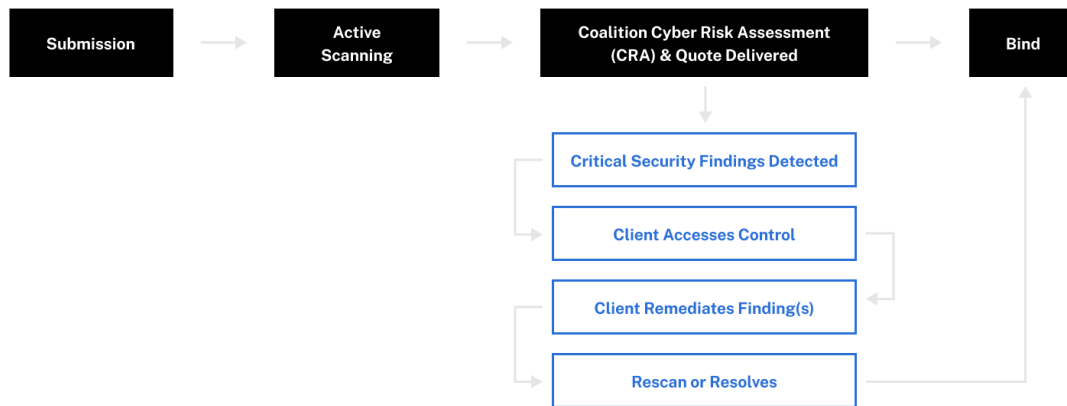## Felixstowe Town Council

coalitioninc.com/en-gb
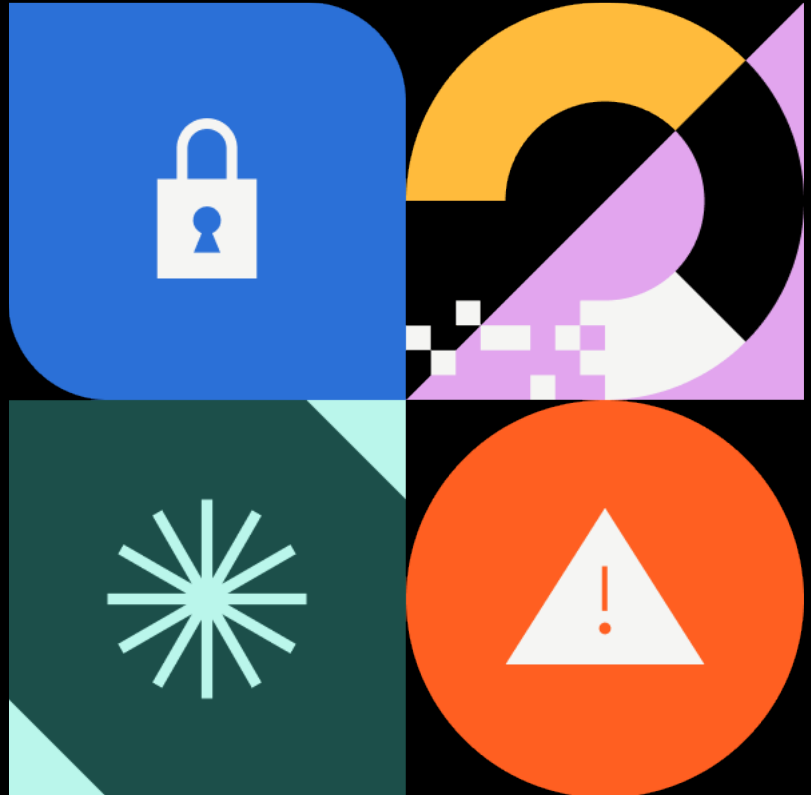
Coalition Control®
Simplify contingency resolution with pre-bind access

Every organisation that receives a quote and Cyber Risk Assessment (CRA) from Coalition also receives exclusive access to Coalition Control®. This allows Coalition to guide you through remediating critical exposures identified by our Active Risk Assessment and help you resolve them before binding coverage.

How does it work?

```
Submission  →  Active      →  Coalition Cyber Risk Assessment  →  Bind
               Scanning        (CRA) & Quote Delivered
                                         ↓
                            Critical Security Findings Detected
                                         
                            Client Accesses Control
                                         
                            Client Remediates Finding(s)
                                         
                            Rescan or Resolves
```

Follow these easy steps to make cybersecurity less daunting with Coalition Control:

1. **Coalition Conducts Active Risk Assessment**
   Coalition uses proprietary attack surface monitoring technology and real-time threat intelligence to provide a customised view of the exposures that are the most severe, likely to impact insurability, and if not resolved could result in claims.

