www.ekspres.ubb.edu.pl

Zarzadzanie ryzykiem bezpieczeństwa informatycznego: Microsoft Security Assessment Tool (MSAT)

Dla dociekliwych

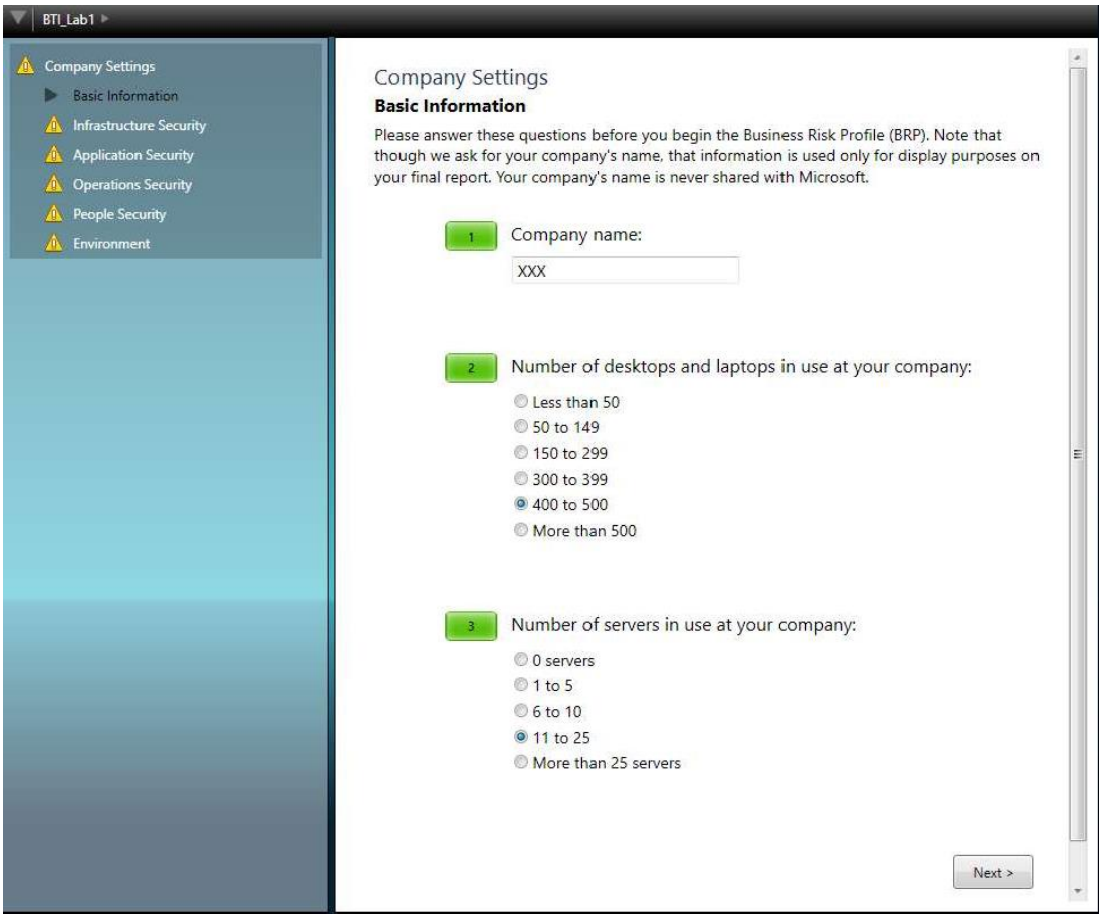
EKSPRES MATURALNY

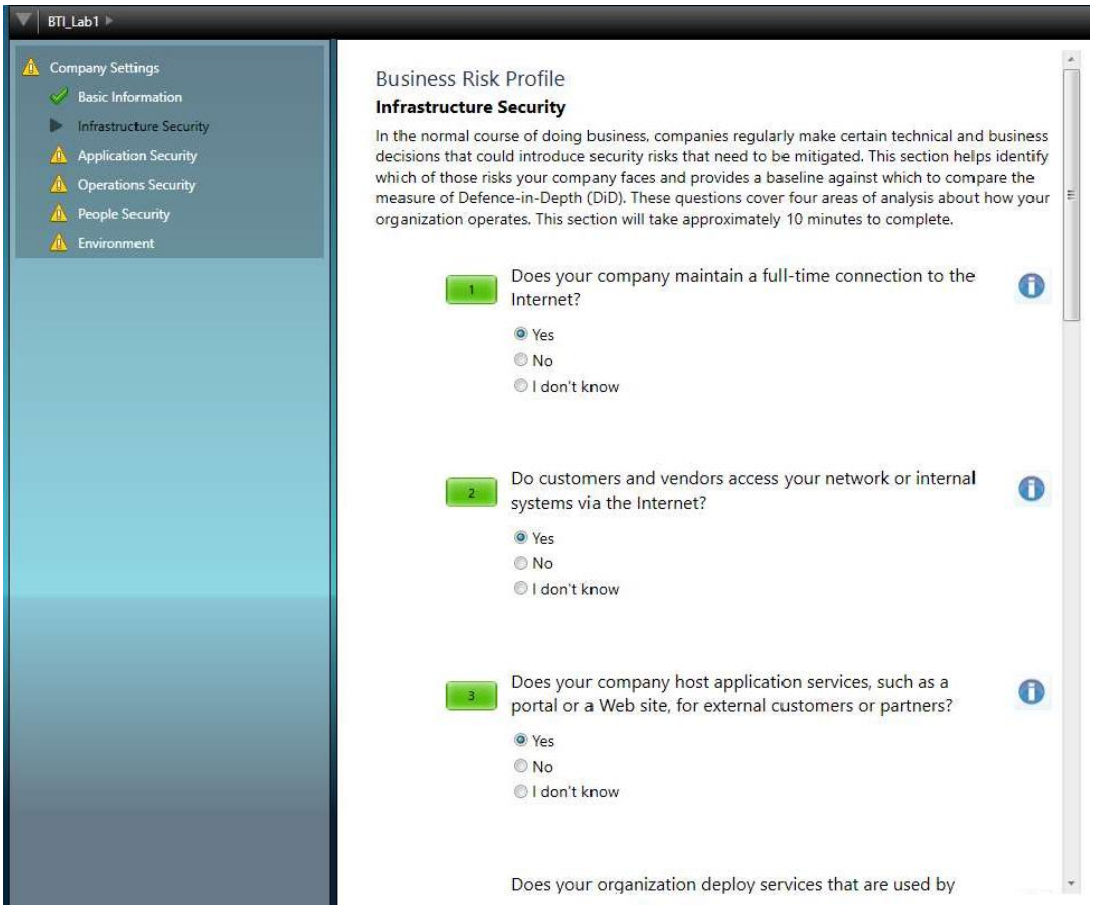
Prof. dr hab. inż. Oleksandr Korchenko
Katedra Informatyki i Automatyki
Wydział Budowy Maszyn i Informatyki

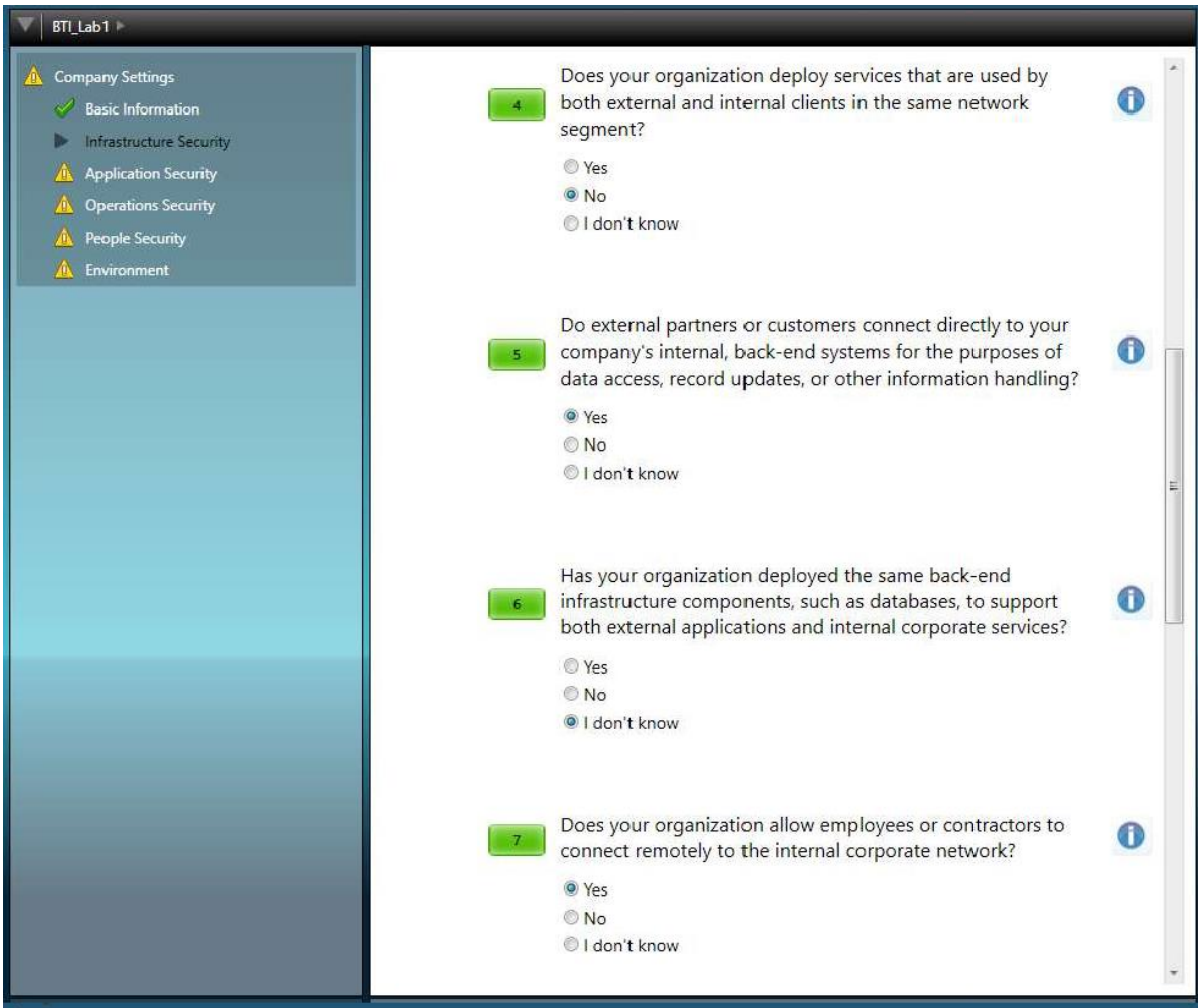
Uniwersytet Bielsko-Bialski

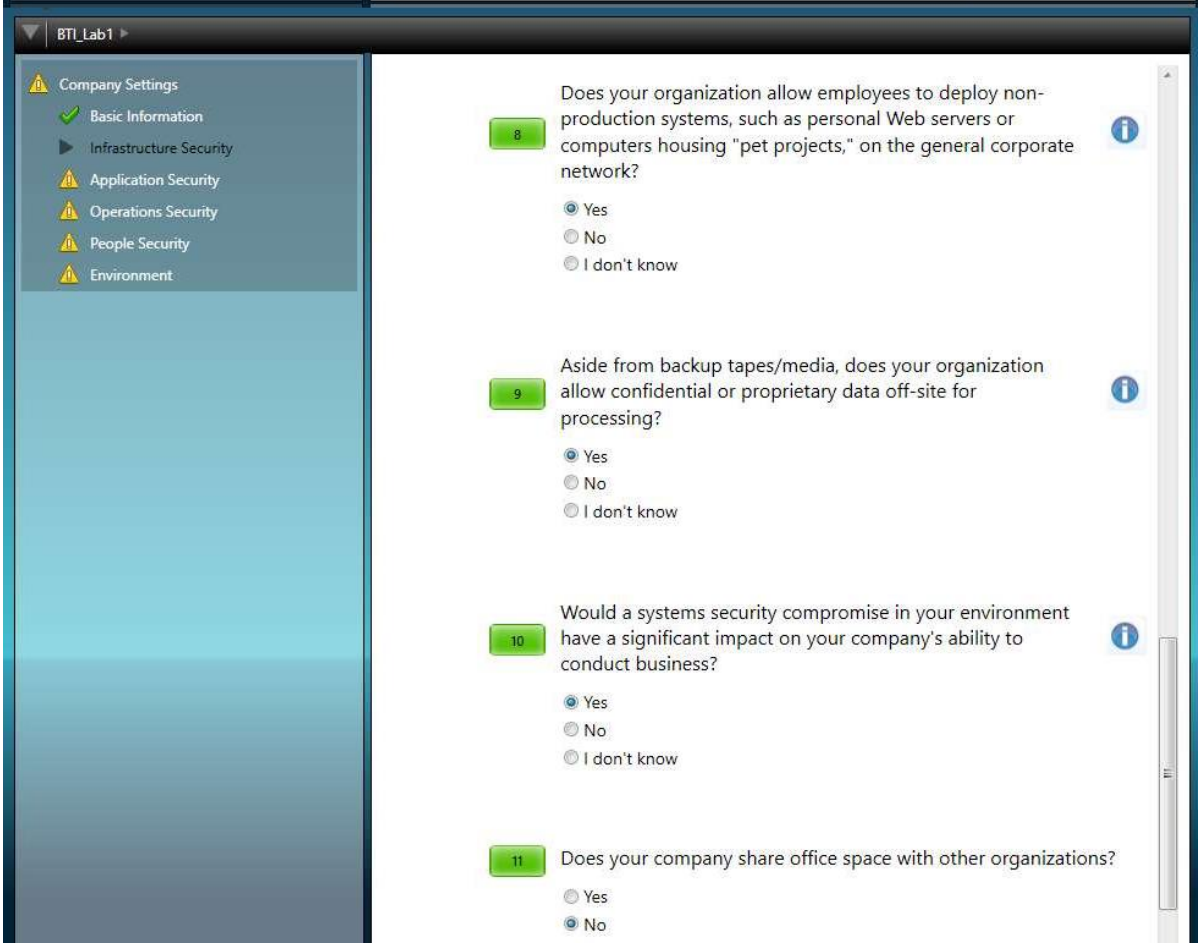
1. Analiza ryzyka przy pomocy programu MSAT

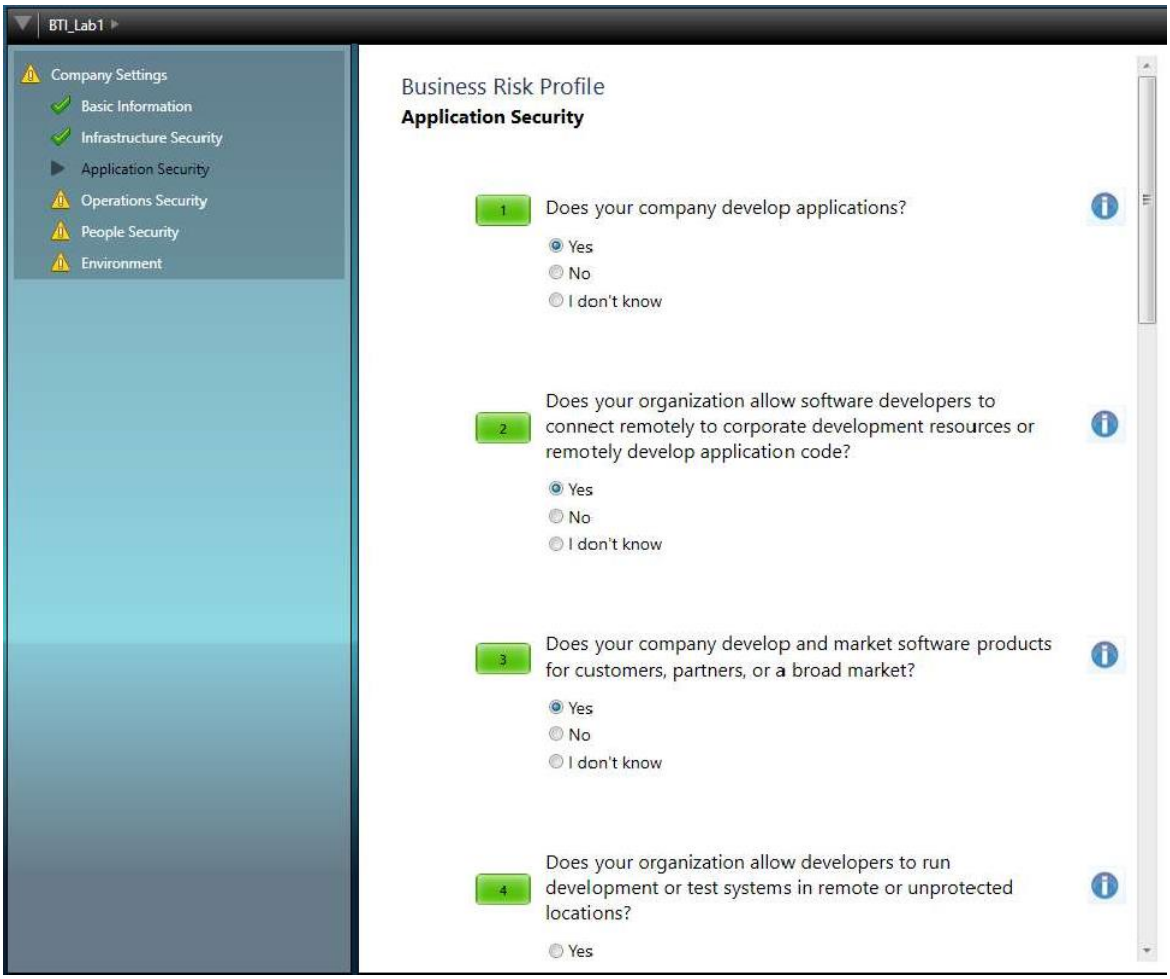
Program umożliwia określenie ryzyka poszczególnych części firmy na podstawie odpowiedzi na zadawane pytania tak jak to zostało pokazane na umieszczonych zdjęciach.

