

Appendix

Appendix A – Cyber risk management objectives interviews

| Role | Interview Duration |
|--------------------------------|---------------------------|
| CISO | 01:30 |
| Professor | 00:50 |
| IT Specialist | 00:42 |
| Professor | 01:10 |
| IT network administrator | 00:46 |
| CISO | 01:21 |
| Security Lead Consultant | 00:45 |
| ISO 27001 Consultant | 00:55 |
| System Administrator | 00:45 |
| IT Support Coordinator | 00:37 |
| IT Systems Director | 00:56 |
| Security Manager | 01:41 |
| Technical Coordinator | 00:47 |
| System Administrator | 00:32 |
| Network & Security Manager | 00:45 |
| Database Administrator | 00:37 |
| System Administrator | 00:28 |
| CIO | 00:32 |
| IT Service Director | 00:54 |
| IS Director | 01:35 |
| Security Business Unit Manager | 01:11 |
| IS Director | 01:23 |
| IT Development Coordinator | 00:58 |
| IT Project team leader | 01:23 |
| IT Support Coordinator | 00:38 |
| IS Director | 00:54 |
| IT Communications Director | 00:39 |
| System Administrator | 00:35 |
| IT Operations Coordinator | 01:11 |
| IT Manager | 00:45 |
| IT Consultant | 00:48 |
| IT Architect | 00:56 |
| IT Director | 01:21 |
| IS Quality | 01:01 |
| IT Support | 00:29 |

Appendix

| | |
|--------------------------------|-------|
| IT Manager | 01:05 |
| Security Consultant | 02:11 |
| Security Auditor | 01:49 |
| Security Consultant | 01:32 |
| Compliance Manager | 00:45 |
| Security Manager | 00:49 |
| Security Specialist | 01:23 |
| 27001 Consultant | 01:08 |
| IT Developer | 00:32 |
| IT Project Manager | 00:29 |
| IT Administrator | 00:51 |
| IT Consultant | 00:47 |
| Professor | 01:35 |
| IT Privacy Specialist | 00:49 |
| IT Consultant | 00:30 |
| Security Consultant | 00:43 |
| IT Support Coordinator | 00:29 |
| Database Administrator | 00:54 |
| Ethical Hacker | 01:11 |
| Professor | 00:39 |
| IT Manager | 01:01 |
| Infrastructure Analyst | 00:34 |
| System Administrator | 00:58 |
| IT Project Manager | 00:45 |
| IT Manager | 00:49 |
| IT Auditor | 01:05 |
| Security Consultant | 01:13 |
| Risk Manager | 01:48 |
| Compliance Manager | 00:56 |
| System Administrator | 00:43 |
| Risk Manager | 01:43 |
| IT Governance Specialist | 00:57 |
| CISO | 01:23 |
| Network Security Administrator | 00:45 |
| DBA Coordinator | 00:36 |
| Security Consultant | 01:02 |

Appendix

Appendix B – Case-study interviews

| Role | Interview Duration |
|---------------------------------|---------------------------|
| Security Director / CISO | 05:35 |
| Managing Director | 00:55 |
| IS Director | 01:56 |
| IT Advisor to the Man. Director | 01:43 |
| Distributed systems Director | 01:34 |
| Infrastructure sub Director | 01:12 |
| Platform sub Director | 01:32 |
| IT Lead Auditor | 01:05 |
| HR Director | 00:42 |
| IT End systems sub Director | 01:41 |
| Network sub Director | 00:57 |
| Central IT systems sub Director | 00:32 |

Appendix

Appendix C – Cyber risk management values

Common form values

- I wish employees accept others suggestions
- I wish there is adequate access control
- I wish there is adequate access control
- I wish there is adequate access control
- I wish there is adequate access control to identities
- I wish there is access security policies for DB
- I wish there is access security policies for Servers
- I wish there is access segmentation
- I wish there is accountability
- I wish there is accountability
- I wish there is accurate documentation
- I wish there is adaptability of company staff
- I wish there is adaptability to chosen software base
- I wish there are adequate planning and test
- I wish we adopt best practices
- I wish we adopt proven or stable methodologies
- I wish there is an alignment between IT and business
- I wish there is an alignment between IT and business
- I wish there is an alignment between IT and business

- I wish there is a clear understanding of the amount of data to be protected
- I wish we analyze current investment documentation
- I wish we applied minimum security baselines
- I wish we assure a sponsor
- I wish communications assurance
- I wish we assure critical processes
- I wish we assure data management uses standards

