COGNISYS

COMPLIANCE

Fractional/ Virtual CISO

Add the right expertise to your organisation. Maximise security and set your compliance direction.

Our vCISO service allows you to take advantage of our expert knowledge, without needing to pay for a full-time Chief Information Security Officer.

Our senior staff integrate with your team, to lead, guide and help improve your cybersecurity strategy. Working with existing internal and third-party resources, we develop a programme of works that reduces your operational risk.

In addition, the knowledge and experience of our entire technical team is available, providing:

- A higher level of technical and governance expertise.
- Full support of an experienced cyber team.
- No single point of failure.

Initial review

The starting point is a comprehensive review, to discover the current cyber security status and objectives of your organisation.

A gap analysis is performed, which may include the following areas:

- IT network topology.
- Application estate.
- Security controls.
- Critical assets – hardware, software & data.
- Business continuity.
- Threat identification.
- Cyber security maturity level.
- Incident management processes.
- Roles and responsibilities.
- Capabilities and capacity.
- Third parties.
- Staff awareness training.
- Risk register.
- Policies.
- Cyber risk governance.
- Contractual, legal or regulatory obligations.

The output from this gap analysis typically informs the action plan to address and mitigate risks, then help move the organisation from its existing state, to its desired state.

Project delivery

Once the action plan is agreed, our Virtual CISO will work with your internal staff to implement any changes.

This is designed to improve the cyber security posture of your organisation, through a project with defined time scales, outputs and milestones, including:

- Security strategy - creation or revision.
- Business case and benefit realisation.
- Budget planning, phasing and time scales.
- People.
- Process.
- Technology.
- Training.
- Roles and responsibilities.
- Criteria for success.
- Security framework alignment (if appropriate).

Operation and monitoring

Following project completion, typically the service moves into the ‘business as usual’ phase, to:

- Monitor and re-evaluate, refining continually.
- Setup and manage security forums
- Provide regular updates on maturity, risk and threat landscapes, tailored to the relevant groups, typically executive, risk management committee and IT teams.

Report

Cognisys presents its findings in a comprehensive yet simple report format.

This typically comprises: an executive summary, methodology, technical findings, and prioritised recommendations for remediation.

BACK TO CONTENTS