



DIGITAL RISK MANAGEMENT

ANALYSIS OF GATOR SMART WATCH

Dinesh Servamsetty

WHAT IS A RISK?

A risk is constituted whenever a threat is capable of accessing an valuable asset by exploiting a vulnerability and circumventing existing security measures.

GATOR: GATHER TOGETHER

Gator Group Co., Ltd is established in 2009. We are dedicated to providing the best GPS Tracking Solutions for every family, organization and government in the world.

Gator GPS watches for both kids and elders have been sold to over 60 countries, including Europe, Australia, America, Canada and Asia, etc.

We have our own factory and strong R&D team to offer you not only high-quality GPS watches, but also highly stable App.

Gator smart watch

Gator application

Users/Parents

GPS

SON OF ACTORS

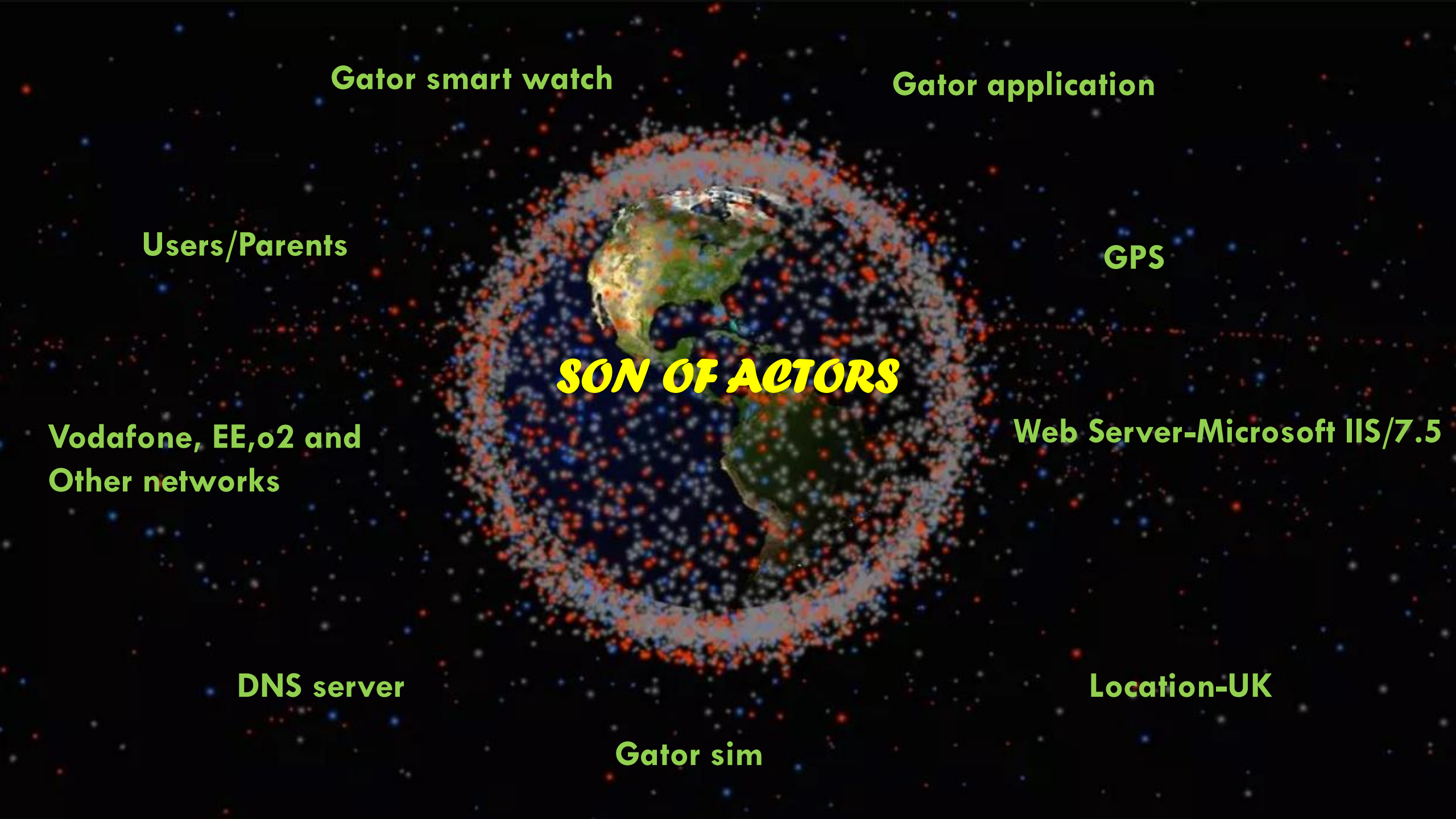
**Vodafone, EE, o2 and
Other networks**

Web Server-Microsoft IIS/7.5

DNS server

Location-UK

Gator sim



GATOR SMART WATCH-OBASHI

GATOR SMART WATCH-OBAHSI							
OBASHI	A	B	C(Gator Sim)	D(ISP)	E(DNS Server)	F(Gator Web Server)	G(Database)
Ownership	User/Parent	User	Gator Sim	Gator	DNS server	Microsoft-IIS/7.5	Database
Bussiness	User	User	Gator	Gator	DNS	Microsoft-IIS	Gator database server
Application	Gator Application	Gator Application	Gator Application	Gator Application	DNS	Microsoft-IIS	Gator database server
System	Gator OS	Gator OS	Gator OS	Gator OS	Gator OS	Microsoft-IIS	Gator database server
Hardware	Gator Smart Watch	Gator Smart Watch	Gator Smart Watch	Gator Smart Watch	Gator Smart Watch	Firewall, IDS,IPS	Firewall, IDS,IPS
Infrastructure	Internet/Wifi	2G/3G	2G/3G	2G/3G	2G/3G	Cisco routers/switches	Cisco routers/switches
Geography	United Kingdom	United Kingdom	United Kingdom	United Kingdom	China	China	China

HACKER STORIES

HS1

As a black hat hacker, launching DDOS attack on gator server for one week to stop the service.

HS2

As a hacker, I want to perform Man-in-the-middle attack between user and server to intercept the network traffic between children smart watch and parents mobile.

HS3

As a cyber terrorist, redirecting all the emergency contacts(SOS ALERT) of all the users to police department of its own country.

HS4

As a sponsored hacker by gator competitor, spreading RANSOMEWARE to gator smart watches to stop its access for all users.

HS5

As a black hat hacker, I want to insert ransomware in database to lock it and demand ransom of \$20Million to unlock it.

HS7

As a competitor, I want to delete all the user's data from database.

HS6

As a black hat hacker, hacking gator server to monitor user's daily visiting places

HS8

As a black hat hacker, I want to steal complete database and sell it to other competitors.



HS9

As a stalker, I wanted to steal all the users contact list and use it for harassing them.

HS11


As a hired free lancer, I want to Insert virus in every smart watch to drain battery within one hour

HS10

As a competitor, I want to stop all gator sim's from working (For 1 week).

HS12