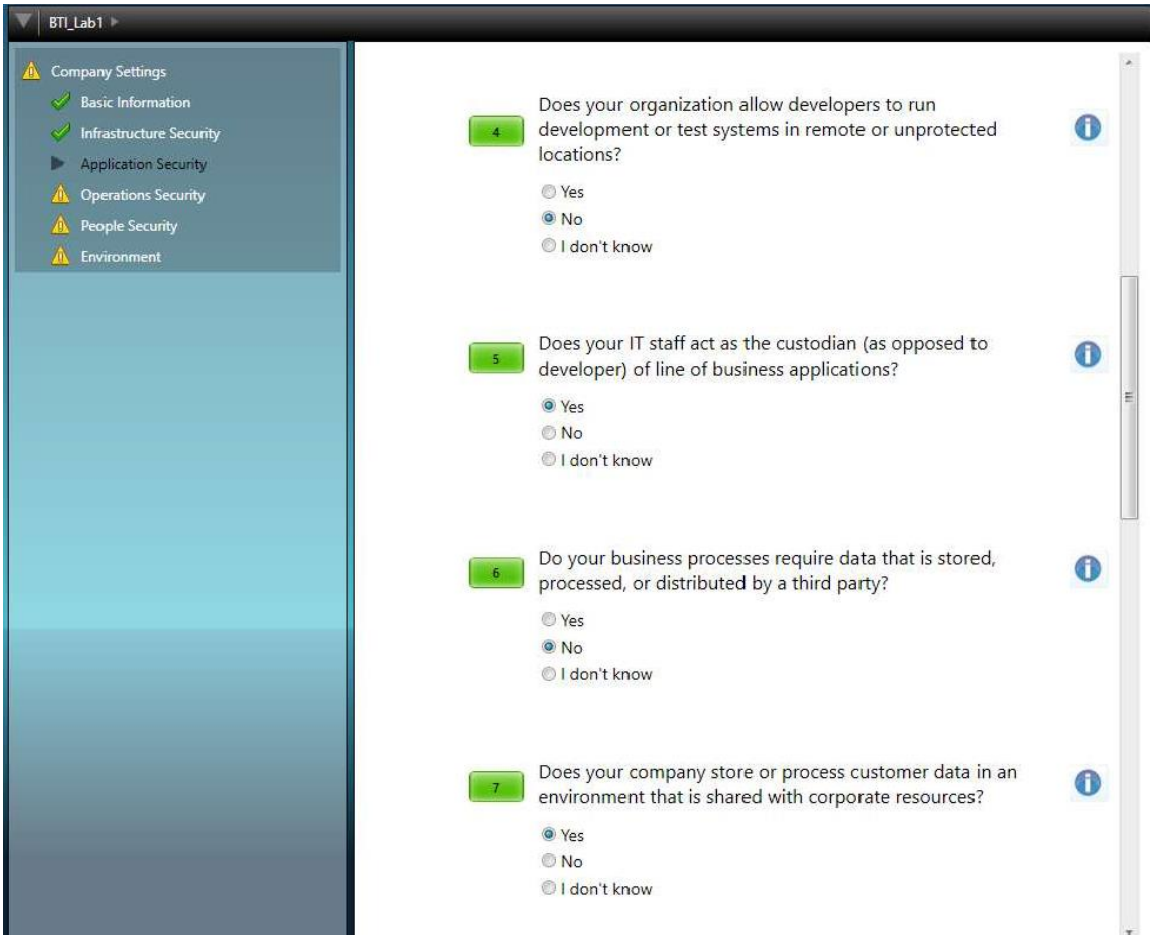


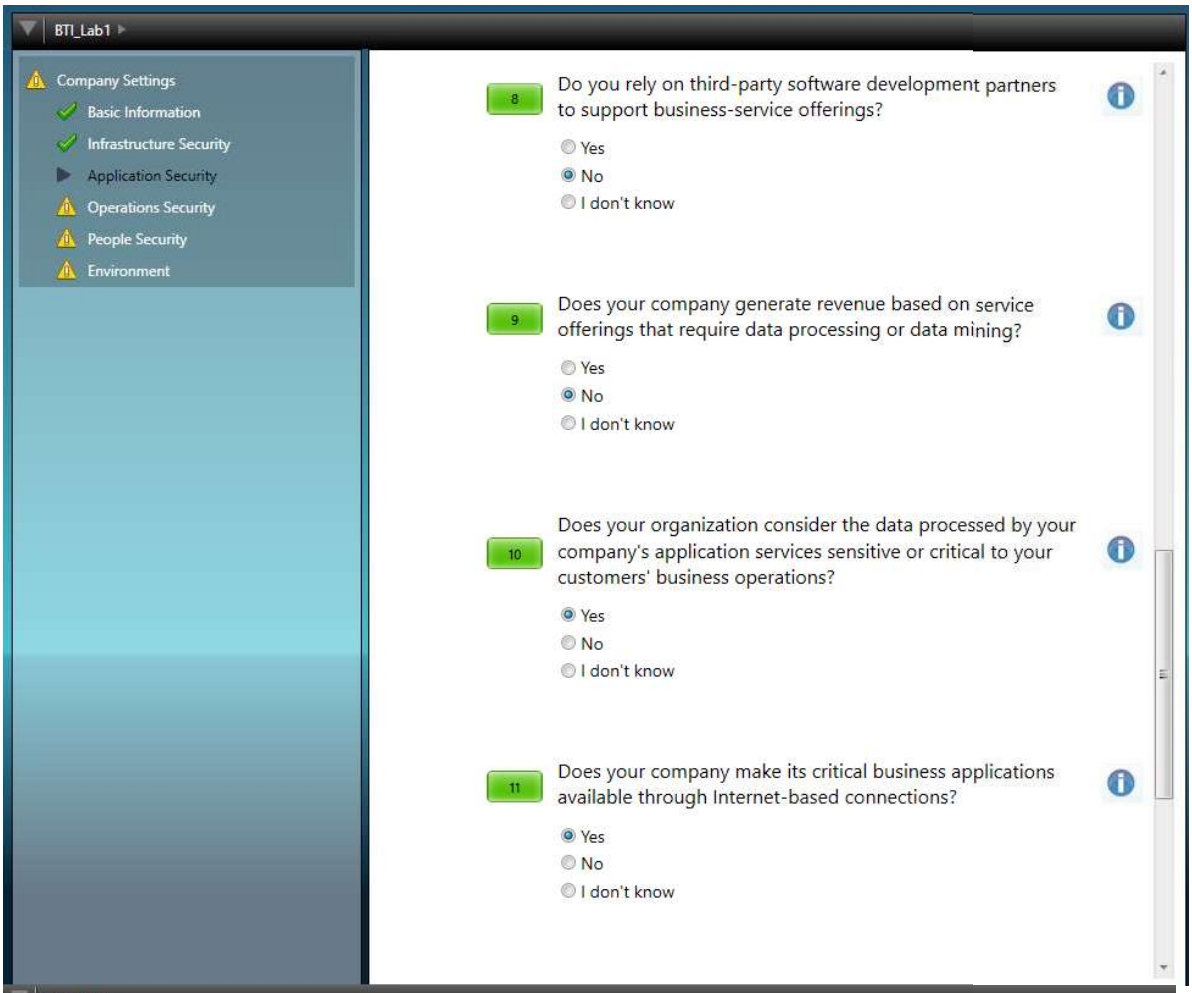

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Business Risk Profile
Infrastructure Security
In the normal course of doing business, companies regularly make certain technical and business decisions that could introduce security risks that need to be mitigated. This section helps identify which of those risks your company faces and provides a baseline against which to compare the measure of Defence-in-Depth (DiD). These questions cover four areas of analysis about how your organization operates. This section will take approximately 10 minutes to complete.
1
Does your company maintain a full-time connection to the Internet?
Yes
No
I don't know
2
Do customers and vendors access your network or internal systems via the Internet?
Yes
No
I don't know
3
Does your company host application services, such as a portal or a Web site, for external customers or partners?
Yes
No
I don't know
Does your organization deploy services that are used by

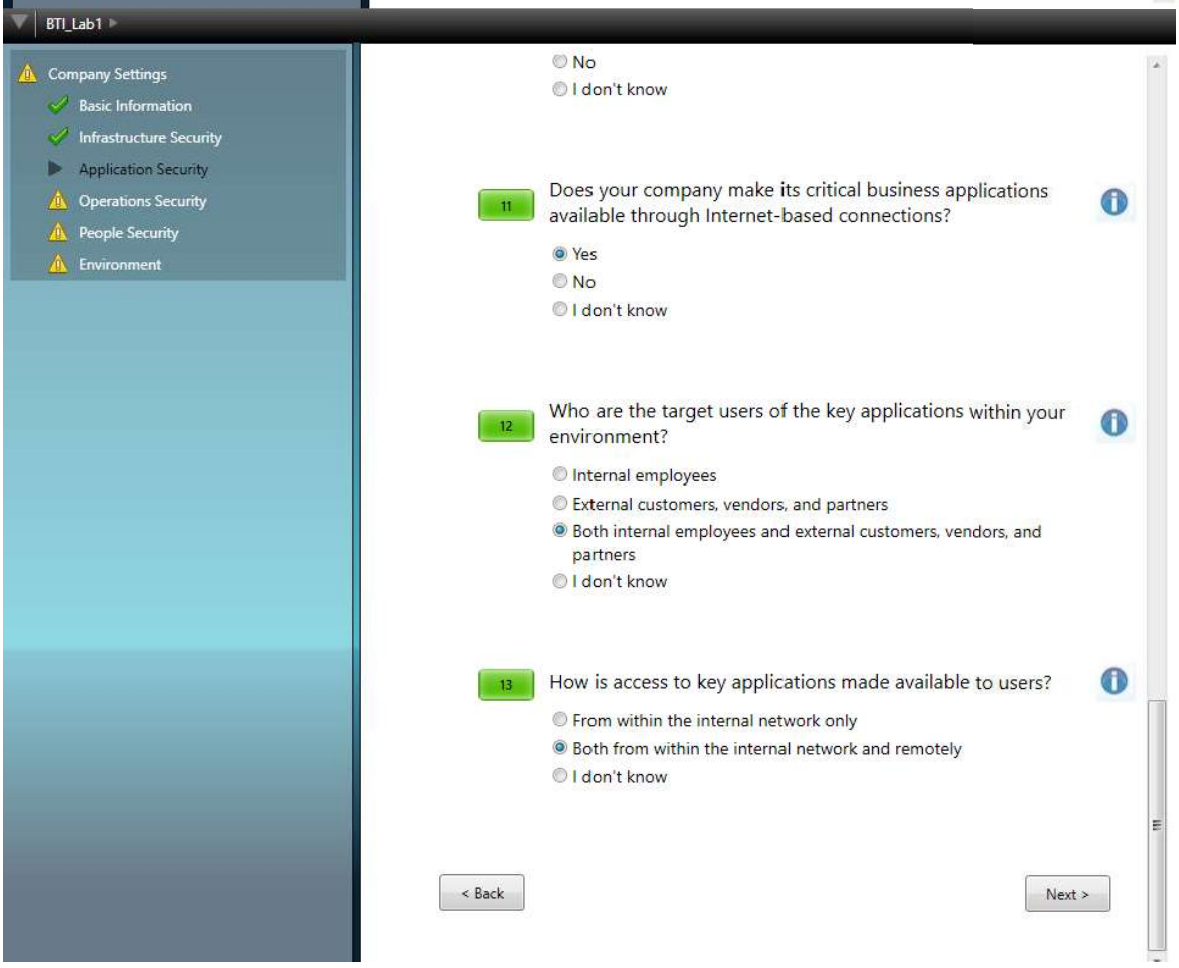

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
4
Does your organization deploy services that are used by both external and internal clients in the same network segment?
Yes
No
I don't know
5
Do external partners or customers connect directly to your company's internal, back-end systems for the purposes of data access, record updates, or other information handling?
Yes
No
I don't know
6
Has your organization deployed the same back-end infrastructure components, such as databases, to support both external applications and internal corporate services?
Yes
No
I don't know
7
Does your organization allow employees or contractors to connect remotely to the internal corporate network?
Yes
No
I don't know

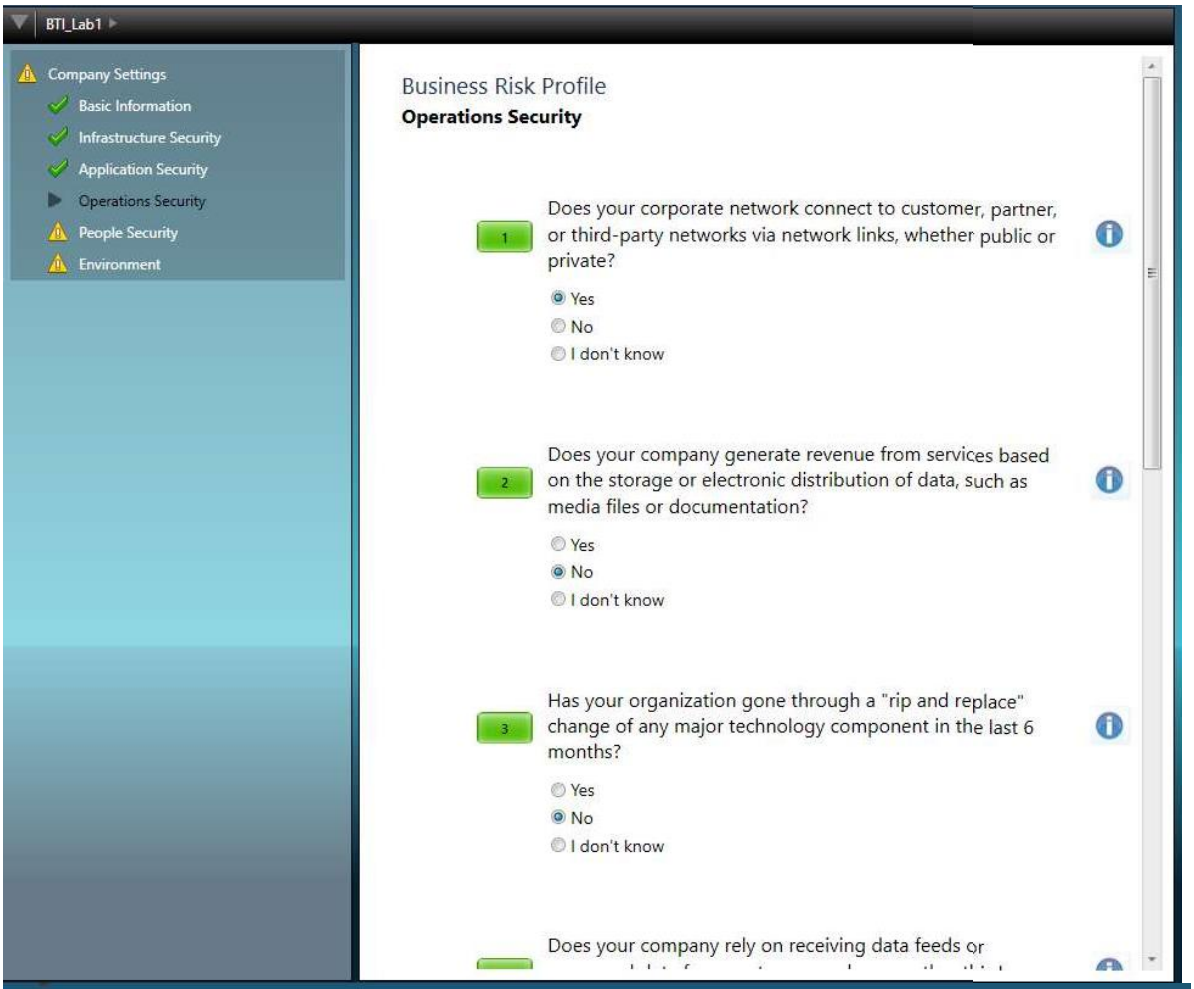

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
8
Does your organization allow employees to deploy non-production systems, such as personal Web servers or computers housing "pet projects," on the general corporate network?
Yes
No
I don't know
9
Aside from backup tapes/media, does your organization allow confidential or proprietary data off-site for processing?
Yes
No
I don't know
10
Would a systems security compromise in your environment have a significant impact on your company's ability to conduct business?
Yes
No
I don't know
11
Does your company share office space with other organizations?
Yes
No

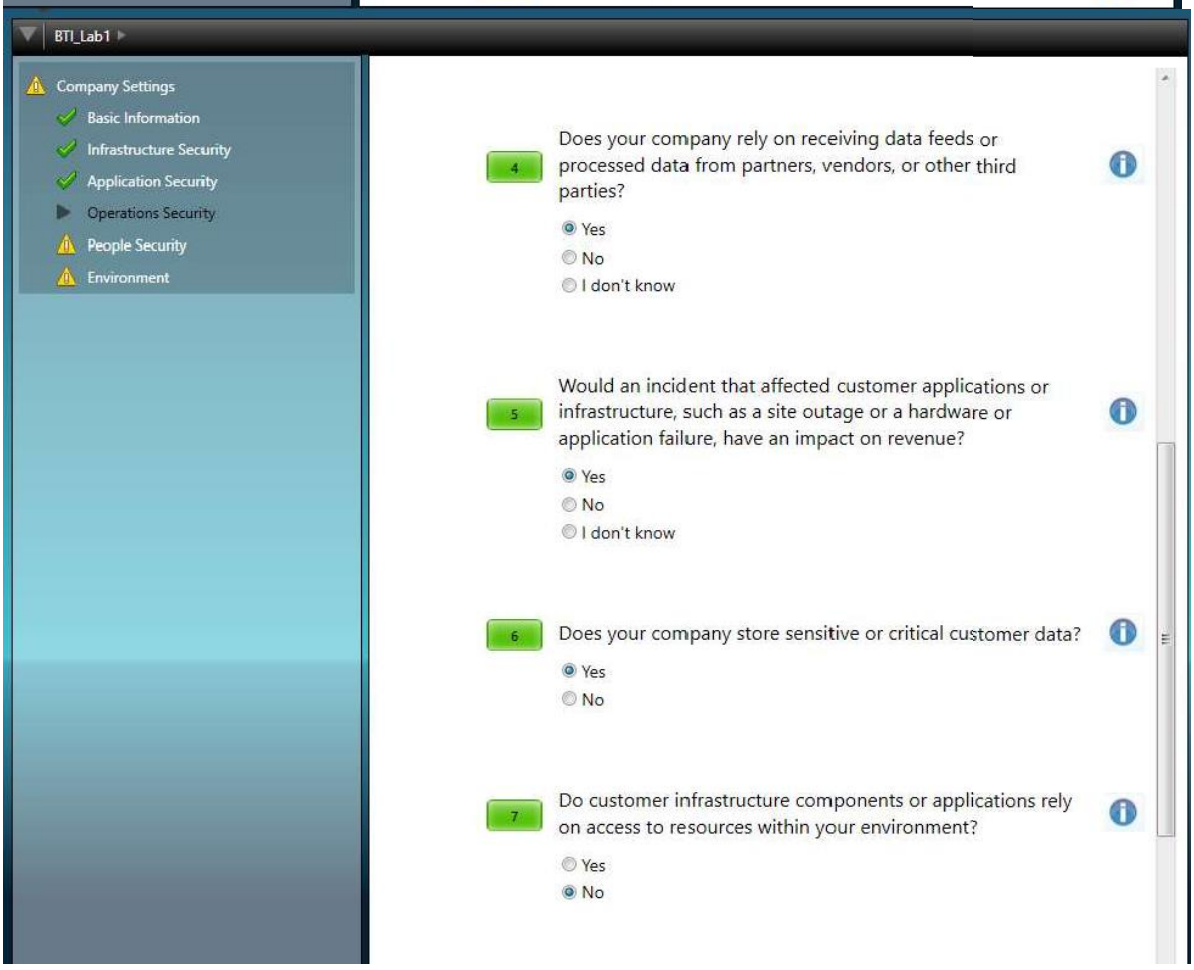

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Business Risk Profile
Application Security
1
Does your company develop applications?
Yes
No
I don't know
2
Does your organization allow software developers to connect remotely to corporate development resources or remotely develop application code?
Yes
No
I don't know
3
Does your company develop and market software products for customers, partners, or a broad market?
Yes
No
I don't know
4
Does your organization allow developers to run development or test systems in remote or unprotected locations?
Yes


BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
4
Does your organization allow developers to run development or test systems in remote or unprotected locations?
Yes
No
I don't know
5
Does your IT staff act as the custodian (as opposed to developer) of line of business applications?
Yes
No
I don't know
6
Do your business processes require data that is stored, processed, or distributed by a third party?
Yes
No
I don't know
7
Does your company store or process customer data in an environment that is shared with corporate resources?
Yes
No
I don't know

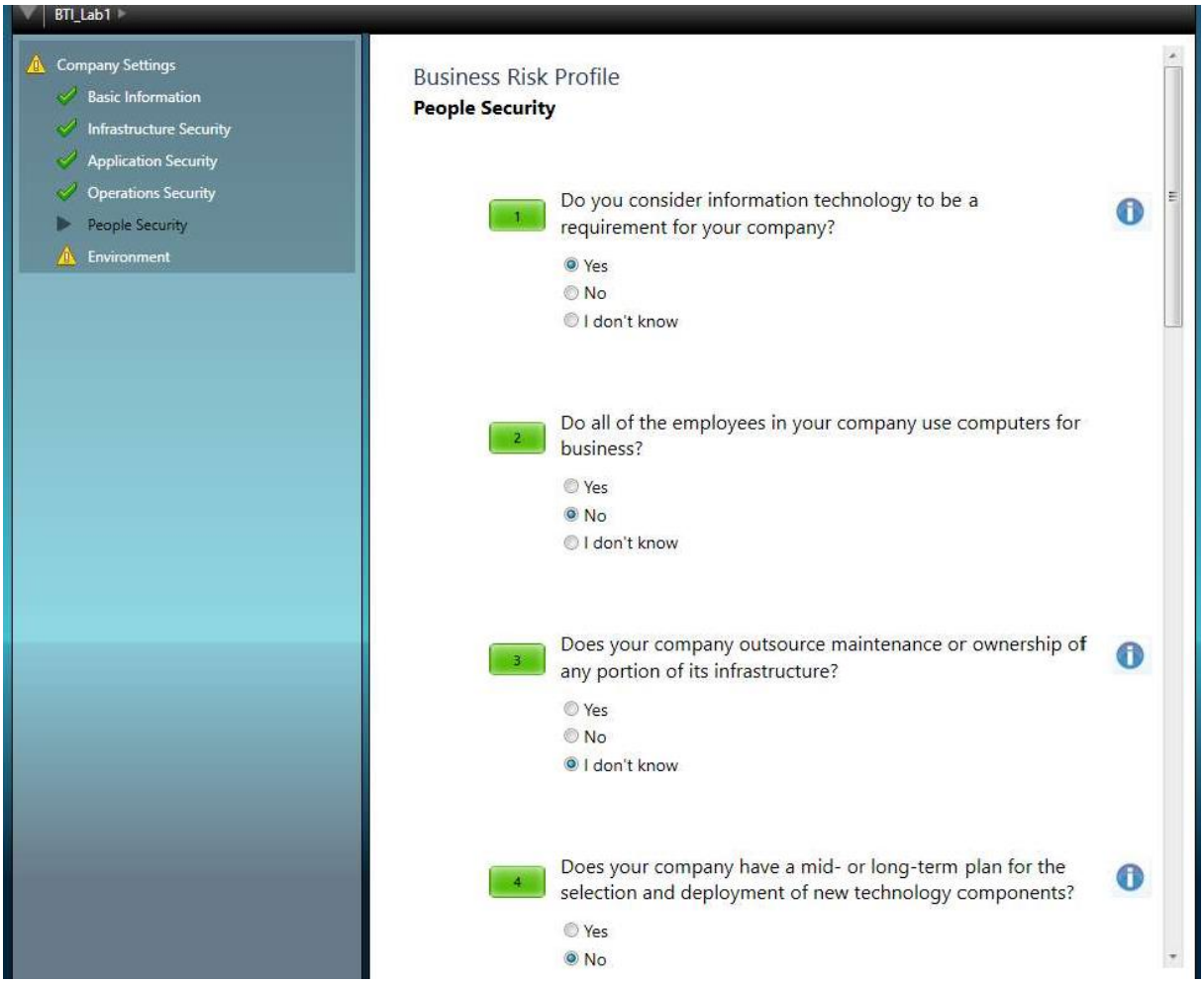

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
8
Do you rely on third-party software development partners to support business-service offerings?
Yes
No
I don't know
9
Does your company generate revenue based on service offerings that require data processing or data mining?
Yes
No
I don't know
10
Does your organization consider the data processed by your company's application services sensitive or critical to your customers' business operations?
Yes
No
I don't know
11
Does your company make its critical business applications available through Internet-based connections?
Yes
No
I don't know

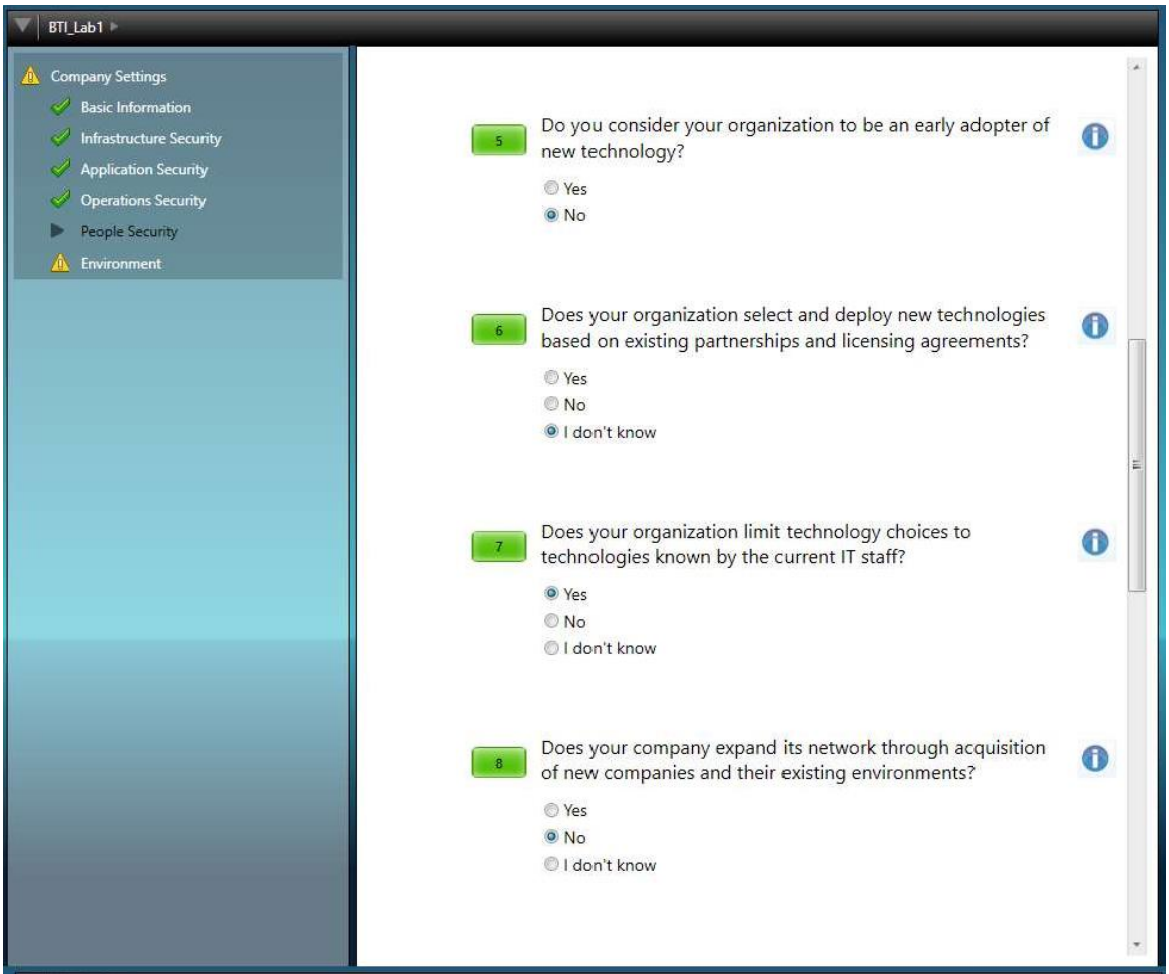

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
No
I don't know
11
Does your company make its critical business applications available through Internet-based connections?
Yes
No
I don't know
12
Who are the target users of the key applications within your environment?
Internal employees
External customers, vendors, and partners
Both internal employees and external customers, vendors, and partners
I don't know
13
How is access to key applications made available to users?
From within the internal network only
Both from within the internal network and remotely
I don't know
< Back
Next >

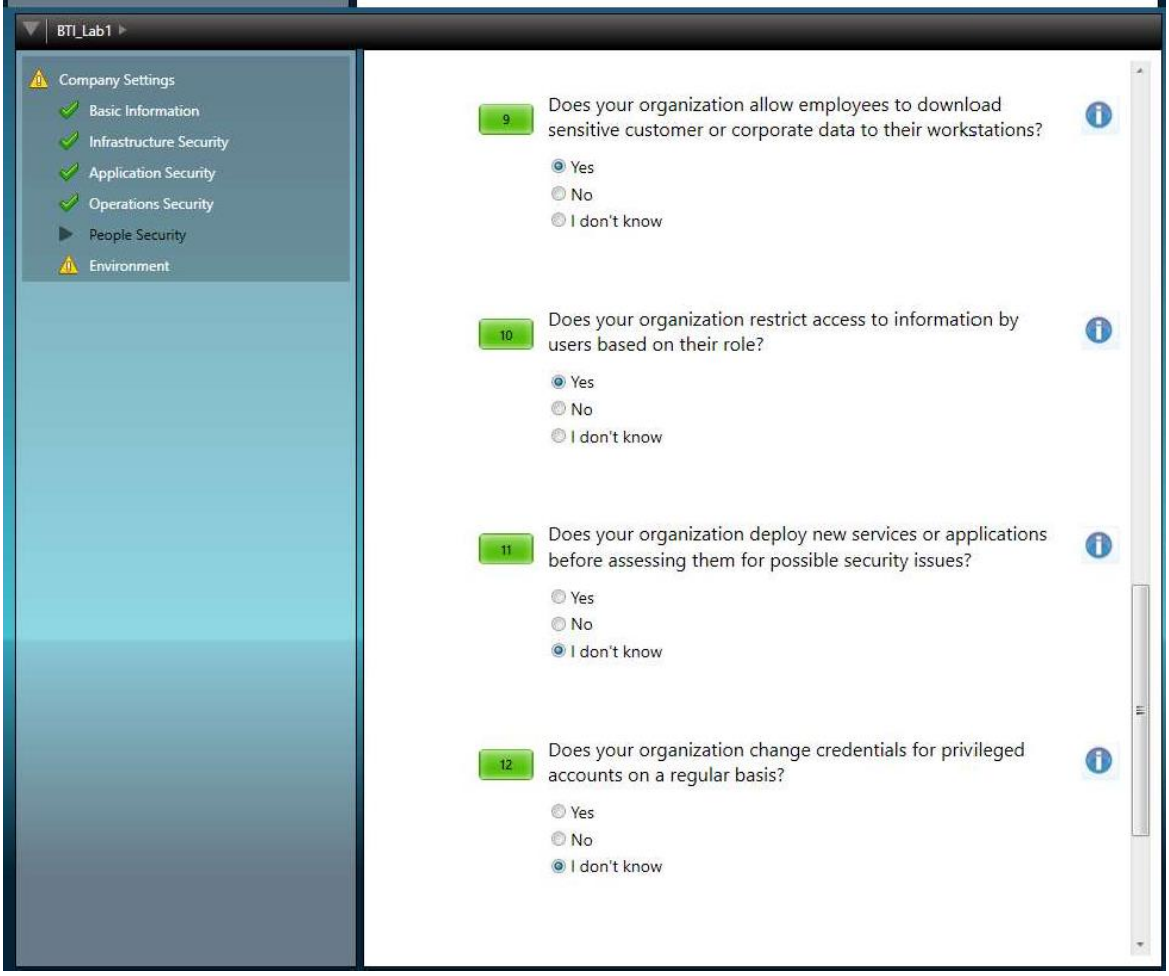

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Business Risk Profile
Operations Security
1
Does your corporate network connect to customer, partner, or third-party networks via network links, whether public or private?
Yes
No
I don't know
2
Does your company generate revenue from services based on the storage or electronic distribution of data, such as media files or documentation?
Yes
No
I don't know
3
Has your organization gone through a "rip and replace" change of any major technology component in the last 6 months?
Yes
No
I don't know
Does your company rely on receiving data feeds or


BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
4
Does your company rely on receiving data feeds or processed data from partners, vendors, or other third parties?
Yes
No
I don't know
5
Would an incident that affected customer applications or infrastructure, such as a site outage or a hardware or application failure, have an impact on revenue?
Yes
No
I don't know
6
Does your company store sensitive or critical customer data?
Yes
No
7
Do customer infrastructure components or applications rely on access to resources within your environment?
Yes
No

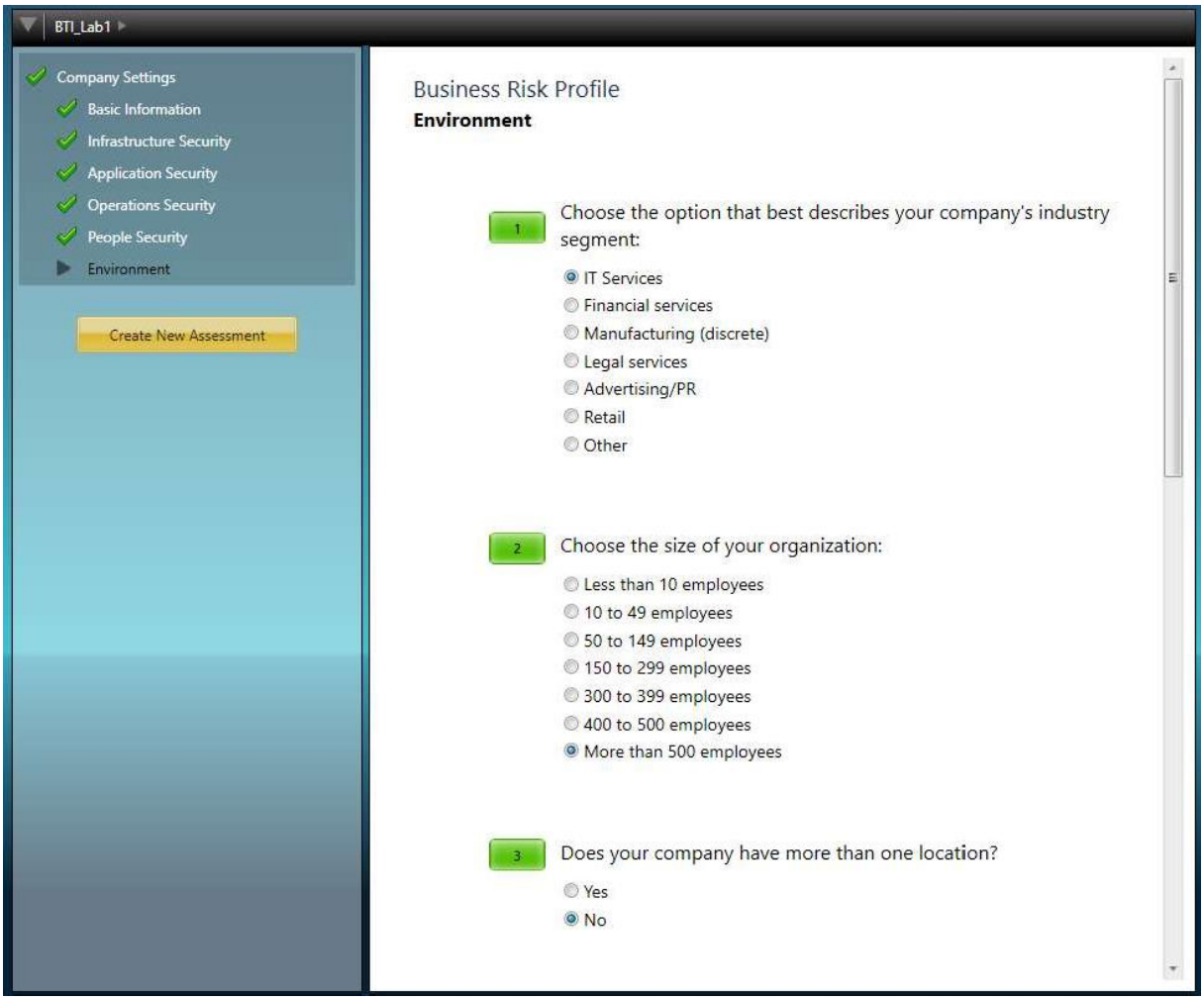

8
Does your company share infrastructure and application components among multiple customers?
Yes
No
< Back
Next >

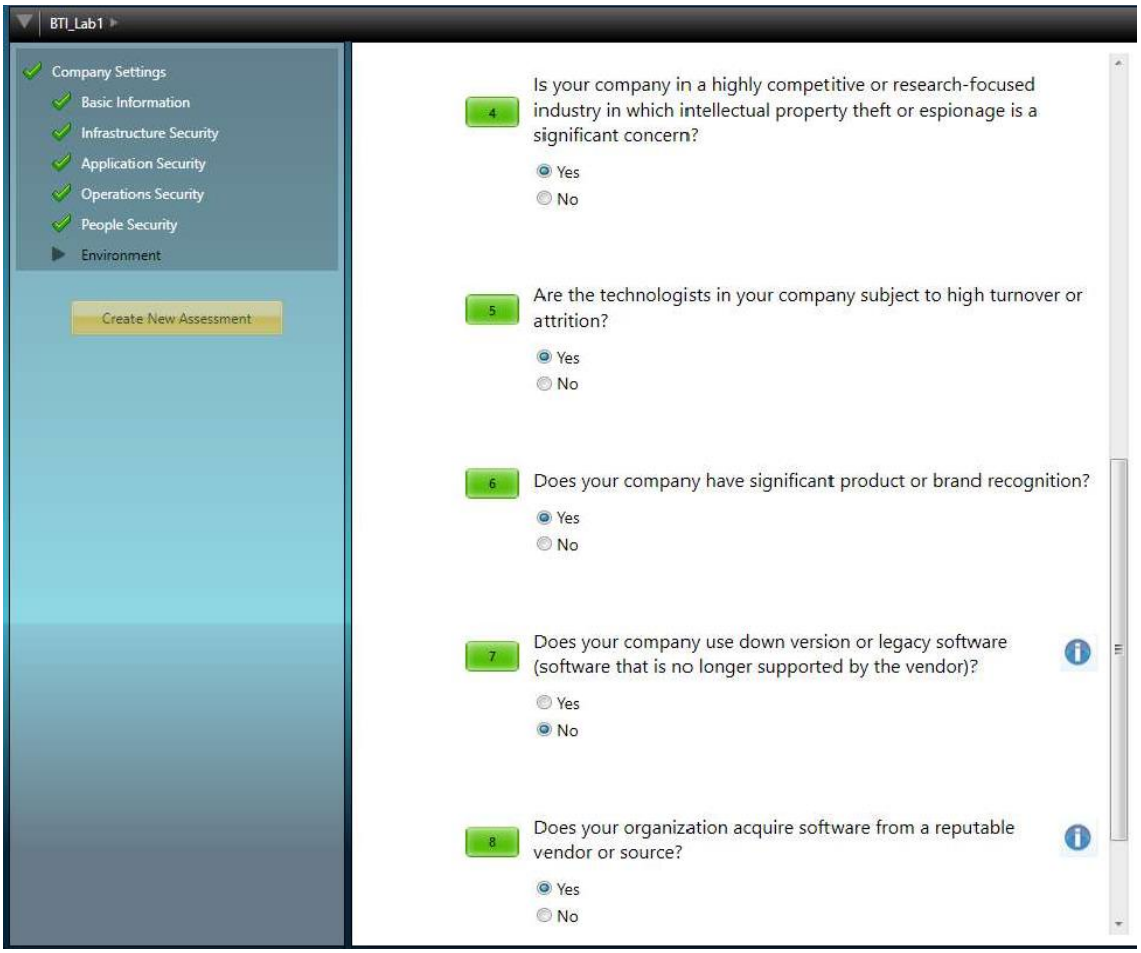

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Business Risk Profile
People Security
1
Do you consider information technology to be a requirement for your company?
Yes
No
I don't know
2
Do all of the employees in your company use computers for business?
Yes
No
I don't know
3
Does your company outsource maintenance or ownership of any portion of its infrastructure?
Yes
No
I don't know
4
Does your company have a mid- or long-term plan for the selection and deployment of new technology components?
Yes
No