2. **Critical Security Findings Detected by Coalition**
   If Critical Security Finding(s) are detected that impact insurability, they will be noted on the quote document as contingencies and in the Coalition Cyber Risk Assessment (CRA) provided with the quote.

3. **Activate your Coalition Control Account by following instructions provided by your broker**
   Every current and prospective Coalition policyholder receives access to Coalition Control, not just those with security findings. New clients can request pre-bind access by contacting their broker. Existing policyholders can log into Coalition Control with a valid email address and policy number.

4. **Remediate Exposures**
   Log into Coalition Control to review the technical details of any security findings, suggested remediation best practices as well as additional support resources.

5. **Rescan and Resolve**
   After exposures have been remediated, follow the instructions to initiate a rescan and resolve contingencies directly in Control. As soon as contingencies are cleared an updated bindable quote will be reissued. Depending on the security finding, rescans could take up to 48 hours.

Coalition®

Coalition's Active Insurance approach incorporates continuous Risk Assessments, Active Protection, and Active Response, providing policyholders with holistic benefits in protecting their organisations against dynamic risks.

This Coalition Risk Assessment provides a customised view of your organisation's risk. Coalition collects and analyses externally observable security data and integrates these findings with our proprietary claims and incident data to identify your organisation's risk exposures. This objective assessment of your cyber risk enables your organisation to take proactive measures to mitigate risk and improve your security.

Coalition's Active Protection and Response provides a holistic risk management solution for your organisation, including:

- Attack surface monitoring and third party risk management in Coalition Control
- Incident response support and in-house claims team
- Cybersecurity education resources

ASSESS
Real-time, external view of cyber risk with customized recommendations

PROTECT
Identify and prevent new threats with tailored remediation guidance and support

COVER
Comprehensive coverage to help give peace of mind following an attack

RESPOND
Immediate expert support to minimize impact and speed up recovery

52% Reported incidents handled at no cost outside of the policy premium
Source

64% Fewer claims than the cyber industry average
Source

24/7 Support from our claims team

Coalition®

Risk Summary

Felixstowe Town Council

Domains: felixstowe.gov.uk   Last Scanned: 07 Feb 2025

Cyber Health Rating

The Cyber Health Rating is a dynamic score that reflects the overall health of your organization's cybersecurity posture, with 100 representing optimal health. This rating considers factors such as attack surface exposure, and alignment with best practices to help you understand and improve your cyber resilience.

100 /100 Great

Poor   Fair   Good   Great

Critical Security Findings

Critical Security Findings are high-risk vulnerabilities that strongly correlate with cyber claims and security breaches. Addressing these findings is essential to reducing exposure and maintaining insurability.

◆ 0

How Much Would a Cyber Incident Cost?

Using demographic data on your organization, together with Coalition's global claims data, we've modeled the probability that organizations in your peer group will experience a cyber loss over the next 12 months, as well as the expected severity of loss using a statistical model derived from 10,000 simulated years of cyber incidents.

Your Inherent Risk Rating

Baseline level of cyber risk based on your industry and operational complexity, independent of your attack surface and security controls.

■ Great

Revenue	Under 10M	■■■
PHI/PCI/PII Data	<100,000	■■■
Employees	1-25	■■■
Industry	Utilities	■■■

Estimated loss based on your organization's profile

Type of loss	Median	1 in 10 years	1 in 100 years
Composite	£88,404	£661,599	£3,407,517
Ransomware	£160,352	£977,492	£4,260,026
Funds Transfer Fraud	£77,800	£512,181	£2,376,439
Data Breach	£56,087	£436,205	£2,318,120

Incident likelihood compared to average Coalition insured

0.5x as likely

Aggregate limits purchased by peer organizations

Up to £1M	29%
£1M – £2M	50%
£2M – £5M	0%
£5M – £10M	21%

Data is from multiple sources, including Coalition's own data. Actual numbers may vary significantly from calculator estimates based on additional factors for a given business. The data provided is for informational and educational purposes only. Use of the Coalition Coverage Calculator should not be used as a replacement for a company's own due diligence in regards to their cyber risk. Access and use of the Coalition Coverage Calculator is predicated upon the acceptance of Coalition Control's Terms of Service.

Coalition®

Security Findings

CRITICAL	HIGH	MEDIUM	LOW
◈ CRITICAL	△ HIGH	◯ MEDIUM	▽ LOW
0	**0**	**0**	**1**

Critical risks are contingencies that **impact premium and insurability** if not resolved.

High risks can turn into critical risks if not resolved.

Medium risks may turn to high risk if not resolved.

