

**Information Requirements For
Comprehensive Security Assessment - Scope & Budget**



Company Name: _____

Contact Person: _____

Phone: _____

1 • Please provide a current copy of your complete Information Systems topology diagram

2 • Indicate the number and type of **routers** facing the Internet

0

3 • Indicate the number and type of **firewalls** facing the Internet

Watchguard 810 XTM (2)

4 • Indicate the number and type of **switches**

25 Cisco

5 • Indicate the number and type of **VPNs**

NetMotion, PPTP, Branch Office VPN (2)

6 • Indicate the number and type of intrusion detection systems (**IDS**)

Watchguard 810 XTM (2)

7 • Indicate the number and type of intrusion prevention systems (**IPS**)

Watchguard 810 XTM (2)

8 • Indicate if modems are used

SMC D3G

9 • Indicate if wireless access points are used and how many

Cisco (27)

10 • Indicate if mobile devices are used

Yes

11 • Indicate if network or IT system related services are outsourced and indicate the number and names of providers

N/A

12 • Indicate the number and type of computer hardware used (servers, mid-range, mainframe)

Dell

13 • Indicate the type of **operating systems** used

Windows Server 2016, 2012 R2, 2012, 2008 r2, Windows 7 & 10

14 • Indicate the type of **database systems** used

SQL

15 • Indicate the type of **e-mail systems** used

Office 365

16 • Indicate the type of **anti-virus** system used

OfficeScan XG

Information Requirements For
Comprehensive Security Assessment - Scope & Budget



Company Name: _____

Contact Person: _____

17 • Indicate if other type of **malware security** products are used – provide names

OfficeScan XG

18 • Indicate any other security related hardware and software system products used at your organization – provide names (security products, backups, encryption)

N/A

19 • Indicate if **virtualization** is used / If yes, which provider

VMWare

20 • Indicate if **imaging systems** are used

WDS

21 • Indicate if **camera systems** are used

Yes

22 • Indicate if **access cards** systems are used

Yes

23 • Indicate if **voice over IP** is used

Yes

24 • Indicate if **cloud computing** services are used and provide the names of the providers

Office 365, Power DMS, NeoGov, Civic Plus

25 • Indicate the number of critical business applications

5

26 • Indicate critical business application that are web based

1

27 • Indicate critical mobile applications

0

28 • Indicate the software tools used to log and monitor system and user activities

Misc

29 • Indicate any other type of system software running inside the operating systems and indicate the purpose

None

30 • Indicate the type and name of critical data and/or transactions that requires high level of security – indicates where in the infrastructure it resides

Law Enforcement

31 • Indicate if the Payment Card Industry Data Security Standard (PCI DSS) is applicable to the organization – indicate the PCI level

Yes, level 3

**Information Requirements For
Comprehensive Security Assessment - Scope & Budget**



Company Name: _____

Contact Person: _____

32 • Indicate if you need compliance with the ISO27000 security standards

No

33 • Indicate if you need compliance with the NIST security standards

No

34 • Indicate the specific regulations applicable to your organization such as HIPAA, HITECH, GLBA, FACTA, FERPA, and FISMA

HIPAA

35 • Indicate the number of buildings and physical locations and computer data centers

17 buildings, one data center

36 • Indicate if you have an automated access card system

Yes

37 • Indicate if your organization has a security awareness and training program

Yes

38 • Indicate if your organization has a security incident response plan and needs to be tested

Yes

39 • Indicate if your organization has a business continuity plan

Yes

40 • Indicate the number of security policies, standards, procedures, and other critical documents that need to be evaluated (please state the policies you currently have)

not within scope

• Penetration Testing:

41 o External network penetration test – indicate number of IP addresses facing the Internet

16

42 o Internal network penetration test – indicate number of IP addresses facing the Internet

0

43 o Web Application Hacking – indicate number of applications

6

44 o Mobile Application Hacking – indicate number of applications

0

45 o Wireless Penetration Tests – indicate the number of wireless access cards

N/A

46 o Social Engineering – Indicate the number testing scenarios desired – refer to attachment

N/A