CYBERTEQ

Cyber Security

Secure business through innovation

Cyberteq is an innovative Information and Communication Technology Consulting Company, owned by Cybercom Singapore Pte Ltd.

Mission

To Transform and Secure business through innovation.

Vision

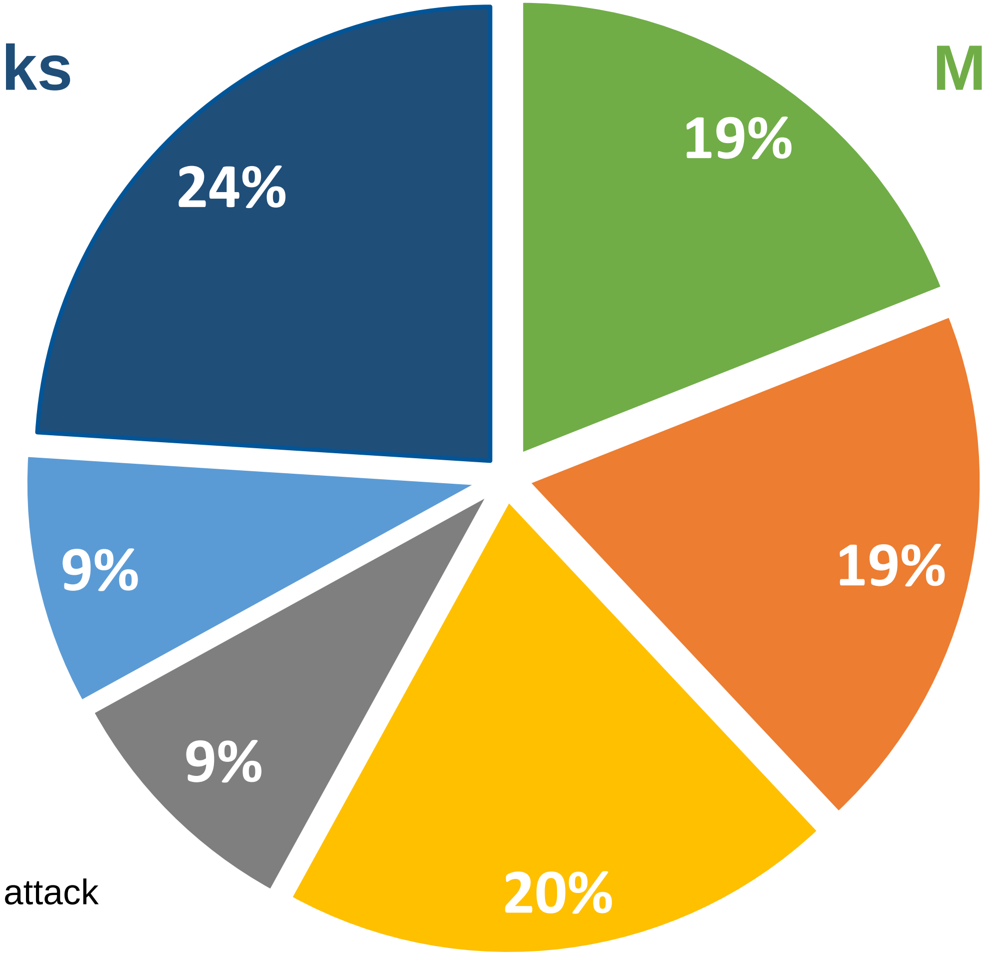
To be the most reliable business partner and employer of choice.

Proposition

We empower our clients to explore new opportunities and improve efficiency while minimizing security risks. Our solutions are tailored by innovation to match clients' unique challenges.