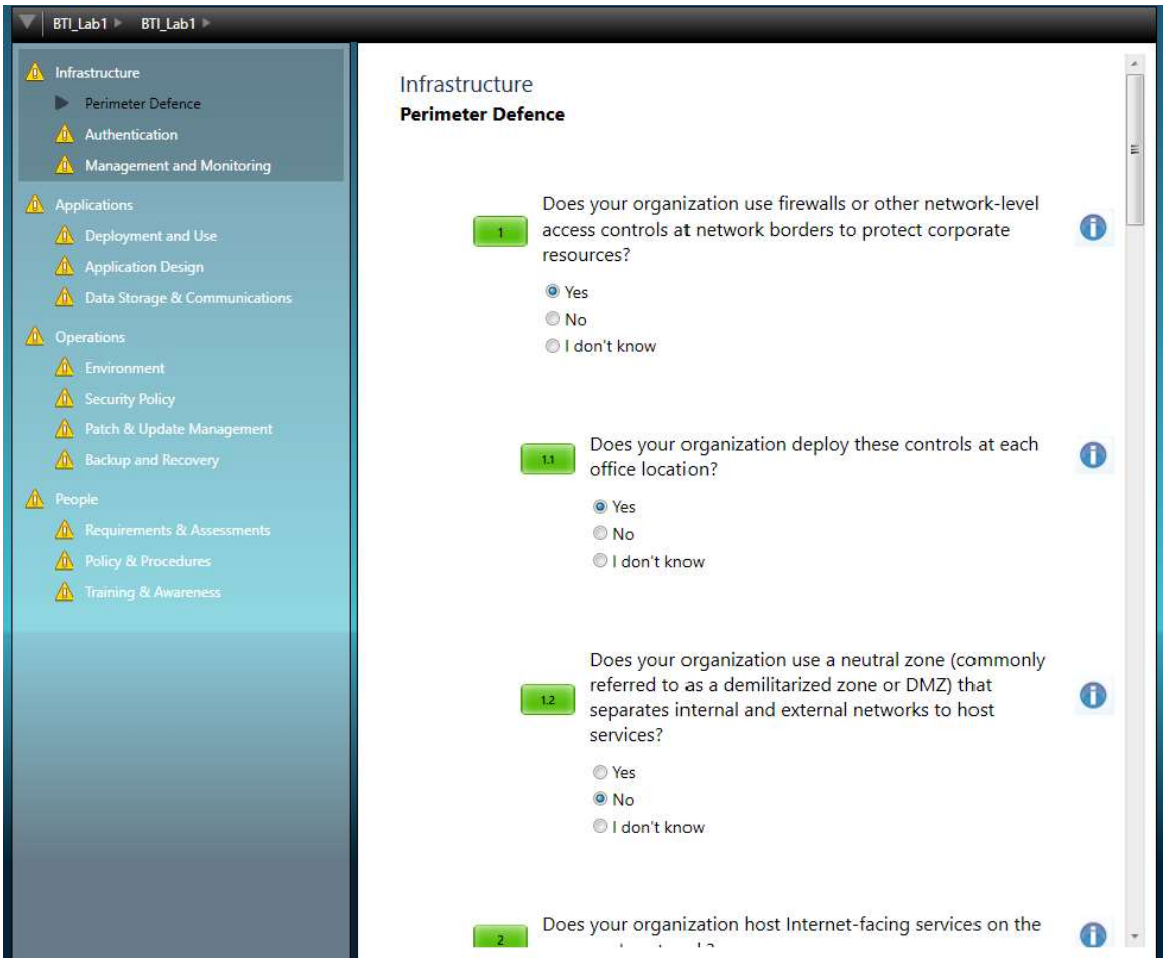

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
5
Do you consider your organization to be an early adopter of new technology?
Yes
No
6
Does your organization select and deploy new technologies based on existing partnerships and licensing agreements?
Yes
No
I don't know
7
Does your organization limit technology choices to technologies known by the current IT staff?
Yes
No
I don't know
8
Does your company expand its network through acquisition of new companies and their existing environments?
Yes
No
I don't know

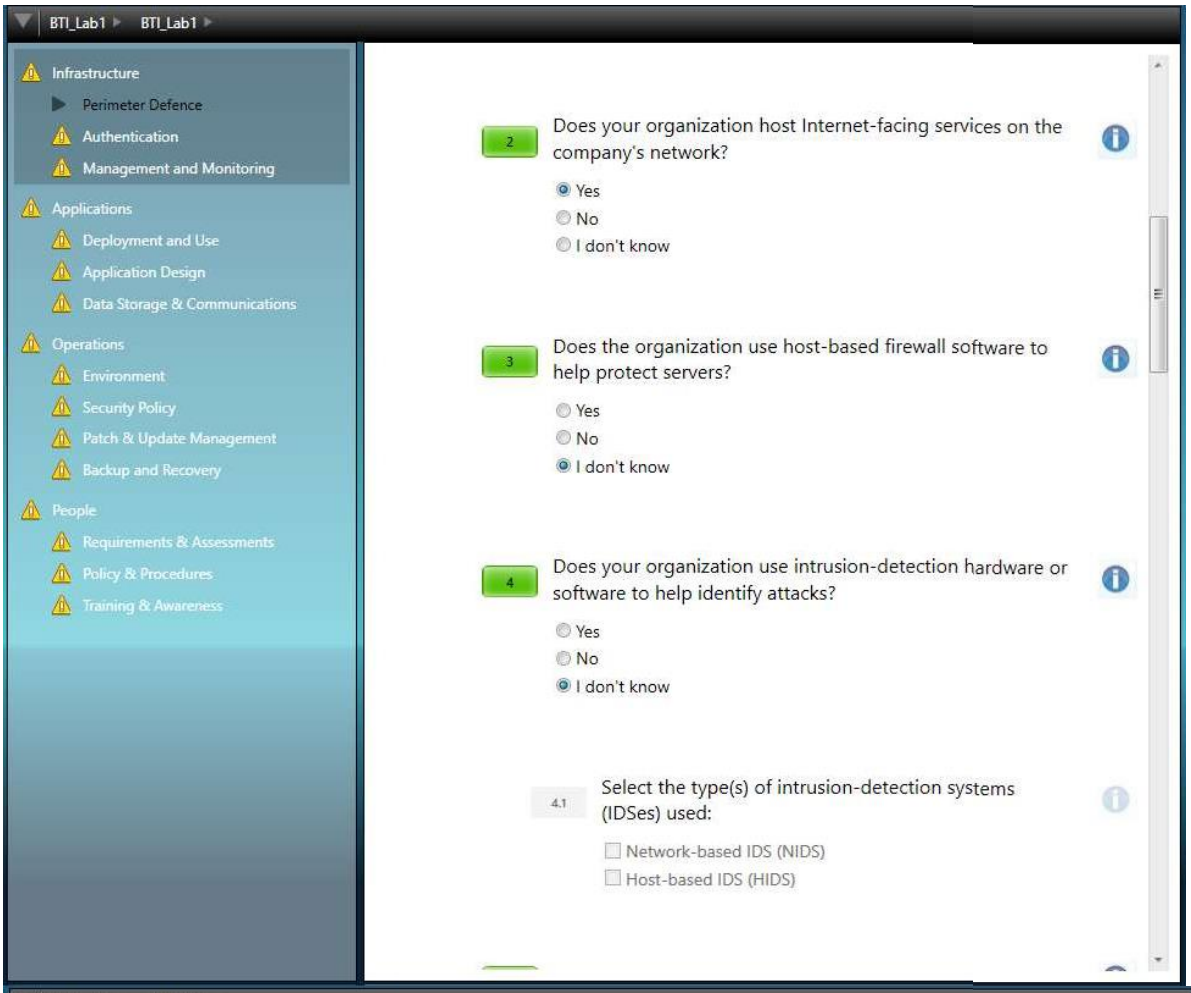

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
9
Does your organization allow employees to download sensitive customer or corporate data to their workstations?
Yes
No
I don't know
10
Does your organization restrict access to information by users based on their role?
Yes
No
I don't know
11
Does your organization deploy new services or applications before assessing them for possible security issues?
Yes
No
I don't know
12
Does your organization change credentials for privileged accounts on a regular basis?
Yes
No
I don't know

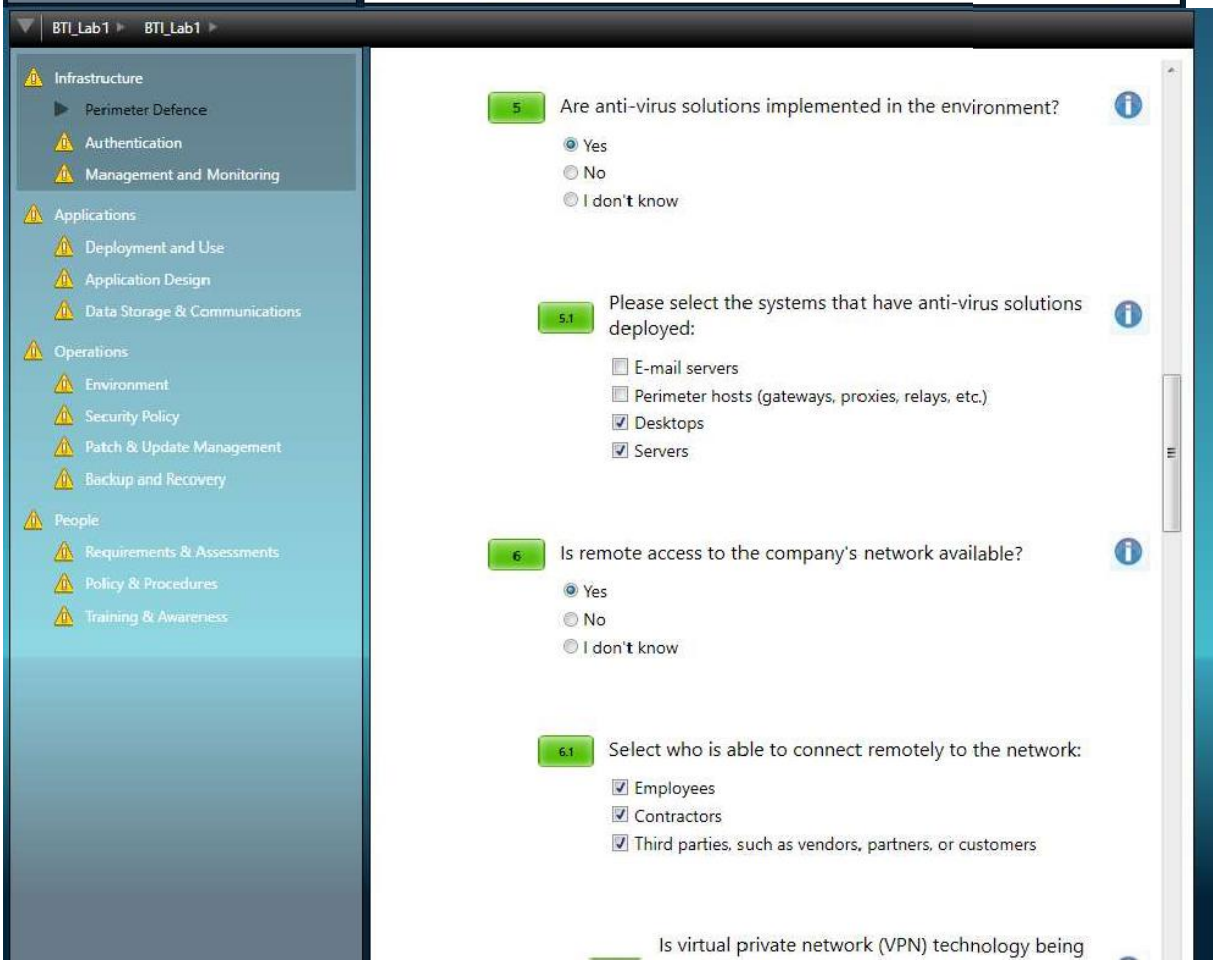

13
Does your organization change credentials for privileged accounts after termination of personnel with privileged access?
Yes
No
I don't know
< Back
Next >

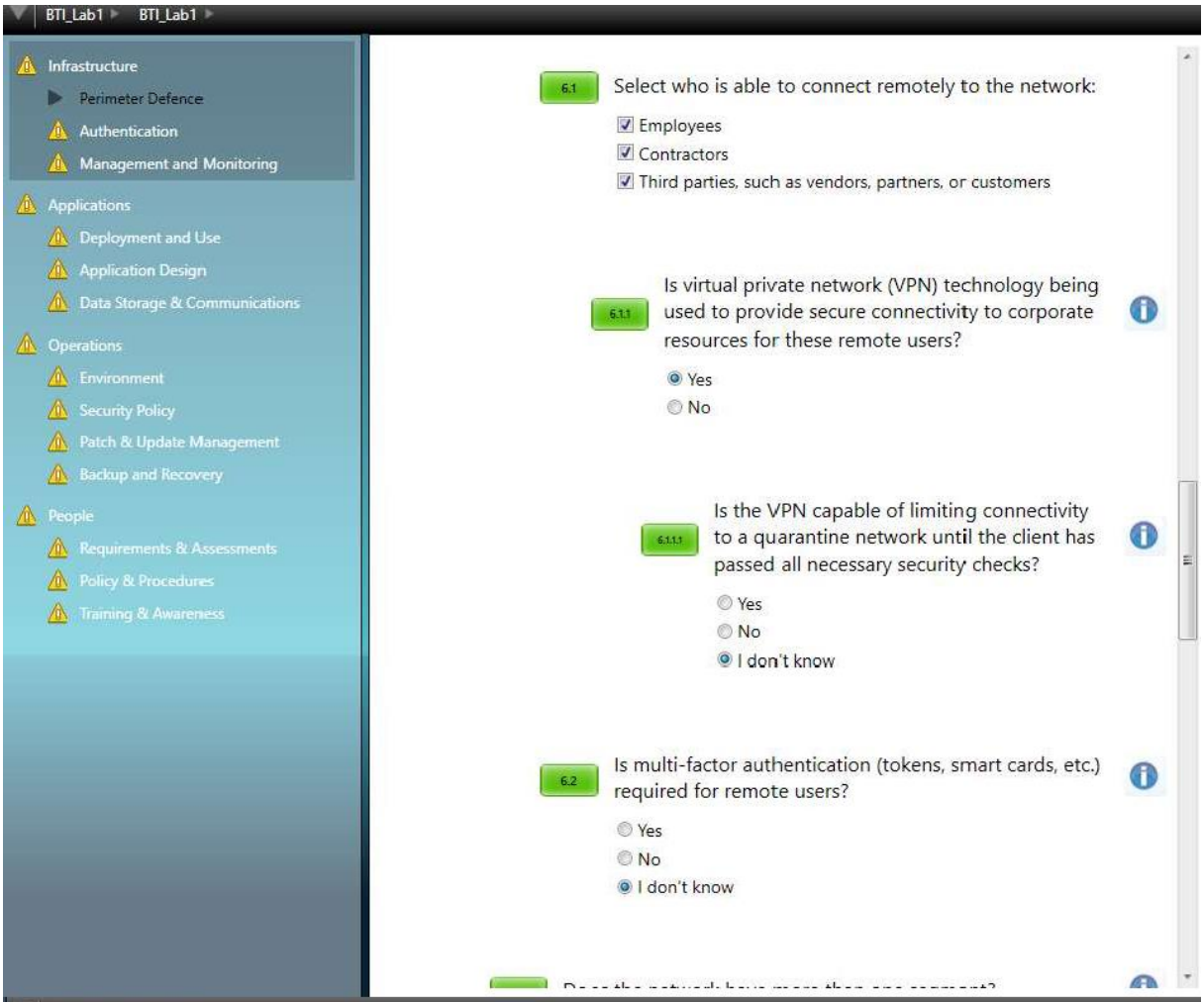

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Create New Assessment
Business Risk Profile
Environment
1
Choose the option that best describes your company's industry segment:
IT Services
Financial services
Manufacturing (discrete)
Legal services
Advertising/PR
Retail
Other
2
Choose the size of your organization:
Less than 10 employees
10 to 49 employees
50 to 149 employees
150 to 299 employees
300 to 399 employees
400 to 500 employees
More than 500 employees
3
Does your company have more than one location?
Yes
No