Low risks may turn to medium risk if not resolved.

Attack Surface Analysed

Sub Domains	5
IP Addresses	13
Applications	28
Services	10

For full list, go to control.coalitioninc.com

Critical Findings

Our Active Risk platform has identified the following critical security findings for your organization. To help reduce a **negative impact on insurability or a potential increase in your premium**, resolve these critical findings using the information provided.

Your organisation is Cyber Savvy!

No critical security findings have been detected.

◈ Critical   △ High   ◯ Medium   ▽ Low

SECURITY FINDINGS

Non-Critical Security Findings

Non-critical security findings have a risk severity of High, Medium, or Low. We still recommend remediating them as they could expose your organisation to other types of cyber risk or become critical security findings later as threat actors change their tactics.

SECURITY FINDING	ASSET
▽ **DMARC Record Missing** DMARC, which stands for "Domain-based Message Authentication, Reporting & Conformance", is an email authentication, policy, and reporting protocol. It builds on the widely deployed SPF and DKIM protocols, adding linkage to the author ("From:") domain name, published policies for recipient handling... For full details, go to control.coalitioninc.com/security-findings/?findingsTab=active	1

How can I test my fix and resolve a vulnerability?

1. Go to https://control.coalitioninc.com/security-findings/?findingsTab=active.
2. Select the security finding you want to test and click **Rescan**.
3. Your security findings will update and a new Cyber Health Rating will appear!

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

🔻 Critical ⚠ High 🟠 Medium ▽ Low
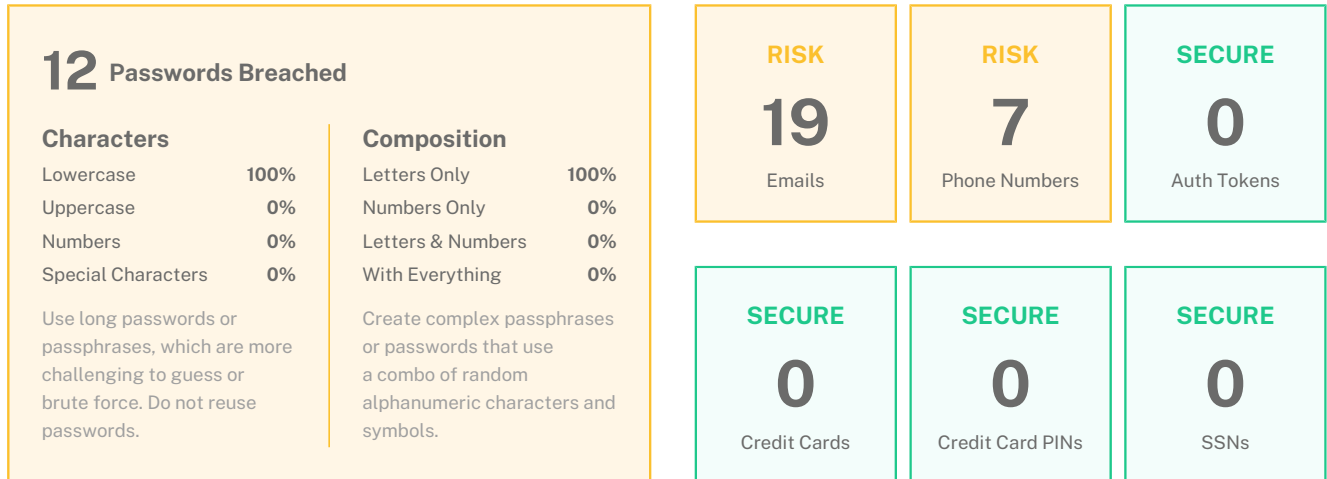
Overall Risk Posture

Your overall risk posture is a holistic look at your organization's cyber exposure. This includes assets, data exposures and technologies that threat actors may exploit identified by our Active Data Graph.

RISK	Data Leaks	**19** leaks
SECURE	Malware	**0** detected
SECURE	Spam	**0** detected
SECURE	Malicious Events	**0** detected
SECURE	Honeypot Events	**0** detected
SECURE	Blocklisted Domains	**0** detected
SECURE	Torrents	**0** detected
RISK	DMARC	**1** failures
SECURE	SPF	**0** failures

OVERALL RISK POSTURE

Data Leaks

This section details the potential impacts of data leaks and phishing. Phishing is often the initial entry point in breaches, and exposed data, like passwords, can be used in subsequent attacks.