As a hacker, I want to stop gator GPS service for 1 week.





HS13

As a script kiddie, I want to display wrong steps for all users during their walk.



HS15

As a black hat hacker, I want to change users email id's, passwords to lock them out of their users.



HS14

As a hacker, I want to stop the notification alert when watchband is off.



HS16

As a hacker, I want to stop remote voice monitoring.

HS17

AS a Gray hat hacker, I want to remove security features to the database and allow access to everyone.

HS19

As a black hat hacker, I want to change users pre-set contacts to some other contact numbers.

HS18

As a robbery organization, remotely recording the top politicians users voice and use it for access to their banking lockers which has a voice recognition to open the lockers.

HS20

As a hacker, I want to steal users contact details and sell it to online marketing companies.

RISK ASSESMENT

IMPACT

High

Medium

Low

	HS3 HS11 HS15 HS17 HS20	HS1 HS4 HS5 HS7 HS10 HS12
HS2 HS16	HS6 HS9	HS8
HS14 HS18	HS19	HS13

Low

Medium

High

PROBABILITY

SECURITY MEASURES

HS:1

- (1) Train the operational teams in information system security
- (3) Control outsourced services
- (4) Identify the most sensitive information and servers and keep a network diagram
- (7) Only allow controlled devices to connect to the network of the organization
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (32) Secure the dedicated network interconnections with partners
- (34) Define and apply a backup policy for critical components
- (38) Undertake regular controls and security audits then apply the associated corrective actions
- (39) Designate a point of contact in information system security and make sure staff are aware of him or her
- (40) Define a security incident management procedure
- (41) Carry out a formal risk assessment

HS:2

- (2) Raise users' awareness about basic information security
- (18) Encrypt sensitive data sent through the Internet
- (20) Ensure the security of Wi-Fi access networks and that users are separated
- (22) Implement a secure access gateway to the Internet

HS:3

- (4) Identify the most sensitive information and servers and keep a network diagram
- (5) Have an exhaustive inventory of privileged accounts and keep it update
- (7) Only allow controlled devices to connect to the network of the organization
- (8) Identify each individual accessing the system by name and distinguish the user/administrator roles
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (18) Encrypt sensitive data sent through the Internet
- (19) Segment the network and implement a partitioning between these areas
- (22) Implement a secure access gateway to the Internet
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (29) Reduce administration rights on workstations to strictly operational needs
- (31) Encrypt sensitive data, in particular on hardware that can potentially be lost
- (38) Undertake regular controls and security audits then apply the associated corrective