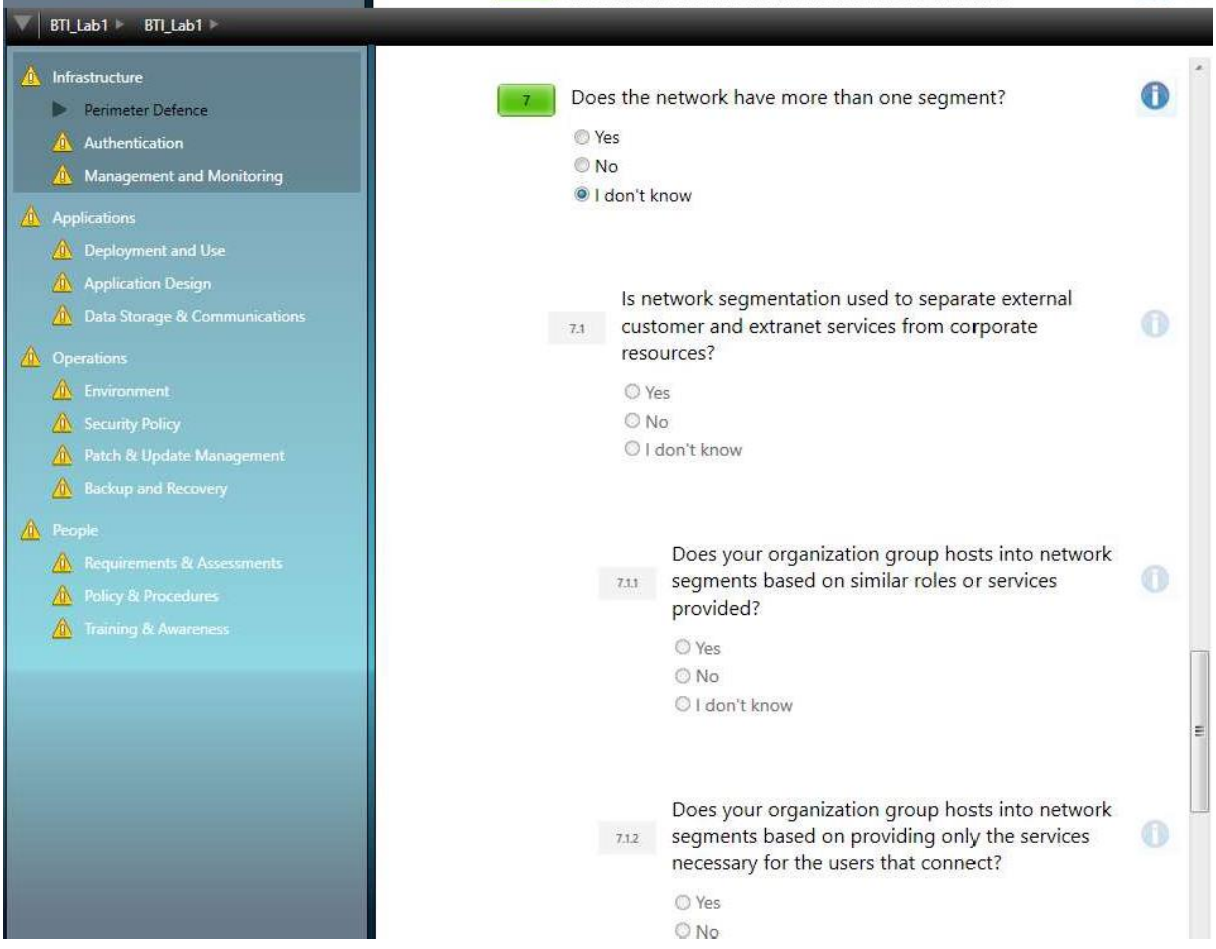

BTI_Lab1
Company Settings
Basic Information
Infrastructure Security
Application Security
Operations Security
People Security
Environment
Create New Assessment
4
Is your company in a highly competitive or research-focused industry in which intellectual property theft or espionage is a significant concern?
Yes
No
5
Are the technologists in your company subject to high turnover or attrition?
Yes
No
6
Does your company have significant product or brand recognition?
Yes
No
7
Does your company use down version or legacy software (software that is no longer supported by the vendor)?
Yes
No
8
Does your organization acquire software from a reputable vendor or source?
Yes
No

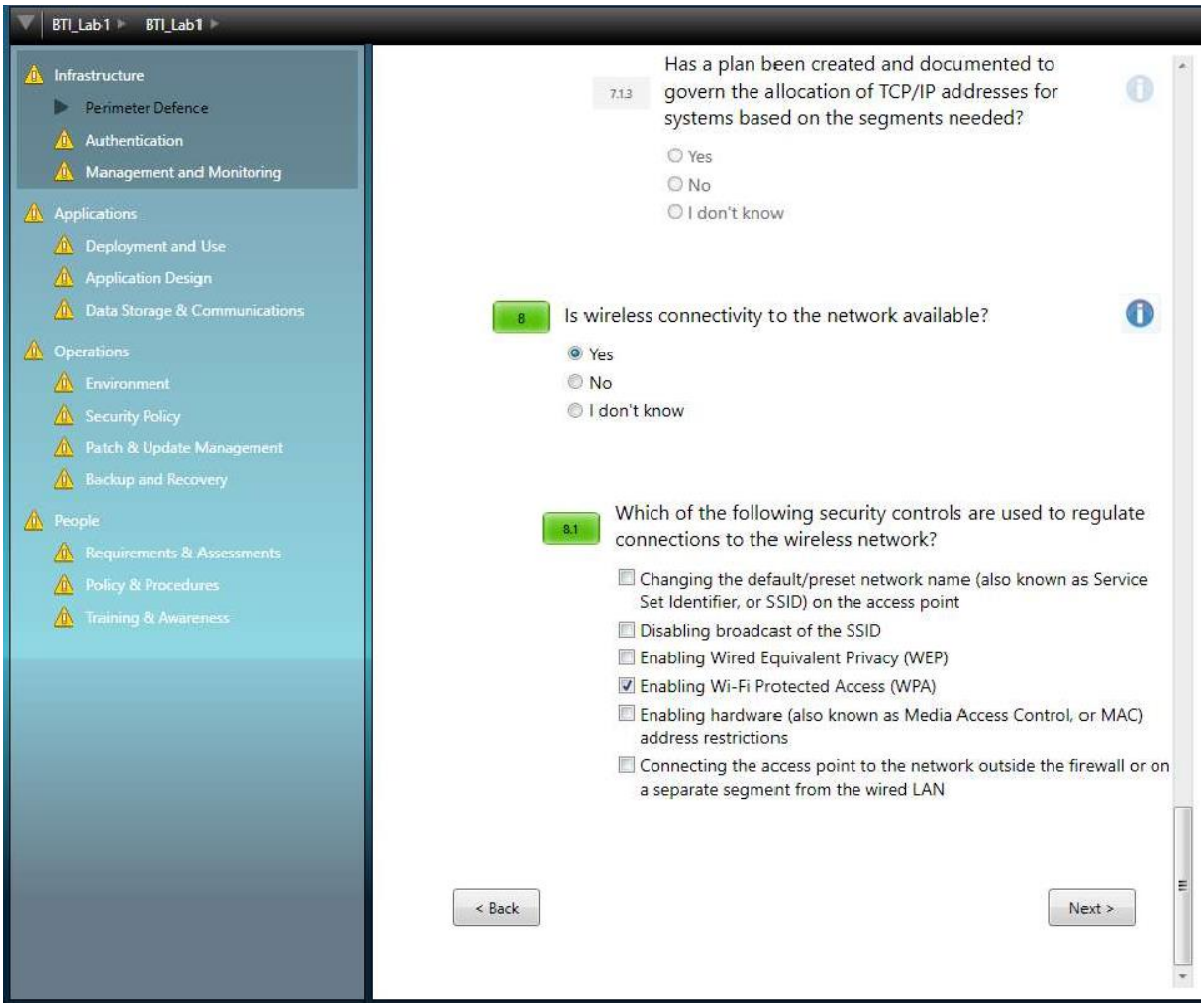

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Infrastructure
Perimeter Defence
1
Does your organization use firewalls or other network-level access controls at network borders to protect corporate resources?
Yes
No
I don't know
1.1
Does your organization deploy these controls at each office location?
Yes
No
I don't know
1.2
Does your organization use a neutral zone (commonly referred to as a demilitarized zone or DMZ) that separates internal and external networks to host services?
Yes
No
I don't know
2
Does your organization host Internet-facing services on the

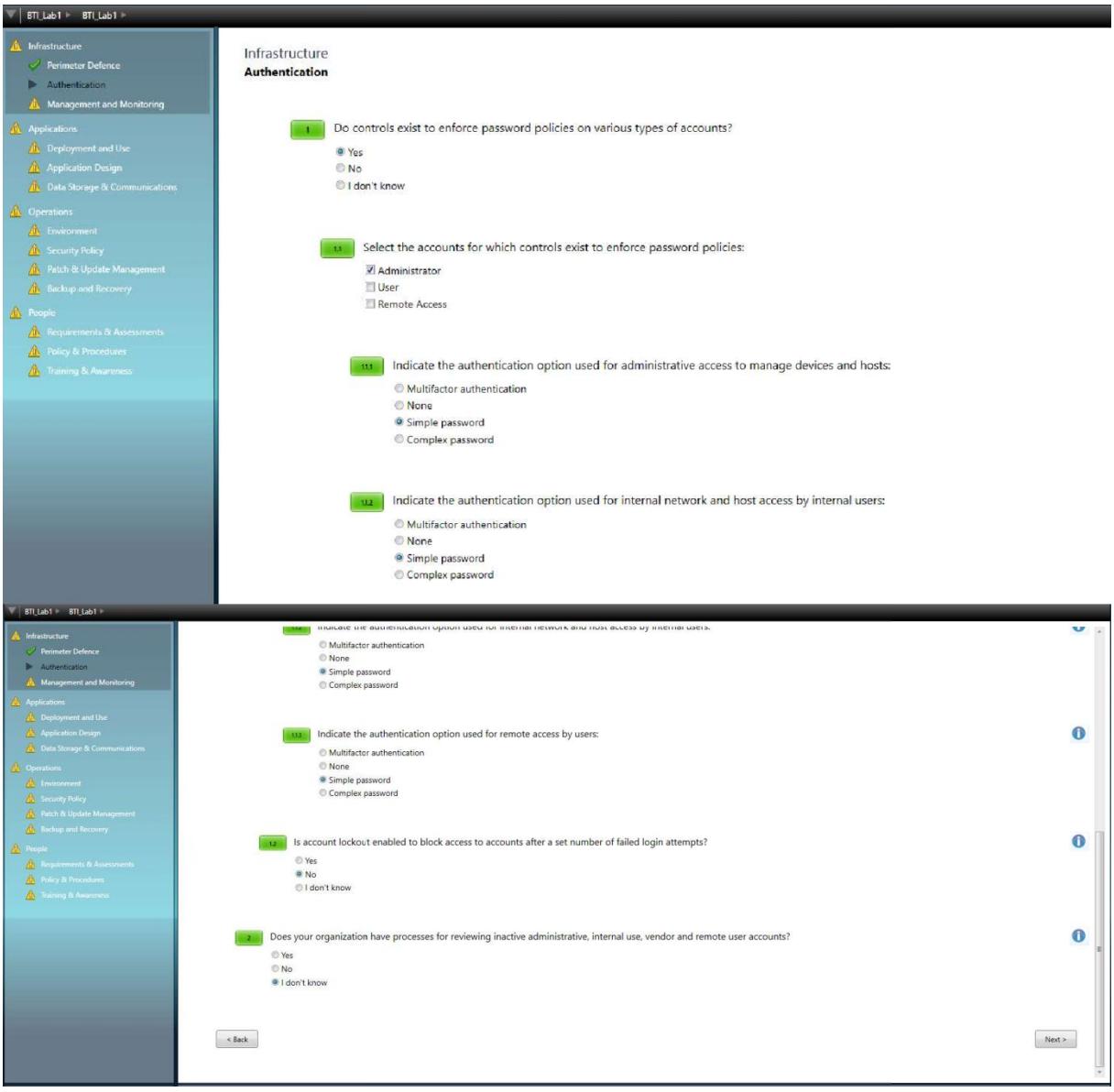

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
2
Does your organization host Internet-facing services on the company's network?
Yes
No
I don't know
3
Does the organization use host-based firewall software to help protect servers?
Yes
No
I don't know
4
Does your organization use intrusion-detection hardware or software to help identify attacks?
Yes
No
I don't know
4.1
Select the type(s) of intrusion-detection systems (IDSes) used:
Network-based IDS (NIDS)
Host-based IDS (HIDS)


BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
5
Are anti-virus solutions implemented in the environment?
Yes
No
I don't know
5.1
Please select the systems that have anti-virus solutions deployed:
E-mail servers
Perimeter hosts (gateways, proxies, relays, etc.)
Desktops
Servers
6
Is remote access to the company's network available?
Yes
No
I don't know
6.1
Select who is able to connect remotely to the network:
Employees
Contractors
Third parties, such as vendors, partners, or customers
Is virtual private network (VPN) technology being

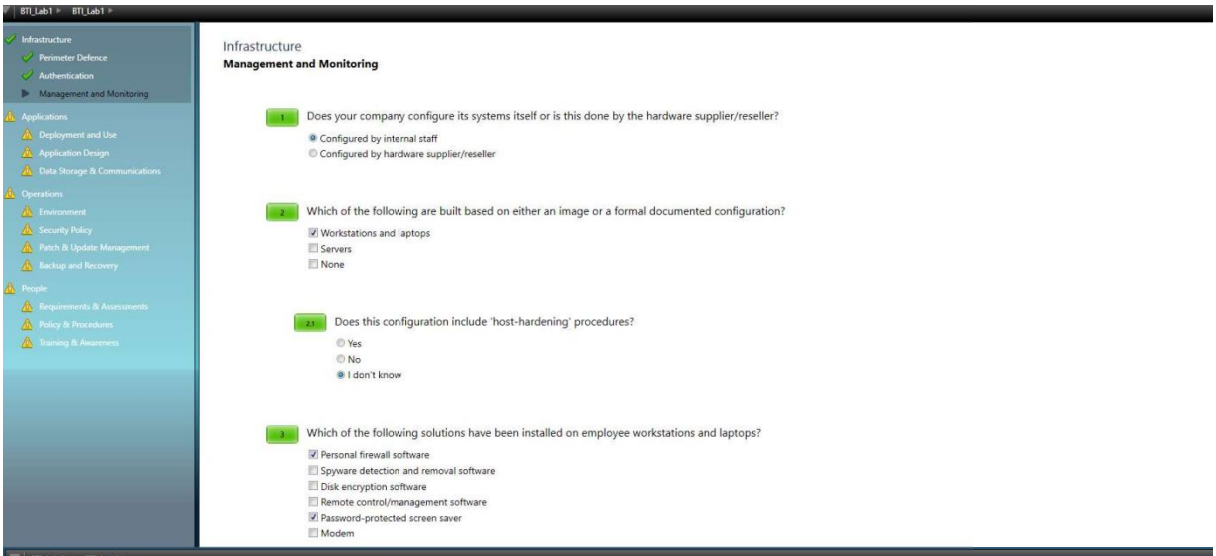

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
6.1
Select who is able to connect remotely to the network:
Employees
Contractors
Third parties, such as vendors, partners, or customers
6.1.1
Is virtual private network (VPN) technology being used to provide secure connectivity to corporate resources for these remote users?
Yes
No
6.1.1.1
Is the VPN capable of limiting connectivity to a quarantine network until the client has passed all necessary security checks?
Yes
No
I don't know
6.2
Is multi-factor authentication (tokens, smart cards, etc.) required for remote users?
Yes
No
I don't know

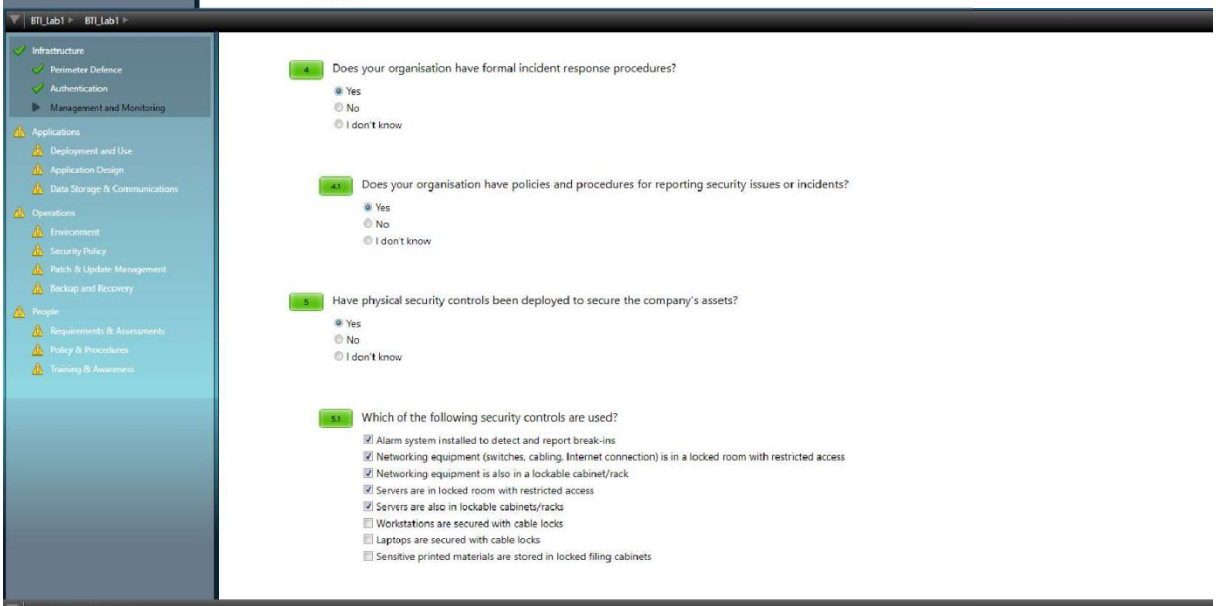

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
7
Does the network have more than one segment?
Yes
No
I don't know
7.1
Is network segmentation used to separate external customer and extranet services from corporate resources?
Yes
No
I don't know
7.1.1
Does your organization group hosts into network segments based on similar roles or services provided?
Yes
No
I don't know
7.1.2
Does your organization group hosts into network segments based on providing only the services necessary for the users that connect?
Yes
No