Top Cyber attacks

CYBERTEQ



Web Application Attacks

- Information from company’s database
- Leak of customer information
- Payment transaction fraud

DoS/DDoS

- Slow network performance
- Unavailable web and mobile applications
- Inability for customers to access banking service

Reconnaissance

- Information gathering is first step in cyber attack
- Determine system vulnerabilities
- Preparation for attacks in the future

Mobile Application Attacks

- Capture data packets from application
- Tailored attacks based on vulnerabilities
- Sniffing of user and server credentials

Malware

- Steal data: System and personal information, banking credentials, financial details, credit card numbers and passwords
- Ransomware: encrypt your data and demand ransom to restore it

Other Attack Types

- Social engineering attacks on employees through phishing e-mail
- Insider threats
- Attacks from supplier organization

Cyberteq competence

Web Application Attacks

- Penetration testing
- Source code review

Cases

- SEB (bank)
- Skandia (bank & insurance)

DoS/DDoS

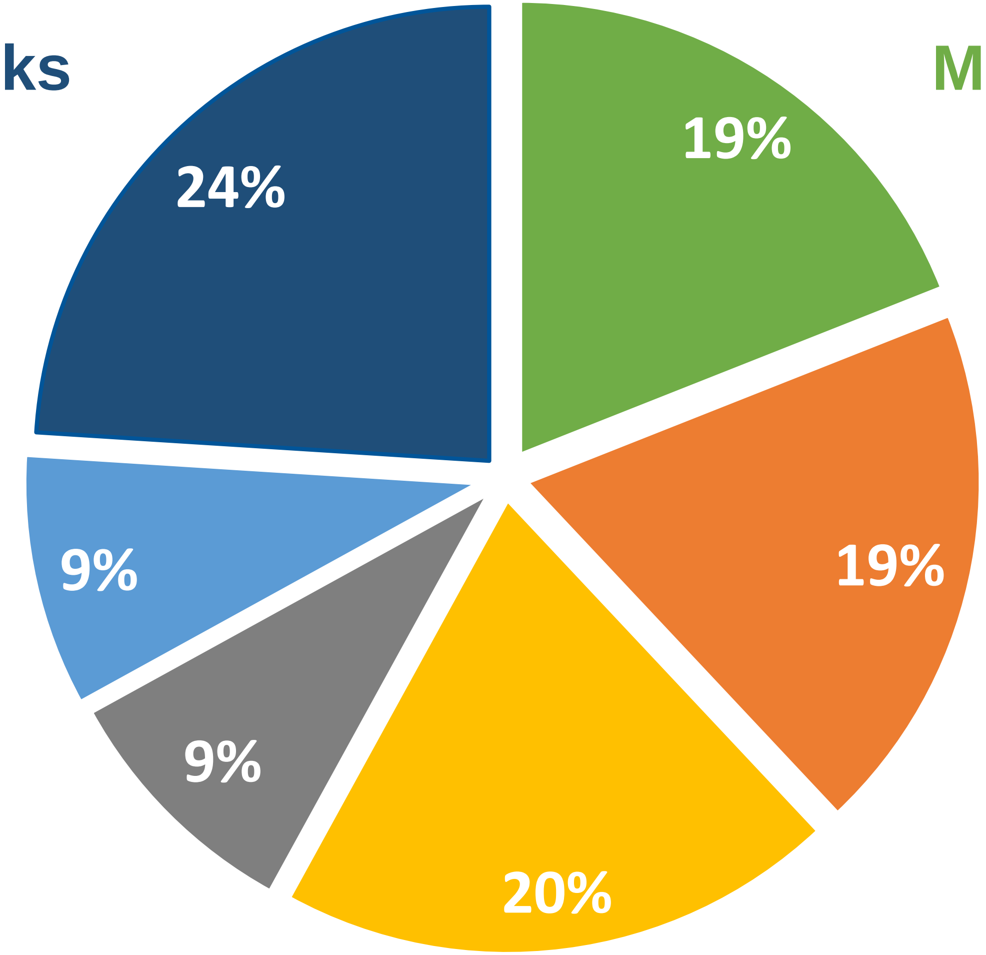
- Security Advisory
- Network Architecture review

Cases

- PostNord

Reconnaissance

- Part of any vulnerability assessment



Mobile Application Attacks

- Mobile application pentest (android + ios)
- Source code review
- Reverse software engineering