12 Passwords Breached

Characters		Composition	
Lowercase	**100%**	Letters Only	**100%**
Uppercase	**0%**	Numbers Only	**0%**
Numbers	**0%**	Letters & Numbers	**0%**
Special Characters	**0%**	With Everything	**0%**

Use long passwords or passphrases, which are more challenging to guess or brute force. Do not reuse passwords.

Create complex passphrases or passwords that use a combo of random alphanumeric characters and symbols.

RISK	RISK	SECURE
19	**7**	**0**
Emails	Phone Numbers	Auth Tokens

SECURE	SECURE	SECURE
0	**0**	**0**
Credit Cards	Credit Card PINs	SSNs

What are your most common breaches?

19	Email addresses
12	Passwords
7	Postal Code
7	Physical addresses
7	Phone numbers
7	Names
7	Job Titles
7	Homepage URLs
7	Government issued IDs
7	Fax

Where are your breaches occurring?

8	Sensitive Source
1	International Combolist
1	Unknown Combolist
1	Collection #4 Combo List
1	2019 Antipublic Combo List
1	Collection #3 Combo List
1	Collection #2 Combo List
1	Collection #1 Combo List
1	Combolist of 1.4 Billion Credentials
1	Anti-Public Combolist

Need more info?

Go to control.coalitioninc.com/data-leaks/ for a full list.

Not a Coalition Control user?

Sign up for free at control.coalitioninc.com

OVERALL RISK POSTURE

Malware

Assets we discovered where malware activity was detected.

SECURE
0
Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Spam

Assets we discovered that send unsolicited communication.

SECURE
0
Assets Detected

ASSET	SOURCE	LAST DETECTED

Scan performed and no results were found

Coalition

OVERALL RISK POSTURE

Malicious Events

Assets detected by Coalition or a third-party partner, noted for their performance leading to attempted or successful unauthorised network intrusion by a threat actor. These attempts can lead to malware, ransomware, or other cyber incidents.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

Honeypot Events

A honeypot is a legitimate security mechanism that is purposely vulnerable to high-risk exploits in order to identify malicious assets that attempt to infiltrate it. Our distributed network of honeypots listens for unsolicited connections and attacks. Your assets should not communicate with our honeypots. Events in this section indicate malicious activity on your network is likely. Shared assets are not an indicator of malicious events.

SECURE

0

Assets Detected

ASSET	TAGS	LAST DETECTED

Scan performed and no results were found

Coalition®

OVERALL RISK POSTURE

Blocklisted Domains

Domains found in public blocklists — if one of your assets is found on these lists typically means that some type of malicious activity was performed.

SECURE
0
Assets Detected

ASSET	SOURCE	LAST DETECTED
	Scan performed and no results were found	

Torrents

Torrent downloads are often illegal and you risk bringing files infected with malware into your network. In this section, we list the torrents seen being downloaded by your assets.

SECURE
0
Assets Detected

ASSET	NAME	LAST DETECTED
	Scan performed and no results were found	

OVERALL RISK POSTURE

DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorised use (known as email spoofing). The purpose of implementing DMARC is to protect a domain from being exploited in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

RISK

1

Domains Failed

PASS (0)

FAIL (1)

felixstowe.gov.uk

SPF

Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of an email. This measure specifies what email servers are allowed to send email from your domain. It helps ensure that someone cannot create an email server and send it as your domain unless you have authorised them to do so in your DNS records.

SECURE

0

Domains Failed

PASS (1)

FAIL (0)

felixstowe.gov.uk

Glossary

Asset	Web properties that your organisation owns, such as an IP Address, Domain, or Subdomain.
Data Breach	A cyber incident where your customer or employee data is accessed, and possibly exfiltrated, by a third party.
Domain	Web address associated with the organisation. Example: coalitioninc.com
Frequent Claim Indicator	A security finding that frequently leads to claims and severely impacts your Cyber Health Rating.
Hosting	Some type of hosting provider or hosting technology being used in one or more of your assets.
IP Address	An IP address associated with your company. Example: 1.1.1.1.
Remote Desktop Protocol (RDP)	RDP is a feature that enables employees to remotely log into their corporate computer from home. While it may be convenient for employees, RDP can also function as an open door for hackers to break into your corporate network.
Secure Sockets Layer (SSL)	SSL is a cryptographic protocol designed to provide secure communications over a computer network.
Services	Technologies used to deliver services from your assets.
Technologies	Technologies found being used in one or more of your assets.
Torrents	Torrenting is a peer-to-peer file-sharing mechanism whereby assets that are hosted on your computers may be downloaded by other people who are outside of your organisation.

This assessment was prepared by

Coalition Risk Solutions Ltd.

34-36 Lime Street

London UK

EC3M 7AT

For more information, visit coalitioninc.com/security