

PCI Audit Process

We provide audits, scans and assessments, and advise on the mitigation of payment card risks. Here, we outline the audit process from initial assessment to issuing a formal signed certificate of compliance.



Gap Analysis

The audit can begin with an initial gap analysis. Our security team review the processes and procedures of the client, identify the gaps against the standard and provide a strategic roadmap to compliance. Giving the client an opportunity to remediate issues, before the assessment starts.



~~~

# **Scoping Session**

The client's environment is taken through a scoping session to determine all the areas where the client has contact with card-holder data including all supporting people, processes and technology.

## Formal Onsite Assessment

During the onsite assessment, we assess the security controls in place that support the 12 PCI DSS requirements and then provide a report. The onsite assessment normally takes 2-5 days depending on the size of the organization.

## Fails Standard

In a case where the client fails to meet the 12 requirements, we issue a report and identify the gaps which should then be remediated by the client.

### Remediation

Cognosec helps and supports clients during this phase until they comply with all the requirements. Once remediation is complete, the client will be considered for certification.



### Meets Standard

When the client meets the requirement we issue a ROC (level 1) or an SAQ (level 2-4) and then issue a formal signed certificate of compliance to the appropriate PCI DSS standard.

If you would like to know more about PCI Auditing by Cognosec, please contact one of our team members in your nearest office.

### **Cognosec Offices** & Contact Details

### **UK & Ireland**

Tel +44 (0)20 3870 1539 sales.uk@cognosec.com

### Austria

Tel +43 (0)1 212 2020 sales.at@cognosec.com

### Germany

Tel +49 (0)69 7593 8490 sales.de@cognosec.com

#### UAE

Tel +971 (0)4 451 1552 sales.dxb@cognosec.com

# cognosec

### **About Cognosec**

Cognosec are a NASDAQ-listed company, headquartered in Sweden, with subsidiaries in the UK. Austria, Germany, UAE, Kenya and South Africa.

Our purpose is to help companies comply with international, regional and local laws, and become cyber resilient.

We provide solutions that protect organizations and help them withstand significant cyber attacks.