- I wish there is an assurance that security policies are followed
- I wish there is audit capacity
- I wish there is code audit
- I wish that there are automated tasks that reduce human errors
- I wish there is awareness for the need of project governance
- I wish there are backups
- I wish there are backups
- I wish there are backups
- I wish there are periodical backup and restoration tests
- I wish there is backup redundancy
- I wish there was adequate planning
- I wish there is promotion of creative thinking
- I wish there is promotion of critical thinking

Appendix

I wish employees are organized
I wish there is promotion of proactive thinking
I wish the employees behave professionally
I wish there is benefits management process
I wish we adopt best practices
I wish we adopt best practices
I wish we block external removable devices
I wish we build an IT architecture
I wish there is alignment between IT and business
I wish there is Business Continuity Planning
I wish there was no business disruption related to IT
I wish there are Bring your own device practices
I wish there are no cascading risks due to IT failure
I wish there is a centralized antivirus management
I wish there is centralized control of IT
I wish we could change employees mentality towards security
I wish there is change management
I wish we change passwords periodically
I wish there is a clean desk policy
I wish IT objectives are clearly defined
I wish IT objectives are clearly defined
I wish processes are clearly defines
I wish project are clearly defined
I wish there are risk mitigation procedures
I wish there are clear security policies
I wish there is data leakage protection of client information
I wish the integrity of client's data is preserved
I wish we have clear client requirements
I wish the client is satisfied
I wish there is a cloud adoption strategy
I wish we collaborate more efficiently with partners
I wish we are able to communicate the need for security to top management
I wish the chosen solution is compatible with others solutions
I wish we adopt complex passwords
I wish we adopt complex passwords
I wish we assure compliance
I wish we comply with partners requirements
I wish we have confidentiality agreements
I wish there isn't a constant replacement of key users in projects
I wish there is a continuous improvement of security processes
I wish there is a continuous monitoring and updating of IT risks
I wish there is a continuous risk process
I wish there is a control of access to external networks
I wish there is copyright management
I wish costs are minimized

Appendix

I wish costs are minimized
I wish we perform cost benefit analysis
I wish the cost of losing information is minimized
I wish the cost of infrastructure ownership is minimized
I wish the cost of recovering assets is minimized
I wish costs to implement solutions are minimized
I wish the cost to recover information is minimized
I wish costs are minimized
I wish the customer is satisfied with IT service
I wish the HR asked for criminal records for employees
I wish there is crisis management training
I wish we assure the availability of critical operations
I wish we define the information criticality
I wish we define the asset's criticality
I wish we preserve the data authenticity
I wish we adopt data encryption
I wish we adopt data leakage protection measures
I wish we identify the impact of data loss
I wish we adopt data leakage protection measures
I wish we assure data privacy
I wish we adopt data leakage protection measures
I wish we assure data quality
I wish we assure data recovery
I wish we store data in multiple physical locations
I wish we decide based on our past experience
I wish service maximum downtime is defined
I wish we give different privileges to distinct users
I wish we evaluate the difficulty of implementing a solution
I wish valuing information is not difficult
I wish we adopt disaster recovery measures
I wish we adopt disaster recovery measures
I wish no human life is harmed during a crisis
I wish there is adequate documentation
I wish there is adequate documentation
I wish there are documented procedures
I wish it is easy to access data when necessary
I wish there is an effective maintenance of systems
I wish there is an effective team communication
I wish we encrypt cloud information
I wish we ensure good people communication
I wish we promote intrapreneurship within the organization
I wish we enumerate the dependencies of IT
I wish we measure the solution exposure factor
I wish we adopt filesystem security
I wish we adopt harddrive encryption

Appendix

I wish there is adequate hardware maintenance
I wish hardware is reliable
I wish hardware requirements are clearly defined
I wish there is adequate hardware support
I wish there is high availability of IT infrastructure
I wish there is high availability of IT infrastructure
I wish there is high availability of IT infrastructure
I wish there is high quality security software
I wish there are high security networks
I wish we decide based on our past experience
I wish we decide based on our past experience
I wish we minimize the difficulty of operating a solution
I wish we have human resources technical skills
I wish we have human resources technical skills
I wish there is adequate human resources technical training
I wish there are adequate IT skills
I wish we use HW and SW for professional purposes exclusively
I wish there is hardware redundancy
I wish we identify process stakeholders
I wish we promote identity management
I wish we perform IT impact analysis
I wish we perform IT impact analysis
I wish we perform IT impact analysis
I wish we perform IT impact analysis
I wish we implement best practices
I wish we improve communication among team members
I wish we maximize the incident response team efficiency
I wish the IT department is included in decisions
I wish all enterprise areas are informed about existing risks
I wish there is information authenticity
I wish there is information availability
I wish there is information availability
I wish there is information availability
I wish there is information availability
I wish there is information confidentiality
I wish there is information confidentiality
I wish information criticality is defined
I wish there is adequate destruction of information
I wish there is information integrity
I wish there is information integrity
I wish there is information integrity
I wish there is adequate information protection
I wish information recovery time is minimized
I wish information is reliable
I wish information is reliable