Cases

- Försäkringskassan (Swedish social insurance agency)

Malware

- Incident response
- Malware investigation

Cases

- Confidential

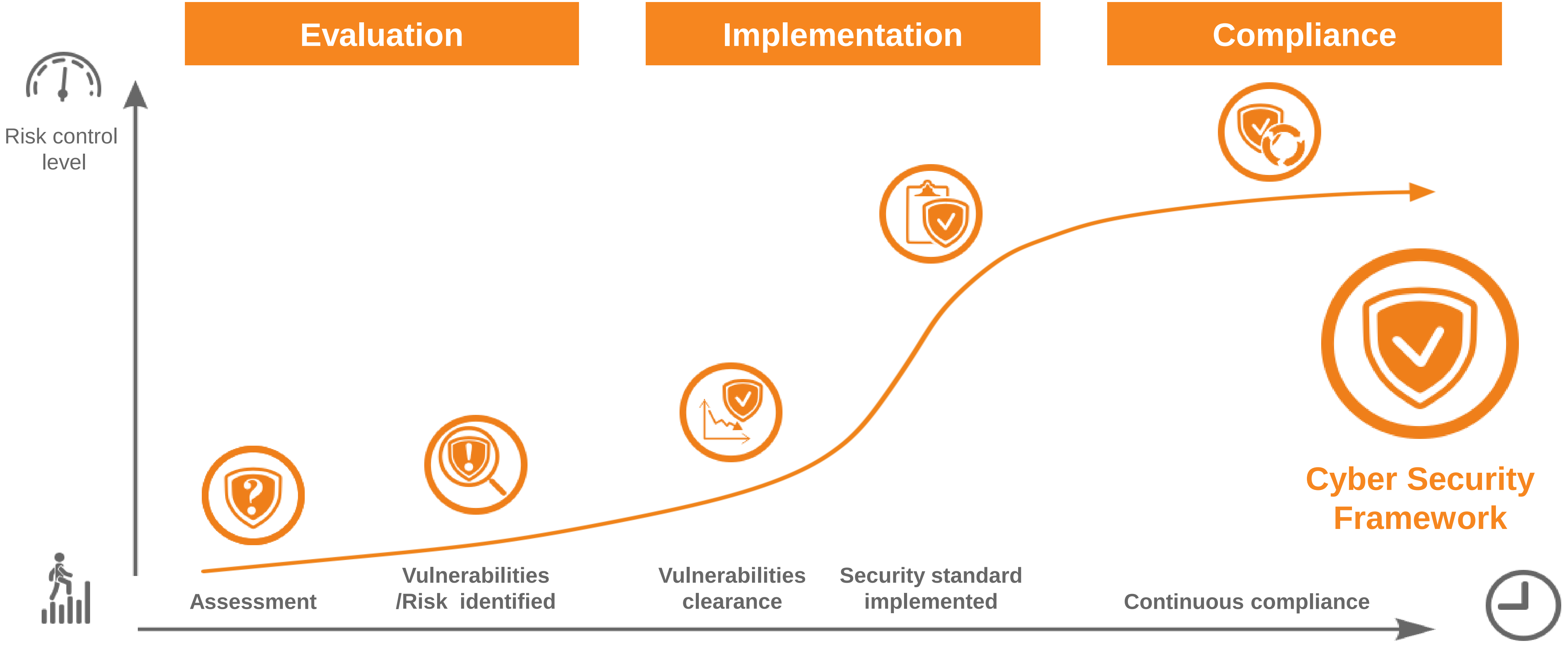
Other Attack Types

- Social engineering attacks:

Cases : Telecom and insurance companies

- Access control review
- Policies and procedure review

Cyberteq cyber security framework



Evaluation

Implementation

Compliance

Risk control level

Assessment

Vulnerabilities /Risk identified

Vulnerabilities clearance

Security standard implemented

Continuous compliance

Cyber Security Framework

Client challenges

- Is my organization secured
- Is my organization compromised
- What are my organization vulnerabilities
- What is my risk level

- How to mitigate my risk
- What type of standard is required
- How to protect my information and assets
- How to manage end point security

- How to assure constant compliance
- How to maintain my organization security level
- How to keep my risk controlled

Time

Security kits

CYBERTEQ

Assessment kit

Boost Kit

Compliance kit

Help clients to assess current information security measures , identify vulnerabilities and gaps, analyze risks and derive mitigation plan.