HS:4

- (2) Raise users' awareness about basic information security
- (7) Only allow controlled devices to connect to the network of the organization
- (14) Implement a minimum level of security across the whole IT stock
- (15) Protect against threats relating to the use of removable media
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:5

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced service
- (4) Identify the most sensitive information and servers and keep a network diagram
- (5) Have an exhaustive inventory of privileged accounts and keep it updated
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:6

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (26) Control and protect access to the server rooms and technical areas
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:7

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (19) Segment the network and implement a partitioning between these areas
- (26) Control and protect access to the server rooms and technical areas
- (31) Encrypt sensitive data, in particular on hardware that can potentially be lost
- (37) Define and apply a backup policy for critical components

HS:8

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (19) Segment the network and implement a partitioning between these areas

HS:9

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (4) Identify the most sensitive information and servers and keep a network diagram
- (7) Only allow controlled devices to connect to the network of the organization
- (14) Implement a minimum level of security across the whole IT stock
- (26) Control and protect access to the server rooms and technical areas
- (31) Encrypt sensitive data, in particular on hardware that can potentially be lost

HS:10

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (4) Identify the most sensitive information and servers and keep a network diagram
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (14) Implement a minimum level of security across the whole IT stock
- (37) Define and apply a backup policy for critical component

HS:11

- (14) Implement a minimum level of security across the whole IT stock
- (15) Protect against threats relating to the use of removable media
- (26) Control and protect access to the server rooms and technical areas
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:12

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (14) Implement a minimum level of security across the whole IT stock
- (25) Secure the dedicated network interconnections with partners
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:13

- (1) Train the operational teams in information system security
- (7) Only allow controlled devices to connect to the network of the organization
- (8) Identify each individual accessing the system by name and distinguish the user/administrator roles
- (14) Implement a minimum level of security across the whole IT stock
- (21) Use secure network protocols when they exist
- (26) Control and protect access to the server rooms and technical areas
- (29) Reduce administration rights on workstations to strictly operational needs
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:14

- (1) Train the operational teams in information system security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (26) Control and protect access to the server rooms and technical areas
- (34) Define an update policy for the components of the information system
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:15

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (4) Identify the most sensitive information and servers and keep a network diagram
- (7) Only allow controlled devices to connect to the network of the organization
- (8) Identify each individual accessing the system by name and distinguish the user/administrator roles
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (27) Prohibit Internet access from devices or servers used by the information system administration
- (28) Use a dedicated and separated network for information system administration
- (37) Define and apply a backup policy for critical component
- (38) Undertake regular controls and security audits then apply the associated corrective actions
- (39) Designate a point of contact in information system security and make sure staff are aware of him or her
- (40) Define a security incident management procedure

HS:16

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (38) Undertake regular controls and security audits then apply the associated corrective actions

HS:17

- (1) Train the operational teams in information system security
- (7) Only allow controlled devices to connect to the network of the organization
- (8) Identify each individual accessing the system by name and distinguish the user/administrator roles
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (16) Use a centralised management tool to standardise security policies
- (19) Segment the network and implement a partitioning between these areas

HS:18

- (2) Raise users' awareness about basic information security
- (18) Encrypt sensitive data sent through the Internet
- (30) Take measures to physically secure mobile devices
- (33) Adopt security policies dedicated to mobile devices

HS:19

- (4) Identify the most sensitive information and servers and keep a network diagram
- (5) Have an exhaustive inventory of privileged accounts and keep it update
- (7) Only allow controlled devices to connect to the network of the organization
- (8) Identify each individual accessing the system by name and distinguish the user/administrator roles
- (9) Allocate the correct rights to the information system's sensitive resources
- (14) Implement a minimum level of security across the whole IT stock
- (17) Activate and configure the firewall on workstations
- (19) Segment the network and implement a partitioning between these areas
- (22) Implement a secure access gateway to the Internet
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (31) Encrypt sensitive data, in particular on hardware that can potentially be lost
- (38) Undertake regular controls and security audits then apply the associated corrective

HS:20

- (1) Train the operational teams in information system security
- (2) Raise users' awareness about basic information security
- (3) Control outsourced services
- (7) Only allow controlled devices to connect to the network of the organization
- (9) Allocate the correct rights to the information system's sensitive resources
- (12) Change the default authentication settings on devices and services
- (14) Implement a minimum level of security across the whole IT stock
- (19) Segment the network and implement a partitioning between these areas
- (25) Secure the dedicated network interconnections with partners
- (26) Control and protect access to the server rooms and technical areas
- (31) Encrypt sensitive data, in particular on hardware that can potentially be lost
- (38) Undertake regular controls and security audits then apply the associated corrective