Appendix

I wish information sharing is maximized
I wish information sharing is maximized
I wish there is adequate information systems protection
I wish that the information value is defined
I wish that the information value is defined
I wish the infrastructure is updated
I wish we adopt innovative solutions
I wish we adopt solutions that interact with other systems
I wish there are internal team technical skills
I wish we minimize the exposure of systems to Internet
I wish we evaluate the investment time of life
I wish we involve business data owners
I wish we involve other people in decisions
I wish we involve technological partners
I wish we maximize the autonomy of the IT department
I wish IT is involved in decisions as early as possible
I wish there are adequate IT skills
I wish there is training of IT skills
I wish we promote IT staff mobility
I wish there is IT Staff technical training
I wish we minimize authenticated users
I wish we adopt key user participation in IT decisions
I wish we promote technology know how
I wish every employee knows the security policy
I wish there are knowledge management measures
I wish we promote knowledge sharing
I wish there are business continuity measures
I wish there is adequate communication in different IT areas
I wish there is an adequate infrastructure
I wish there is a IT culture in political management
I wish there is a IT strategy
I wish there is adequate technical skills
I wish there is adequate user training
I wish there is leadership
I wish we promote the least privilege principles
I wish we maximize legal compliance
I wish we maximize legal compliance
I wish legal requirements remain stable
I wish legal requirements remain stable
I wish we limit access to external consultants
I wish we limit automated access
I wish we limit indirect information flows
I wish we limit the number of maximum processes per user in a system
I wish we limit remote management of systems
I wish we have logging of operations

Appendix

I wish we have logical and physical infrastructure redundancy
I wish the business remains interested in the IT service provided
I wish loss of information is minimized
I wish the loss of reputation due to security issues is minimized
I wish staff competencies are maintained
I wish maintenance tasks are automated
I wish there is adequate maintenance of infrastructure
I wish maintenance costs are minimized
I wish systems appear invisible to the user
I wish the IT solution is easy to manage
I wish there is more management commitment in IT projects
I wish there is more management involvement in IT projects
I wish there is no media pressure that impact IT solutions
I wish we collect IT metrics
I wish we minimize computer bugs exploited by malware
I wish we minimize IT costs
I wish we minimize IT downtime
I wish we minimize the IT exposure factor
I wish we minimize impact of human failures with detailed processes documented
I wish we minimize mobile equipment theft
I wish we minimize IT project delays
I wish we minimize the risk of network security assets compromise
I wish we minimize the risk of online banking fraud
I wish we minimize the risk of password theft
I wish we minimize the exploitation of security vulnerabilities
I wish we minimize the impact in case of IT failure
I wish we assure minimum privilege
I wish we minimize mission critical system failures
I wish we monitor external consultants in IT maintenance tasks
I wish we maximize the IT monitorization
I wish we maximize the IT monitorization
I wish we promote employee motivation
I wish the network administrator has undergone security training
I wish we assure network data protection
I wish we assure network segmentation
I wish there is no personal equipment connected to the enterprise
I wish we adopt non disclosure agreements
I wish we are able to communicate IT requirements to top management
I wish non public information is protected with a password
I wish we assure non repudiation of operations
I wish we evaluate open source versus commercial software in IT solutions
I wish we maximize operating system security
I wish we optimize IT resources
I wish we optimize code to improve application performance