Support clients to apply corrective actions, create and implement adequate security standards , define required solution and boost security awareness overall organization.

Help clients to apply right measures, monitor compliance level to wide range of security standards and maintain accountability throughout their organizations.

Assessment kit

Advisory

- Security strategy review
- Security awareness

Security Assurance

- Vulnerability assessment - IT network, servers
- Penetration testing - Web and mobile application
- Code review
- System and configuration review
- Network architecture review
- Access control review
- Social engineering

Risk Assessment

- Threat analysis
- Business impact

Boost kit

Advisory

- Asset and Data classification
- End point Security
- IAM and PAM advisory

Risk Mitigation

- Mitigation action plan
- Implementation management
- Patch management
- Vulnerability post assessment

Governance

- Standard/policy awareness
- ISO 2700x , PCI/DSS GAP Assessment
- Policy review , creation and implementation

Compliance kit

Advisory

- Compliance awareness

Compliance Portal

- Standards/policies integration
- Compliance process
- Admin/user training

Compliance Monitoring

- Compliance status per dep/sys/user
- Periodic compliance audit and vulnerability assessment

mUnit is the next generation cyber security appliance created by Cyberteq. It has re-shaped the way of working with security and will replace traditional security and risk assessments. It is also your trusted partner in your road to achieving compliance to any standard.

mUnit provides **assessment** to identify and track vulnerabilities with related business impact.

mUnit **boosts** your organization security, by dynamic clearance of security gaps and adequate policies implementation.