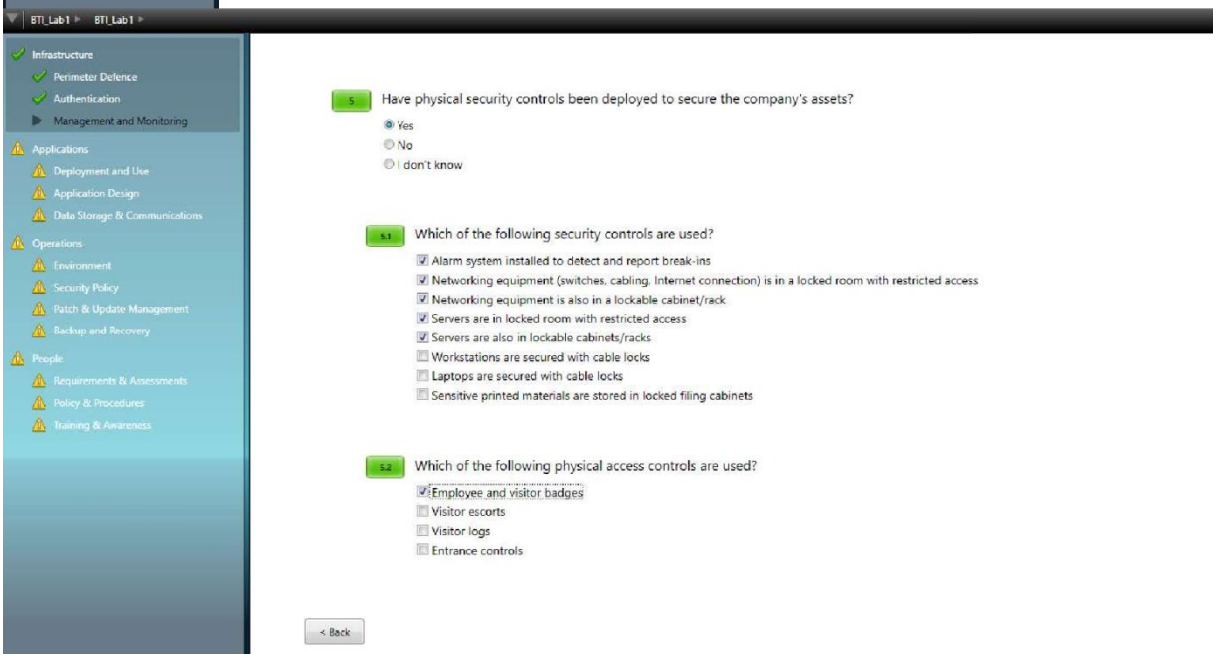

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
7.1.3
Has a plan been created and documented to govern the allocation of TCP/IP addresses for systems based on the segments needed?
Yes
No
I don't know
8
Is wireless connectivity to the network available?
Yes
No
I don't know
8.1
Which of the following security controls are used to regulate connections to the wireless network?
Changing the default/preset network name (also known as Service Set Identifier, or SSID) on the access point
Disabling broadcast of the SSID
Enabling Wired Equivalent Privacy (WEP)
Enabling Wi-Fi Protected Access (WPA)
Enabling hardware (also known as Media Access Control, or MAC) address restrictions
Connecting the access point to the network outside the firewall or on a separate segment from the wired LAN
< Back
Next >

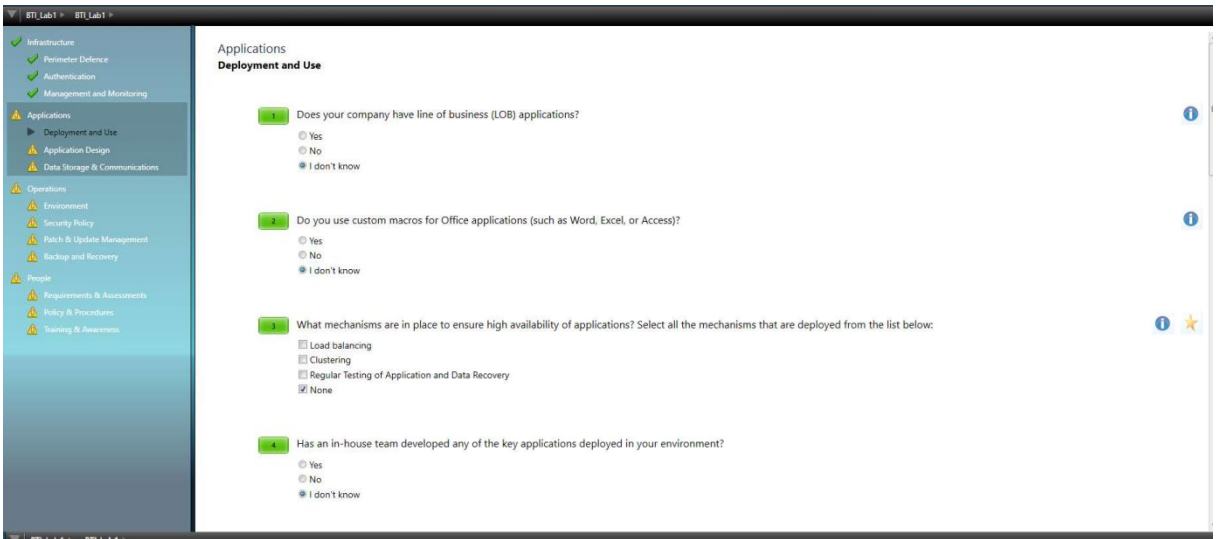

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Infrastructure
Authentication
1 Do controls exist to enforce password policies on various types of accounts?
Yes
No
I don't know
1.1 Select the accounts for which controls exist to enforce password policies:
Administrator
User
Remote Access
1.1.1 Indicate the authentication option used for administrative access to manage devices and hosts:
Multifactor authentication
None
Simple password
Complex password
1.1.2 Indicate the authentication option used for internal network and host access by internal users:
Multifactor authentication
None
Simple password
Complex password

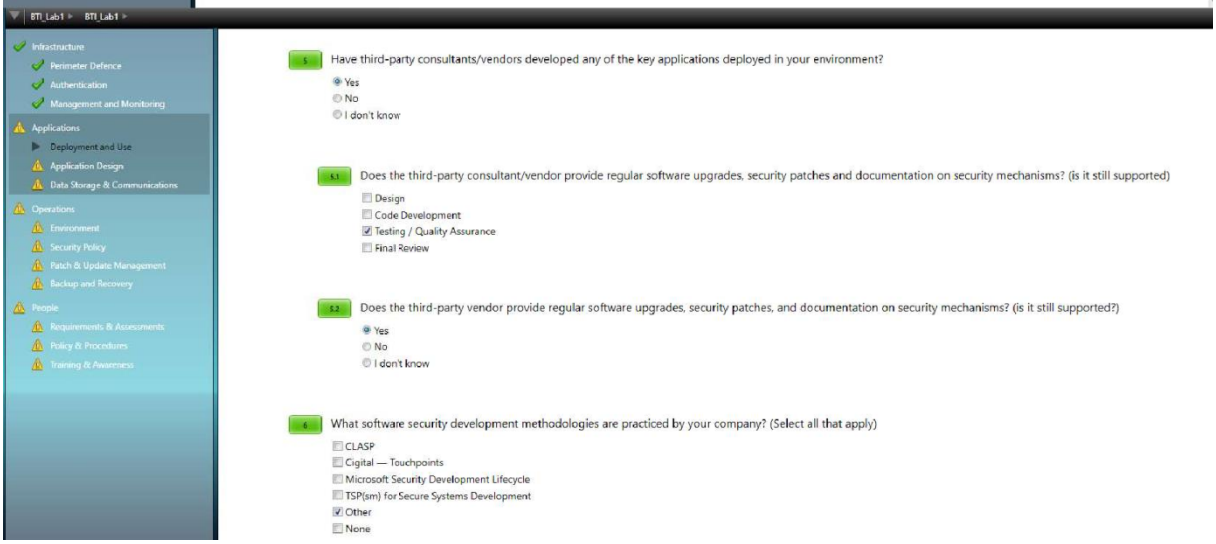
BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Multifactor authentication
None
Simple password
Complex password
1.1.2 Indicate the authentication option used for remote access by users:
Multifactor authentication
None
Simple password
Complex password
1.2 Is account lockout enabled to block access to accounts after a set number of failed login attempts?
Yes
No
I don't know
2 Does your organization have processes for reviewing inactive administrative, internal use, vendor and remote user accounts?
Yes
No
I don't know
< Back
Next >

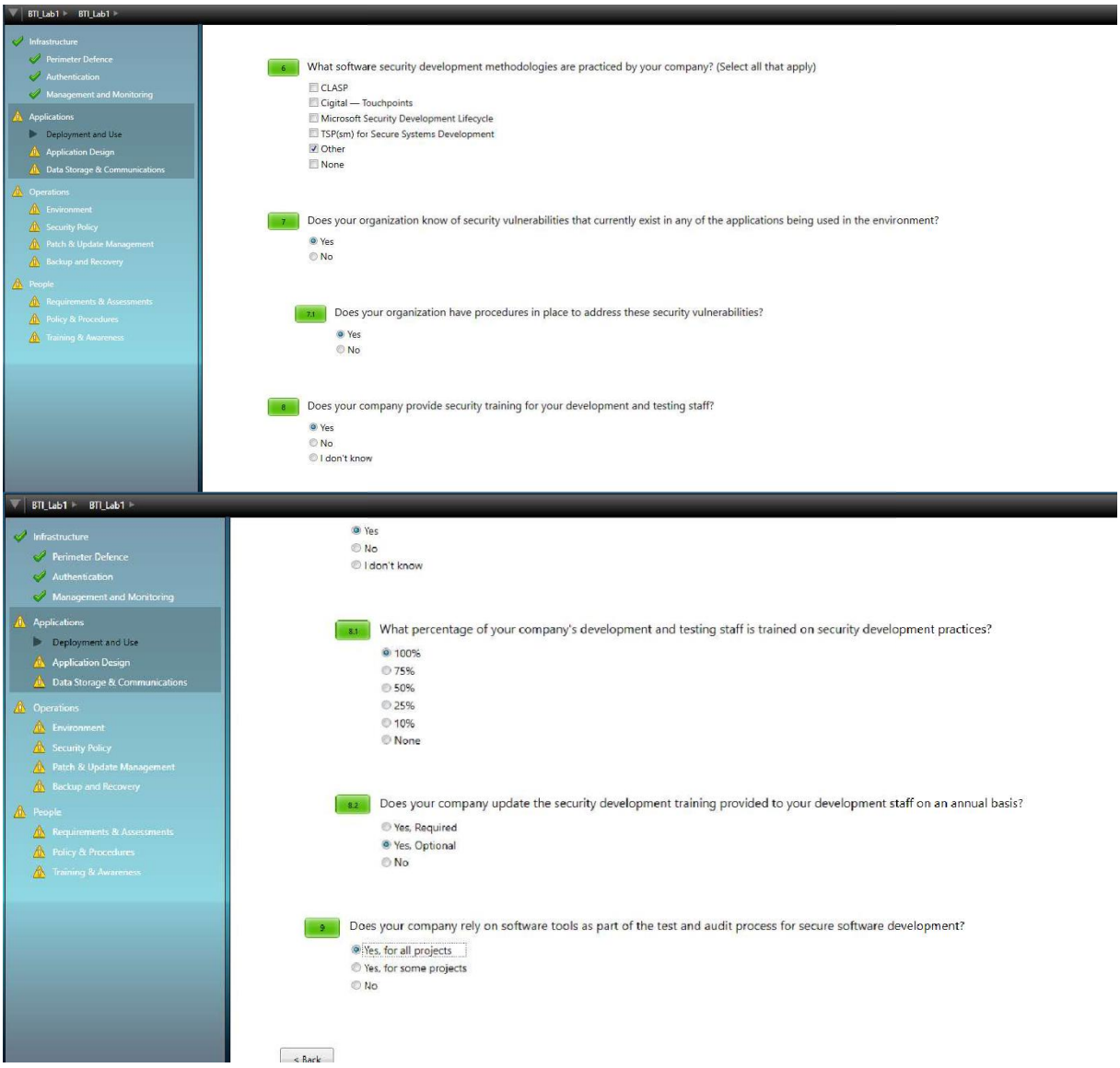

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Infrastructure
Management and Monitoring
1 Does your company configure its systems itself or is this done by the hardware supplier/reseller?
Configured by internal staff
Configured by hardware supplier/reseller
2 Which of the following are built based on either an image or a formal documented configuration?
Workstations and laptops
Servers
None
2.1 Does this configuration include 'host-hardening' procedures?
Yes
No
I don't know
3 Which of the following solutions have been installed on employee workstations and laptops?
Personal firewall software
Spyware detection and removal software
Disk encryption software
Remote control/management software
Password-protected screen saver
Modem


BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
4 Does your organisation have formal incident response procedures?
Yes
No
I don't know
4.1 Does your organisation have policies and procedures for reporting security issues or incidents?
Yes
No
I don't know
5 Have physical security controls been deployed to secure the company's assets?
Yes
No
I don't know
5.1 Which of the following security controls are used?
Alarm system installed to detect and report break-ins
Networking equipment (switches, cabling, Internet connection) is in a locked room with restricted access
Networking equipment is also in a lockable cabinet/rack
Servers are in locked room with restricted access
Servers are also in lockable cabinets/racks
Workstations are secured with cable locks
Laptops are secured with cable locks
Sensitive printed materials are stored in locked filing cabinets

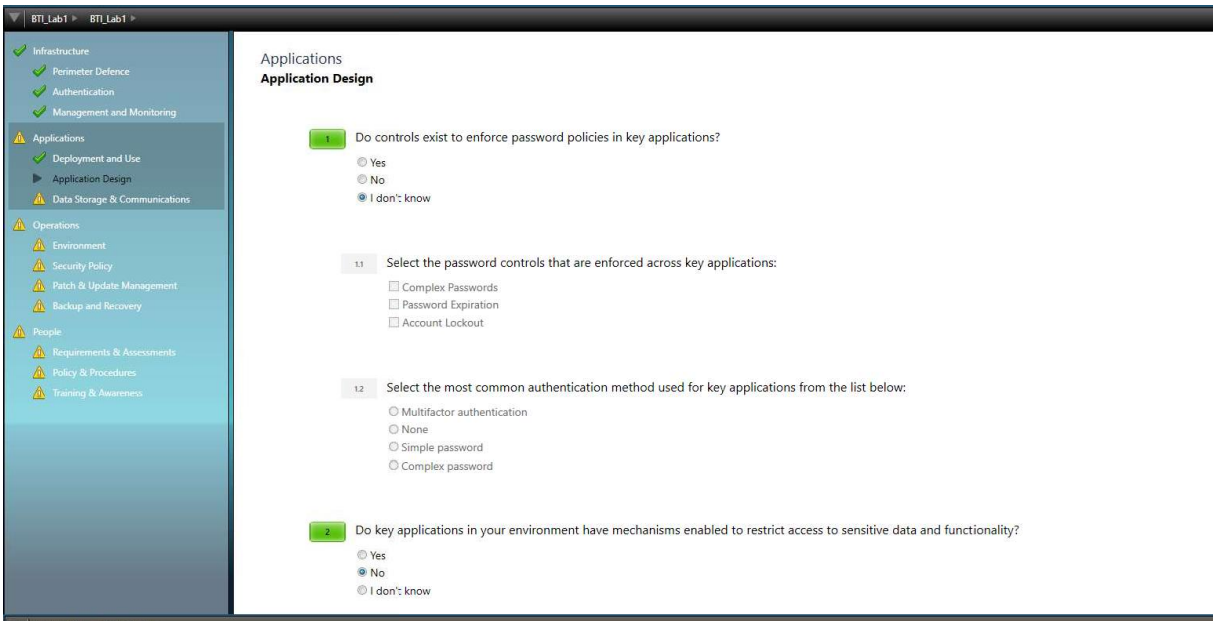

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
5 Have physical security controls been deployed to secure the company's assets?
Yes
No
I don't know
5.1 Which of the following security controls are used?
Alarm system installed to detect and report break-ins
Networking equipment (switches, cabling, Internet connection) is in a locked room with restricted access
Networking equipment is also in a lockable cabinet/rack
Servers are in locked room with restricted access
Servers are also in lockable cabinets/racks
Workstations are secured with cable locks
Laptops are secured with cable locks
Sensitive printed materials are stored in locked filing cabinets
5.2 Which of the following physical access controls are used?
Employee and visitor badges
Visitor escorts
Visitor logs
Entrance controls
< Back

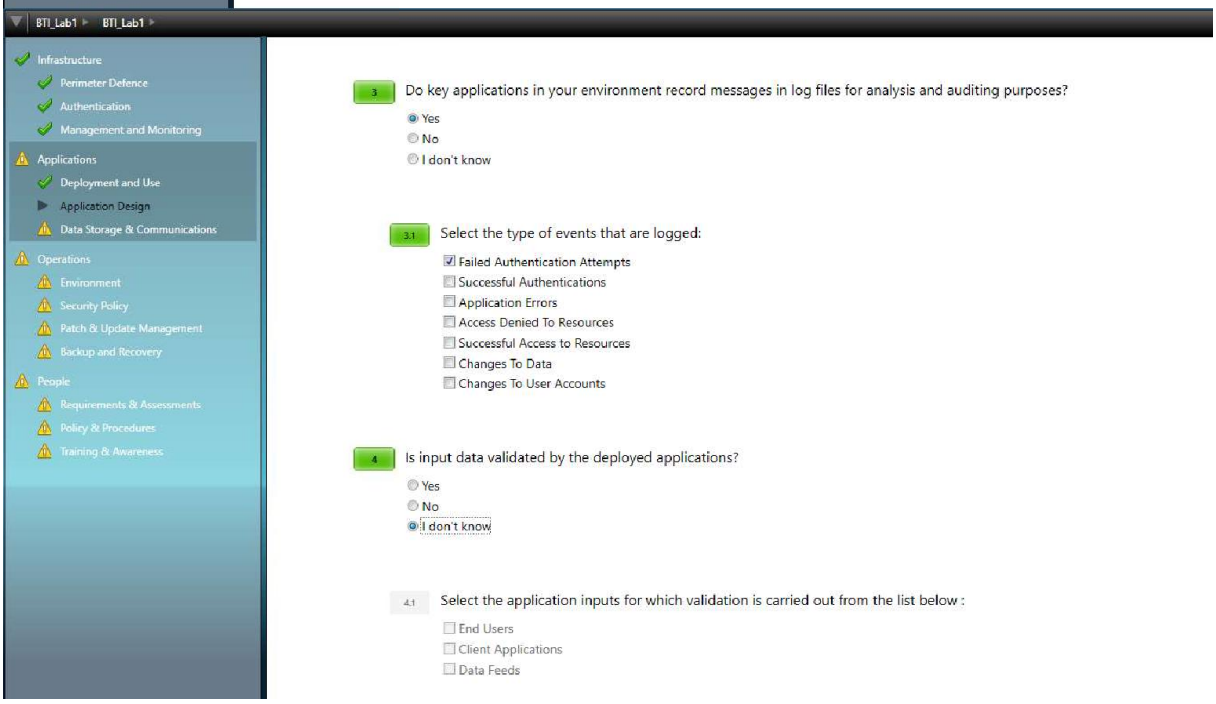

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Applications
Deployment and Use
1 Does your company have line of business (LOB) applications?
Yes
No
I don't know
2 Do you use custom macros for Office applications (such as Word, Excel, or Access)?
Yes
No
I don't know
3 What mechanisms are in place to ensure high availability of applications? Select all the mechanisms that are deployed from the list below:
Load balancing
Clustering
Regular Testing of Application and Data Recovery
None
4 Has an in-house team developed any of the key applications deployed in your environment?
Yes
No
I don't know