Appendix

I wish direct orders do not bypass previous planning
I wish we improve partners relationship
I wish we adopt stakeholders risk acceptability measures
I wish we adopt password management measures
I wish we maximize IT performance
I wish we maximize IT performance
I wish we assure network perimeter security
I wish we perform periodical audits
I wish we perform periodical backups
I wish we assure personal data privacy
I wish there is physical access control to building areas
I wish we protect physical facilities
I wish there is physical hazards protection
I wish we promote physical security
I wish we promote physical security
I wish there is adequate backup planning
I wish IT work is planned with partners
I wish there is adequate IT planning
I wish policies and procedures are documented
I wish IT is not affected by political decisions
I wish IT is not affected by political pressure
I wish the IT team adopts a positive attitude
I wish there is adequate IT planning
I wish we are able to predict consequences of IT failures
I wish we are able to preserve human life in case of failure
I wish we can prevent identity theft
I wish we can prevent single point of failure
I wish we can maximize privacy
I wish we can maximize privacy
I wish we can minimize privacy issues
I wish we promote proactive IT monitorization
I wish we adopt best practices
I wish there is a process to maintain company know how
I wish we can assure product scalability
I wish we can prevent productivity loss
I wish we can assure project autonomy
I wish we can assure project confidentiality
I wish we develop adequate project management methodology
I wish we develop project monitoring
I wish we promote project portfolio management
I wish we can simplify projects
I wish we promote meetings to improve communication
I wish we develop a proof of concept
I wish we protect access to physical infrastructure
I wish we protect clients data

Appendix

I wish we can protect legacy IT
I wish we protect the network with firewalls
I wish we protect IT from physical hazards
I wish we protect stakeholders information
I wish we protect the clients data
I wish we protect user data
I wish there is protection versus virus and malware
I wish we implement quality of service
I wish we define quality of service levels
I wish we question solutions proposed by external consultants
I wish we can recruit IT specialists
I wish we can minimize the number of different partners
I wish we can reduce technological dispersion
I wish we have redundancy of skills in IT
I wish we evaluate time to replace of infrastructure
I wish we evaluate the reliability of infrastructure
I wish we minimize people's resistance to change
I wish we promote adequate resource management
I wish we optimize resources
I wish we promote responsibility
I wish IT results are aligned with business needs
I wish we evaluate the return of investment of IT solutions
I wish we evaluate the return of investment of IT solutions
I wish the RFI includes penalties for information unavailability
I wish we minimize the risk of not accomplishing project deadlines
I wish we optimize the risk management process
I wish there is a clear role definition of key users
I wish there are rollback measures in case of attack
I wish there is rollback plan in IT solution implementation
I wish we promote sandboxing
I wish the can assure the scalability of IT solutions
I wish we implement secure communications
I wish we secure data sharing
I wish we secure online money
I wish we promote secure programming best practices
I wish we promote security clearance measures
I wish we implement a security committee
I wish we implement security metrics
I wish we adopt security policies
I wish we adopt security policies
I wish we adopt security policies
I wish we adopt security policies for external consultants
I wish we perform security tests
I wish we segment networks based on information value
I wish we segregate internal and external users

Appendix

I wish we promote separation of privileges
I wish we define service criticality levels
I wish we define service prioritization levels
I wish we perform systematic log analysis
I wish we develop skills to develop IT apps internally
I wish we implement sla management and review measures
I wish we monitor software licensing
I wish we identify software requirements
I wish we assure software is updated
I wish we minimize solution costs
I wish we implement IT staff evaluation measures
I wish we involve stakeholders in IT decisions
I wish we adopt state of the art technology
I wish we promote strong authentication
I wish we promote strong authentication based on work position
I wish we assure support with defined SLA
I wish we assure sustained growth
I wish we assure system reliability
I wish we define systems criticality
I wish we implement systems hardening
I wish we implement systems monitorization
I wish we keep systems updated
I wish we keep systems updated
I wish there is task delegation and clear responsibility
I wish we encourage team spirit
I wish we ensure team stability
I wish we have IT staff with adequate technical skills
I wish we encourage technological innovation
I wish we evaluate technology maturity
I wish we have IT staff with adequate technical skills
I wish we test application
I wish we test knowledge of security policies
I wish we test processes periodically
I wish we have separate test and quality environments
I wish we perform threat analysis
I wish we perform threat analysis
I wish we perform threat management
I wish we define time and effort to recover data
I wish we define time to recover protected data
I wish we maximize top management involvement
I wish we maximize top management involvement
I wish we maximize top management satisfaction
I wish we implement network traffic management
I wish we minimize transaction time
I wish we achieve trust to manage data

Appendix

- I wish we update the infrastructure
- I wish we update software through reliable sources
- I wish we use encryption for external connections
- I wish we adopt user access policies
- I wish we promote user security awareness
- I wish we achieve user psychological acceptability of IT solutions
- I wish we perform user security awareness training
- I wish we train users after a new IT solution implementation
- I wish we reduce users panic due to IT security issues
- I wish we evaluate value for money versus project uptime
- I wish we define asset value
- I wish we prevent vendor lock out
- I wish we implement virtualization
- I wish the staff works as a team
- I wish we involve hr in IT security decisions