mUnit manages **compliance** to international security standards

Patent pending

Benefits for your business

Pure action-oriented Security measurements

Dynamic risk mitigation and implementation

Focus on your business

Pay as you need

Control risk and Increased accountability

Improve business continuity

Cyber Security Simpler than ever

Innovative approach

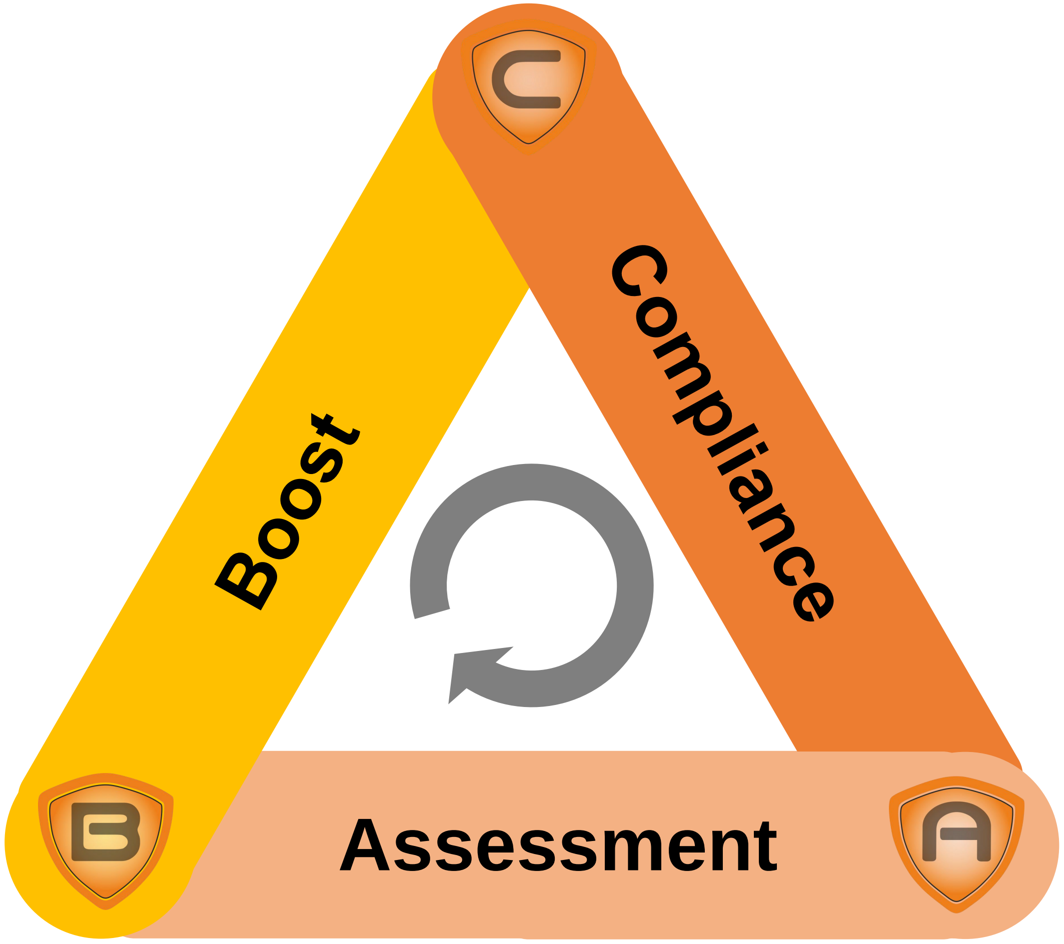
More affordable

Manage brand reputation

Patent pending

mUnit security model

CYBERTEQ



Assessment Boost Compliance

ABC of Cyber Security

ABC Advantages:

- From reports to actions
- From post to dynamic implementation
- From recommendation to accountability
- From periodic compliance to “real time” compliance

Main Functionalities

- Security snapshots
- Vulnerability assessment
- Vulnerability and action tracking
- Patch management
- With layered security architecture
- Covering all security needs
- Security as a Service
- And many others

All in One

Advisory

Assessment

Governance

Mitigation

Compliance

Assurance

Advisory

- General security advisory (Identity access management, EPS , Asset and Data classification and DLP and others)
- Security training and awareness
- Secure coding trainings for developers
- Incident response (Malware infection, DDoS attack, phishing attacks and others)
- Security strategy review

IT security

- Vulnerability assessment
- Ext/Int Penetration testing (Network, Web and mobile applications)
- Source code review
- PCI/DSS ASV vulnerability scan
- Social engineering
- Configuration review
- Network Architecture audit
- Digital Forensics

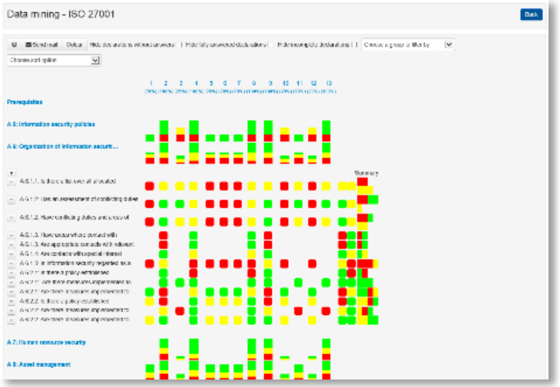
services

Information security

- Compliance (e.g. PCI. ISO 2700x and others)
- Gap Analysis
- ISO 27000X and PCI audit
- Policy review , creation and implementation
- Risk and Business impact assessment
- Risk management
- SDLC
- Compliance portal

Cybercom Compliance portal

CYBERTEQ



Data mining - ISO 27001

Prerequisites

A 5: Information security policies

A 6: Organization of information securit...