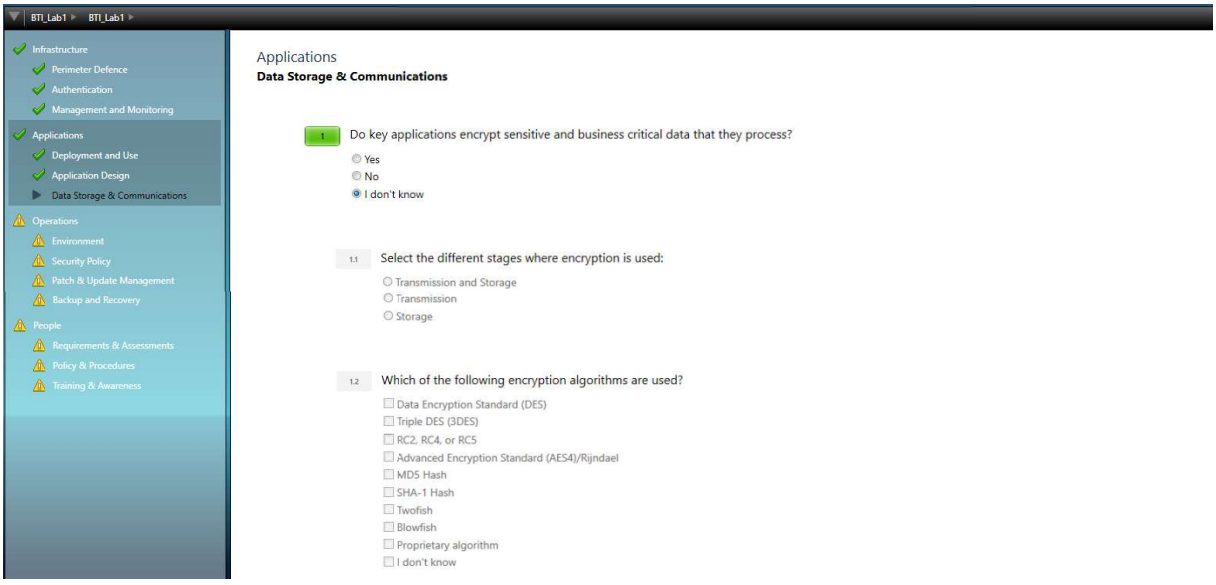

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
5 Have third-party consultants/vendors developed any of the key applications deployed in your environment?
Yes
No
I don't know
5.1 Does the third-party consultant/vendor provide regular software upgrades, security patches and documentation on security mechanisms? (is it still supported)
Design
Code Development
Testing / Quality Assurance
Final Review
5.2 Does the third-party vendor provide regular software upgrades, security patches, and documentation on security mechanisms? (is it still supported?)
Yes
No
I don't know
6 What software security development methodologies are practiced by your company? (Select all that apply)
CLASP
Cigital — Touchpoints
Microsoft Security Development Lifecycle
TSP(sm) for Secure Systems Development
Other
None

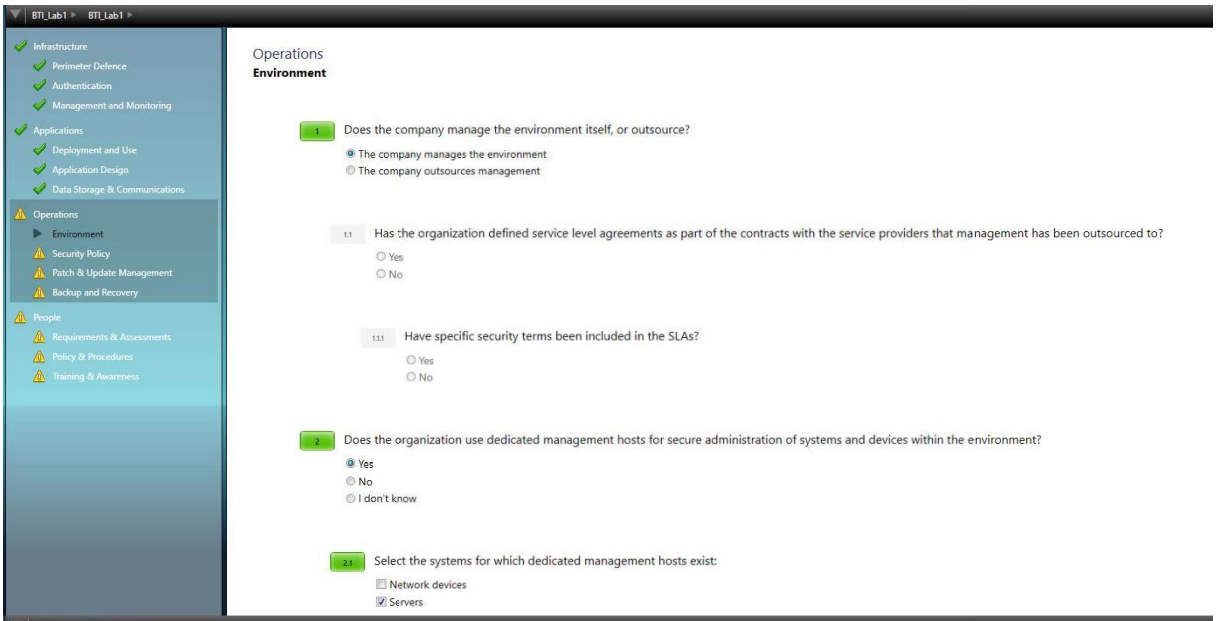

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
6 What software security development methodologies are practiced by your company? (Select all that apply)
CLASP
Cigital — Touchpoints
Microsoft Security Development Lifecycle
TSP(sm) for Secure Systems Development
Other
None
7 Does your organization know of security vulnerabilities that currently exist in any of the applications being used in the environment?
Yes
No
7.1 Does your organization have procedures in place to address these security vulnerabilities?
Yes
No
8 Does your company provide security training for your development and testing staff?
Yes
No
I don't know

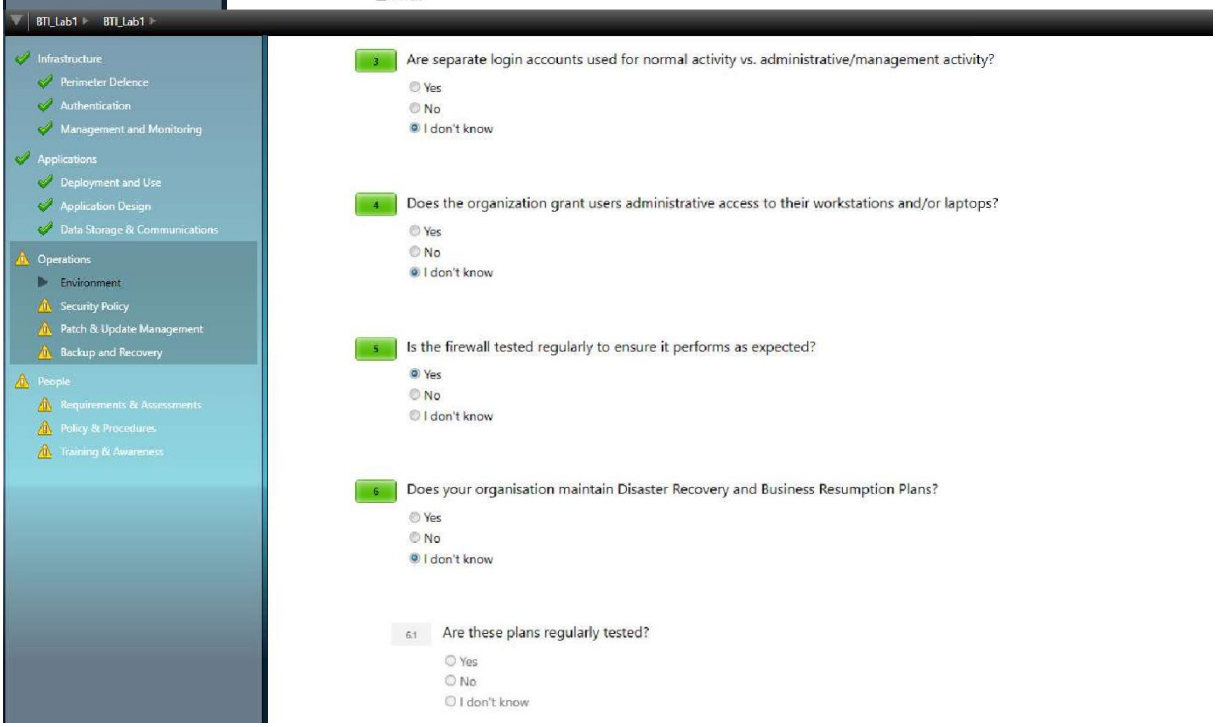
BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Yes
No
I don't know
8.1 What percentage of your company's development and testing staff is trained on security development practices?
100%
75%
50%
25%
10%
None
8.2 Does your company update the security development training provided to your development staff on an annual basis?
Yes, Required
Yes, Optional
No
9 Does your company rely on software tools as part of the test and audit process for secure software development?
Yes, for all projects
Yes, for some projects
No
< Back

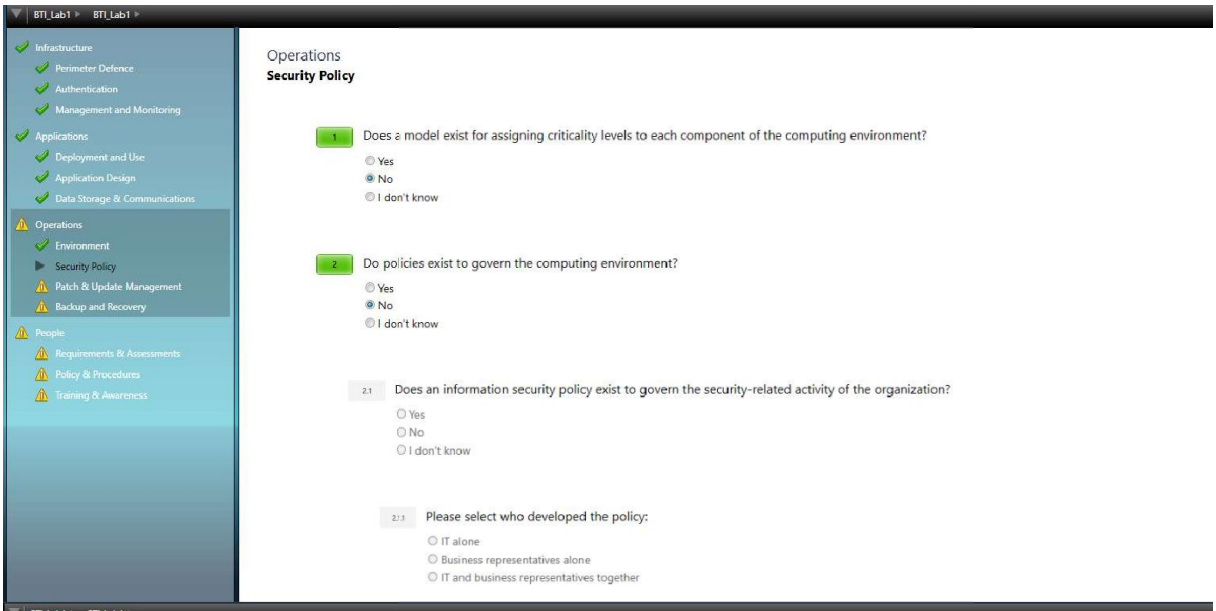

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Applications
Application Design
1 Do controls exist to enforce password policies in key applications?
Yes
No
I don't know
1.1 Select the password controls that are enforced across key applications:
Complex Passwords
Password Expiration
Account Lockout
1.2 Select the most common authentication method used for key applications from the list below:
Multifactor authentication
None
Simple password
Complex password
2 Do key applications in your environment have mechanisms enabled to restrict access to sensitive data and functionality?
Yes
No
I don't know

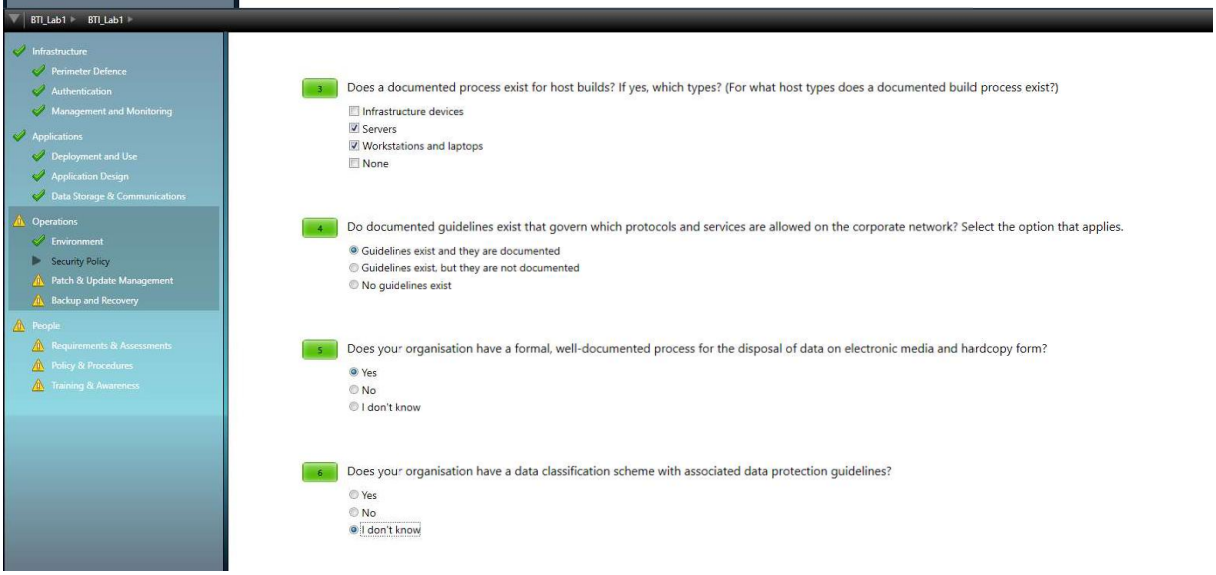

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
3 Do key applications in your environment record messages in log files for analysis and auditing purposes?
Yes
No
I don't know
3.1 Select the type of events that are logged:
Failed Authentication Attempts
Successful Authentications
Application Errors
Access Denied To Resources
Successful Access to Resources
Changes To Data
Changes To User Accounts
4 Is input data validated by the deployed applications?
Yes
No
I don't know
4.1 Select the application inputs for which validation is carried out from the list below :
End Users
Client Applications
Data Feeds

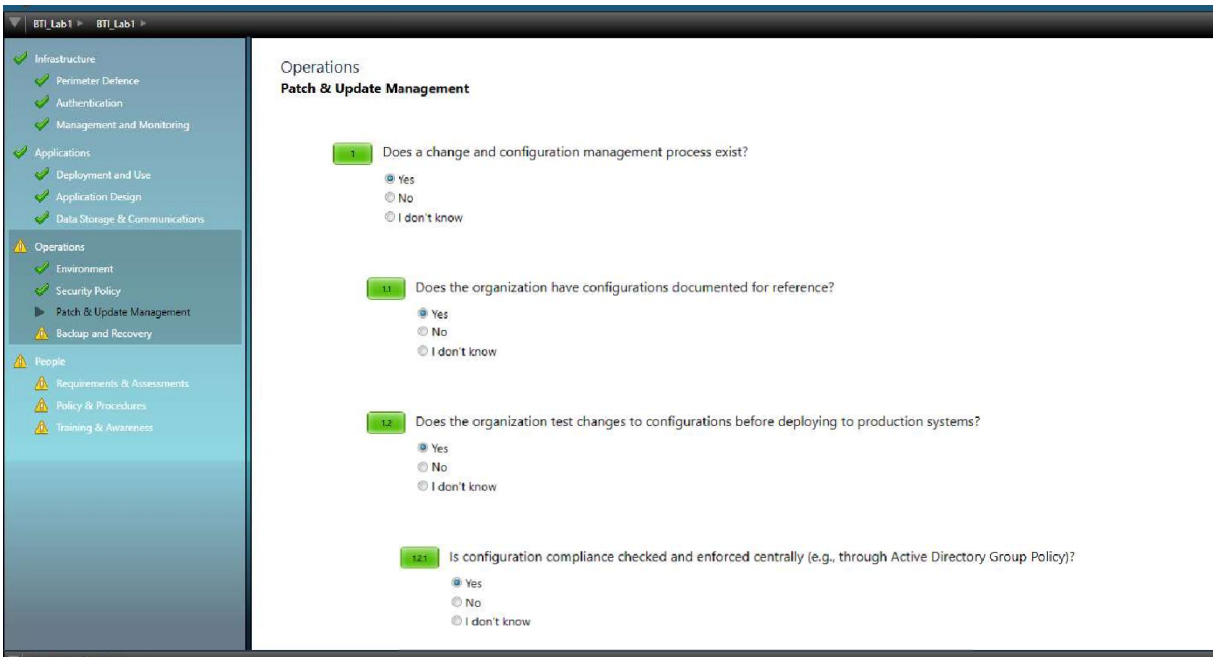

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Applications
Data Storage & Communications
1 Do key applications encrypt sensitive and business critical data that they process?
Yes
No
I don't know
1.1 Select the different stages where encryption is used:
Transmission and Storage
Transmission
Storage
1.2 Which of the following encryption algorithms are used?
Data Encryption Standard (DES)
Triple DES (3DES)
RC2, RC4, or RC5
Advanced Encryption Standard (AES4)/Rijndael
MD5 Hash
SHA-1 Hash
Twofish
Blowfish
Proprietary algorithm
I don't know