A.6.1.1. Is there a list over all allocated

A.6.1.2. Has an assessment of conflicting duties

A.6.1.2. Have conflicting duties and areas of

A.6.1.3. Have areas where contact with

A.6.1.3. Are appropriate contacts with relevant

A.6.1.4. Are contacts with special interest

A.6.1.5. Is information security regarded as a

A.6.2.1. Is there a policy established

A.6.2.1. Are there measures implemented to

A.6.2.1. Are there measures implemented to

A.6.2.2. Is there a policy established

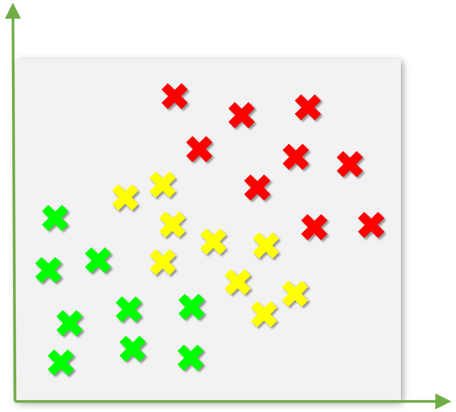
A.6.2.2. Are there measures implemented to

A.6.2.2. Are there measures implemented to

A 7: Human resource security

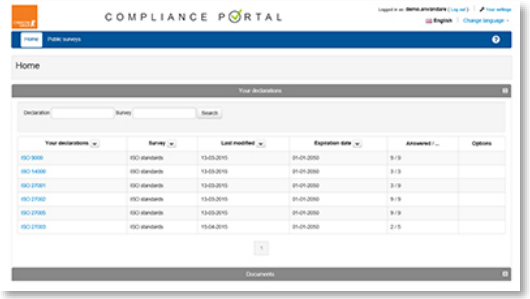
A 8: Asset management

Compliance



Risk

Measures



COMPLIANCE PORTAL

Logged in as: demo.aniwindare (Log out) | Your settings
English | Change language
Home
Public surveys

Home

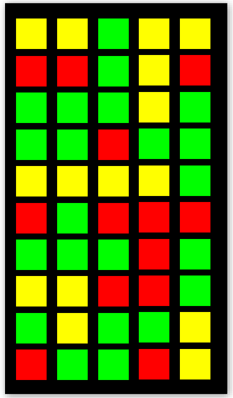
Your declarations

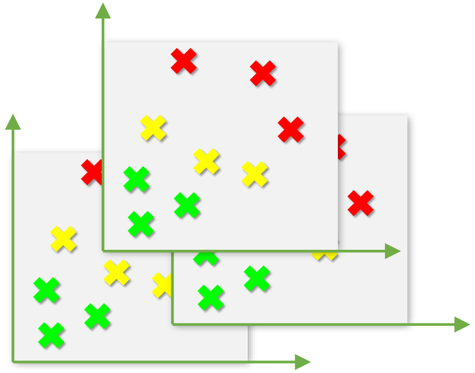
Declaration Survey Search

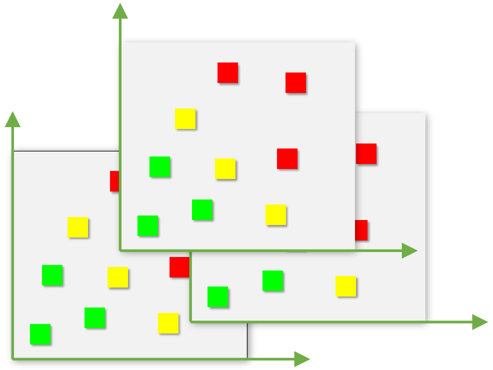
Your declarations	Survey	Last modified	Expiration date	Answered / ...	Options
ISO 9000	ISO standards	13-03-2015	01-01-2050	9 / 9	
ISO 14000	ISO standards	13-03-2015	01-01-2050	3 / 3	
ISO 27001	ISO standards	13-03-2015	01-01-2050	3 / 9	
ISO 27002	ISO standards	13-03-2015	01-01-2050	9 / 9	
ISO 27005	ISO standards	13-03-2015	01-01-2050	9 / 9	
ISO 27003	ISO standards	15-04-2015	01-01-2050	2 / 5	

Documents

Security Requirements







Cybercom Compliance portal

CYBERTEQ

Implementation areas

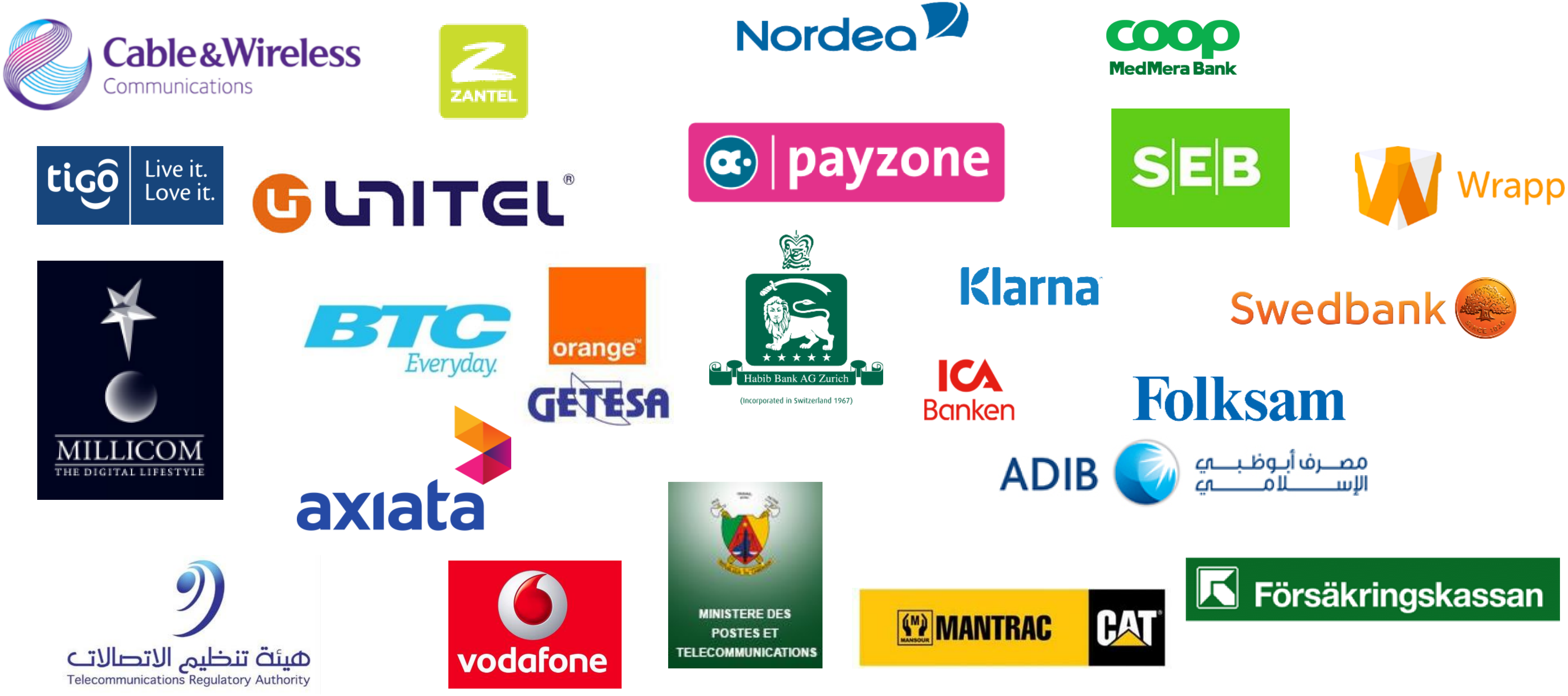
- Internal audit
- ISO security (ISO 2700x)
- Procurement
- HR
- Physical security
- Any other internal policies or standards

Benefits and added values

- Easy for use with flexible configuration
- Possibility to add new area for compliance by client
- All policies and standard in one compliance system for efficient monitoring and evaluation of current compliance and risk assessment

Some of our clients

CYBERTEQ



CYBERTEQ

www.cyber-teq.com