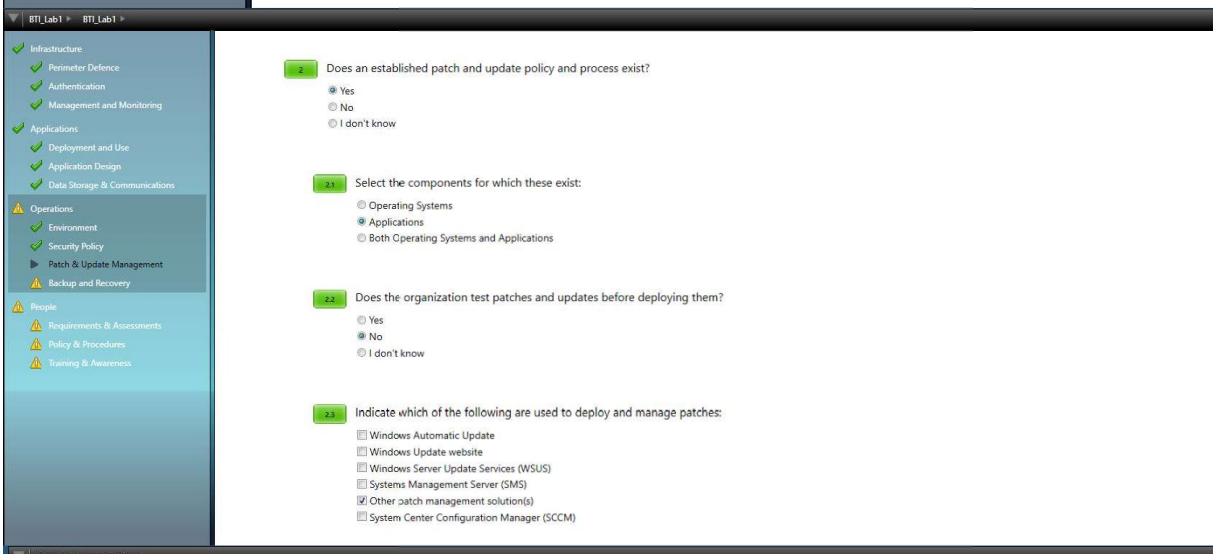

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Operations
Environment
1 Does the company manage the environment itself, or outsource?
The company manages the environment
The company outsources management
1.1 Has the organization defined service level agreements as part of the contracts with the service providers that management has been outsourced to?
Yes
No
1.1.1 Have specific security terms been included in the SLAs?
Yes
No
2 Does the organization use dedicated management hosts for secure administration of systems and devices within the environment?
Yes
No
I don't know
2.1 Select the systems for which dedicated management hosts exist:
Network devices
Servers

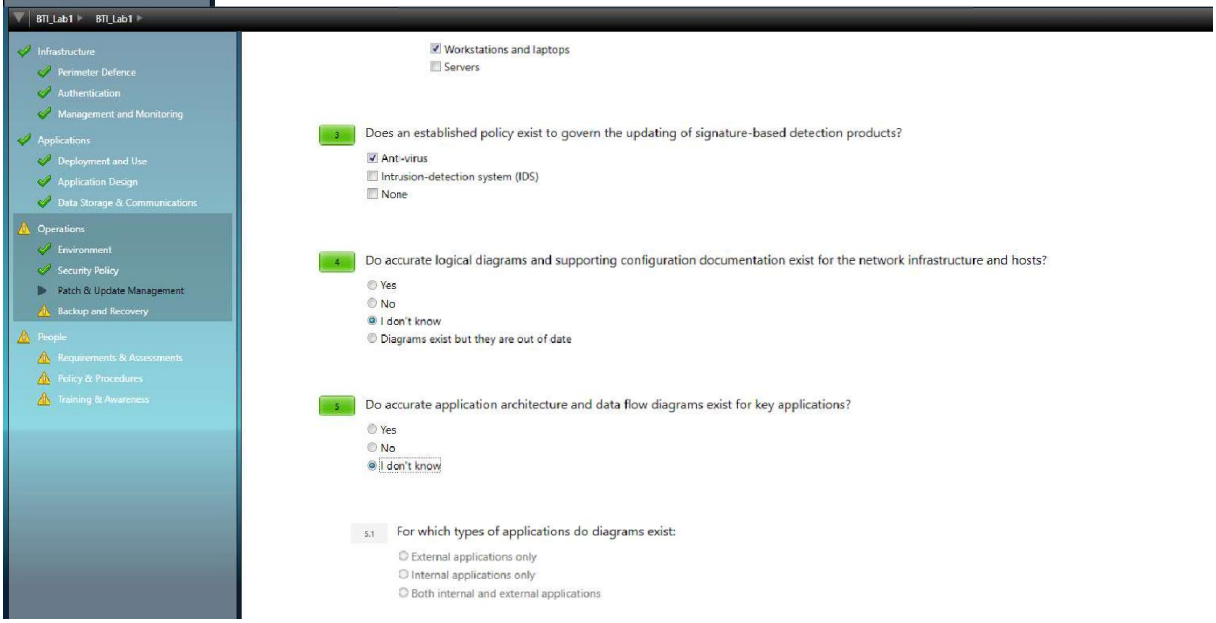

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
3 Are separate login accounts used for normal activity vs. administrative/management activity?
Yes
No
I don't know
4 Does the organization grant users administrative access to their workstations and/or laptops?
Yes
No
I don't know
5 Is the firewall tested regularly to ensure it performs as expected?
Yes
No
I don't know
6 Does your organisation maintain Disaster Recovery and Business Resumption Plans?
Yes
No
I don't know
6.1 Are these plans regularly tested?
Yes
No
I don't know

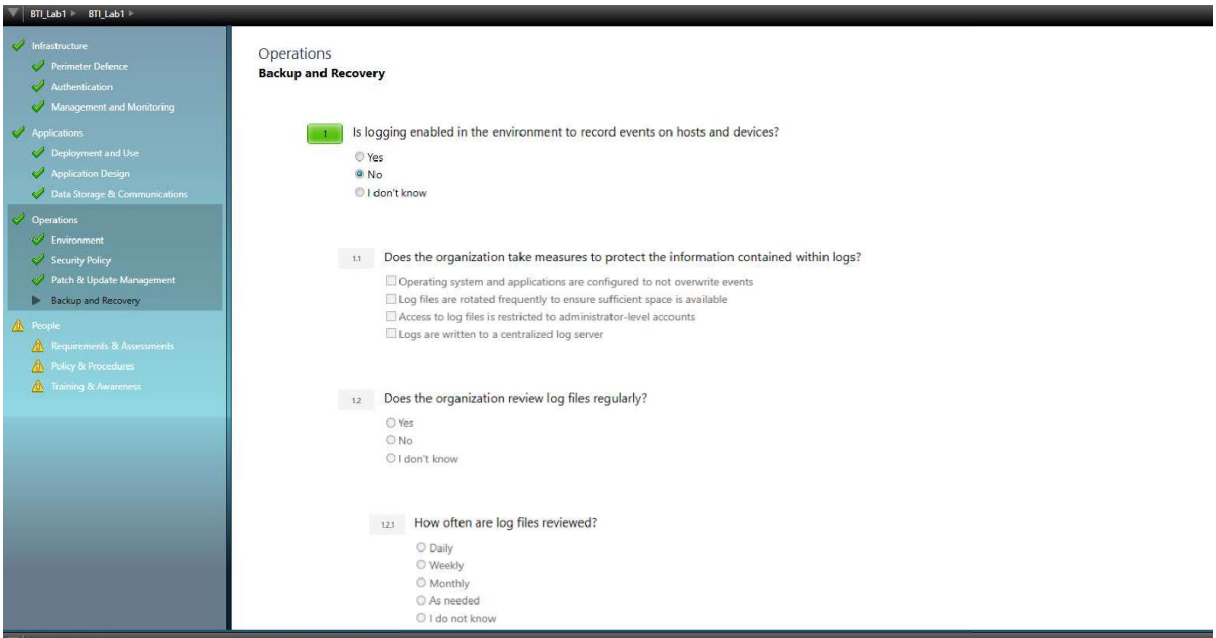

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Operations
Security Policy
1
Does a model exist for assigning criticality levels to each component of the computing environment?
Yes
No
I don't know
2
Do policies exist to govern the computing environment?
Yes
No
I don't know
2.1
Does an information security policy exist to govern the security-related activity of the organization?
Yes
No
I don't know
2.1.1
Please select who developed the policy:
IT alone
Business representatives alone
IT and business representatives together

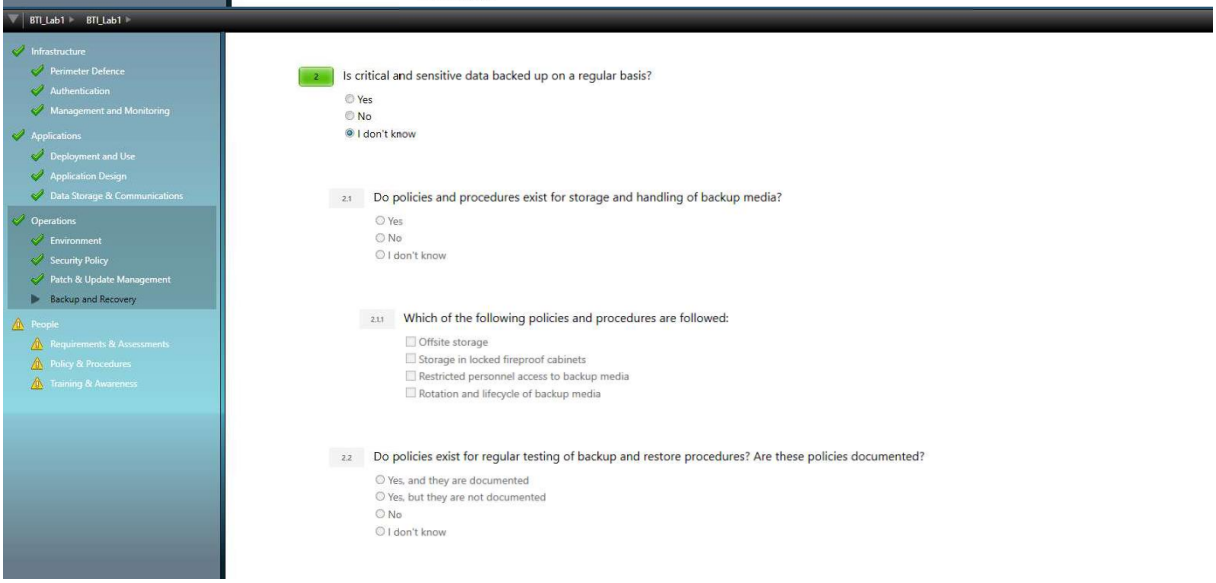

BTI_Lab1
BTI_Lab1
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
3
Does a documented process exist for host builds? If yes, which types? (For what host types does a documented build process exist?)
Infrastructure devices
Servers
Workstations and laptops
None
4
Do documented guidelines exist that govern which protocols and services are allowed on the corporate network? Select the option that applies.
Guidelines exist and they are documented
Guidelines exist, but they are not documented
No guidelines exist
5
Does your organisation have a formal, well-documented process for the disposal of data on electronic media and hardcopy form?
Yes
No
I don't know
6
Does your organisation have a data classification scheme with associated data protection guidelines?
Yes
No
I don't know

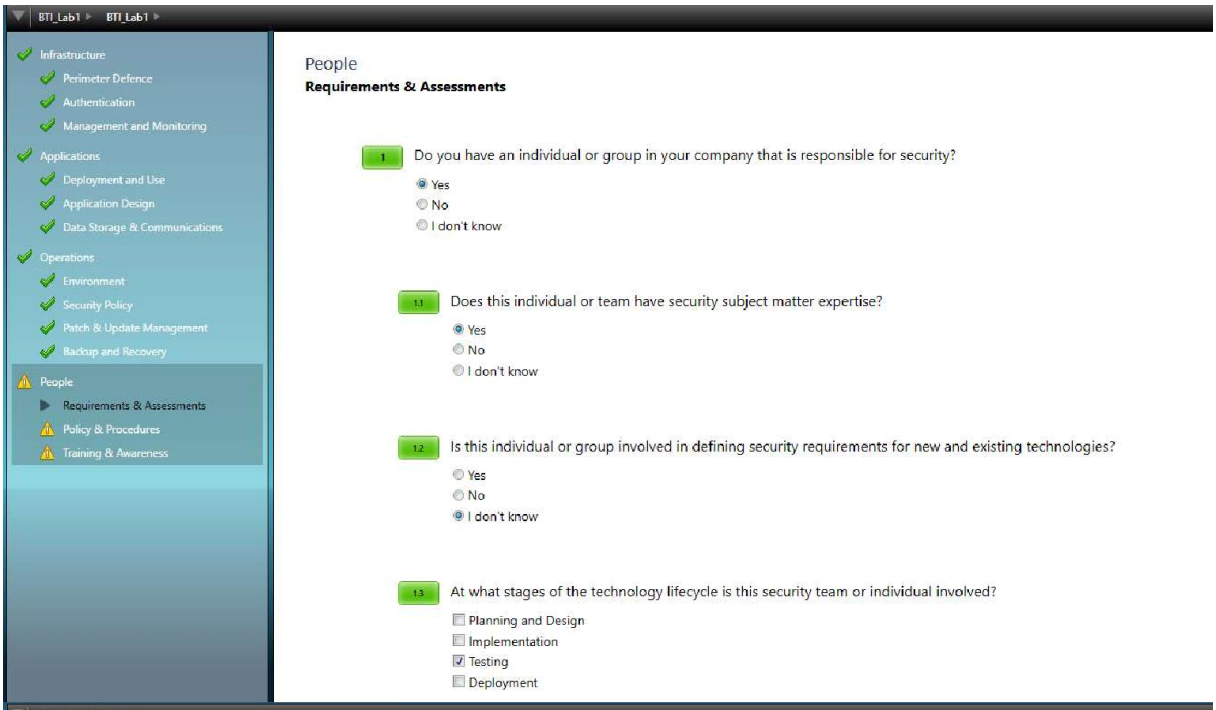

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Operations
Patch & Update Management
1 Does a change and configuration management process exist?
Yes
No
I don't know
1.1 Does the organization have configurations documented for reference?
Yes
No
I don't know
1.2 Does the organization test changes to configurations before deploying to production systems?
Yes
No
I don't know
1.2.1 Is configuration compliance checked and enforced centrally (e.g., through Active Directory Group Policy)?
Yes
No
I don't know

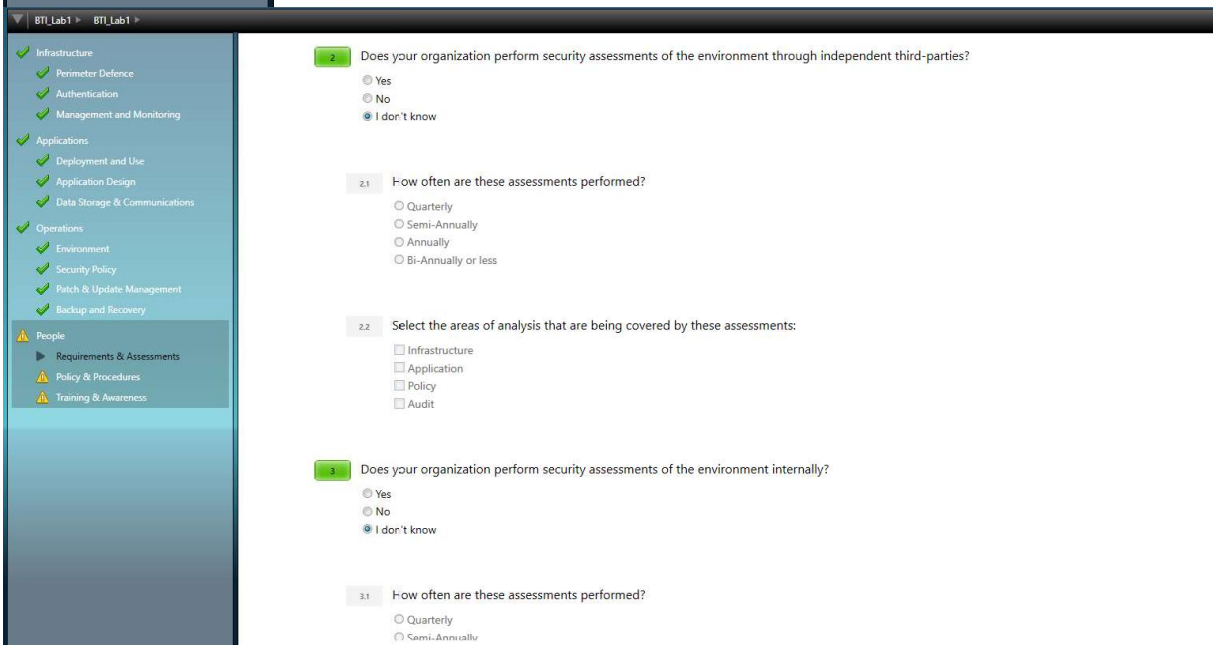

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
2 Does an established patch and update policy and process exist?
Yes
No
I don't know
2.1 Select the components for which these exist:
Operating Systems
Applications
Both Operating Systems and Applications
2.2 Does the organization test patches and updates before deploying them?
Yes
No
I don't know
2.3 Indicate which of the following are used to deploy and manage patches:
Windows Automatic Update
Windows Update website
Windows Server Update Services (WSUS)
Systems Management Server (SMS)
Other patch management solution(s)
System Center Configuration Manager (SCCM)

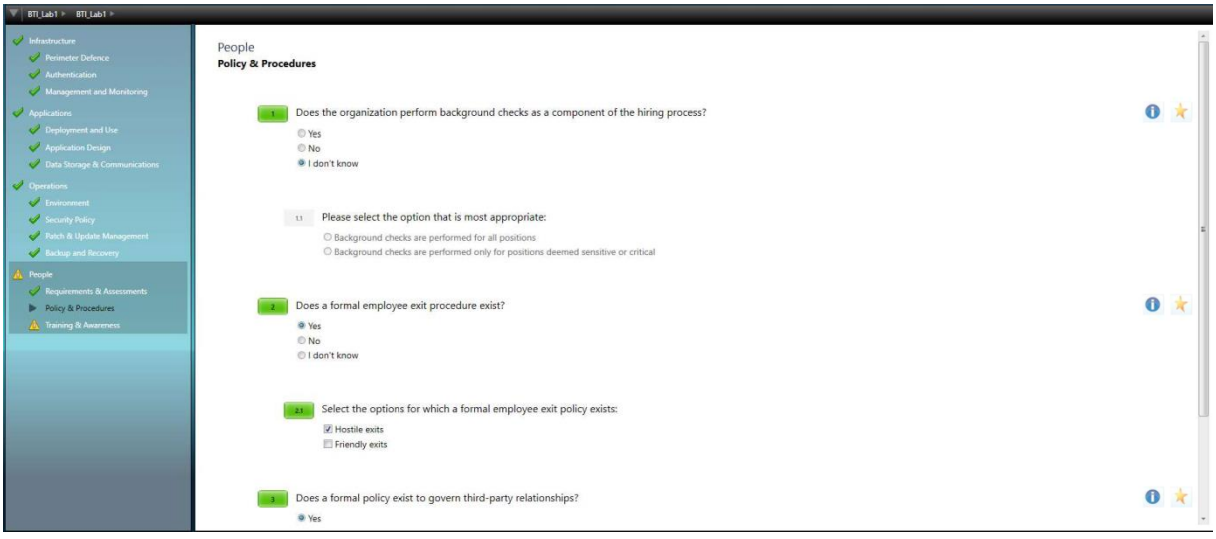

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Workstations and laptops
Servers
3 Does an established policy exist to govern the updating of signature-based detection products?
Ant-virus
Intrusion-detection system (IDS)
None
4 Do accurate logical diagrams and supporting configuration documentation exist for the network infrastructure and hosts?
Yes
No
I don't know
Diagrams exist but they are out of date
5 Do accurate application architecture and data flow diagrams exist for key applications?
Yes
No
I don't know
5.1 For which types of applications do diagrams exist:
External applications only
Internal applications only
Both internal and external applications

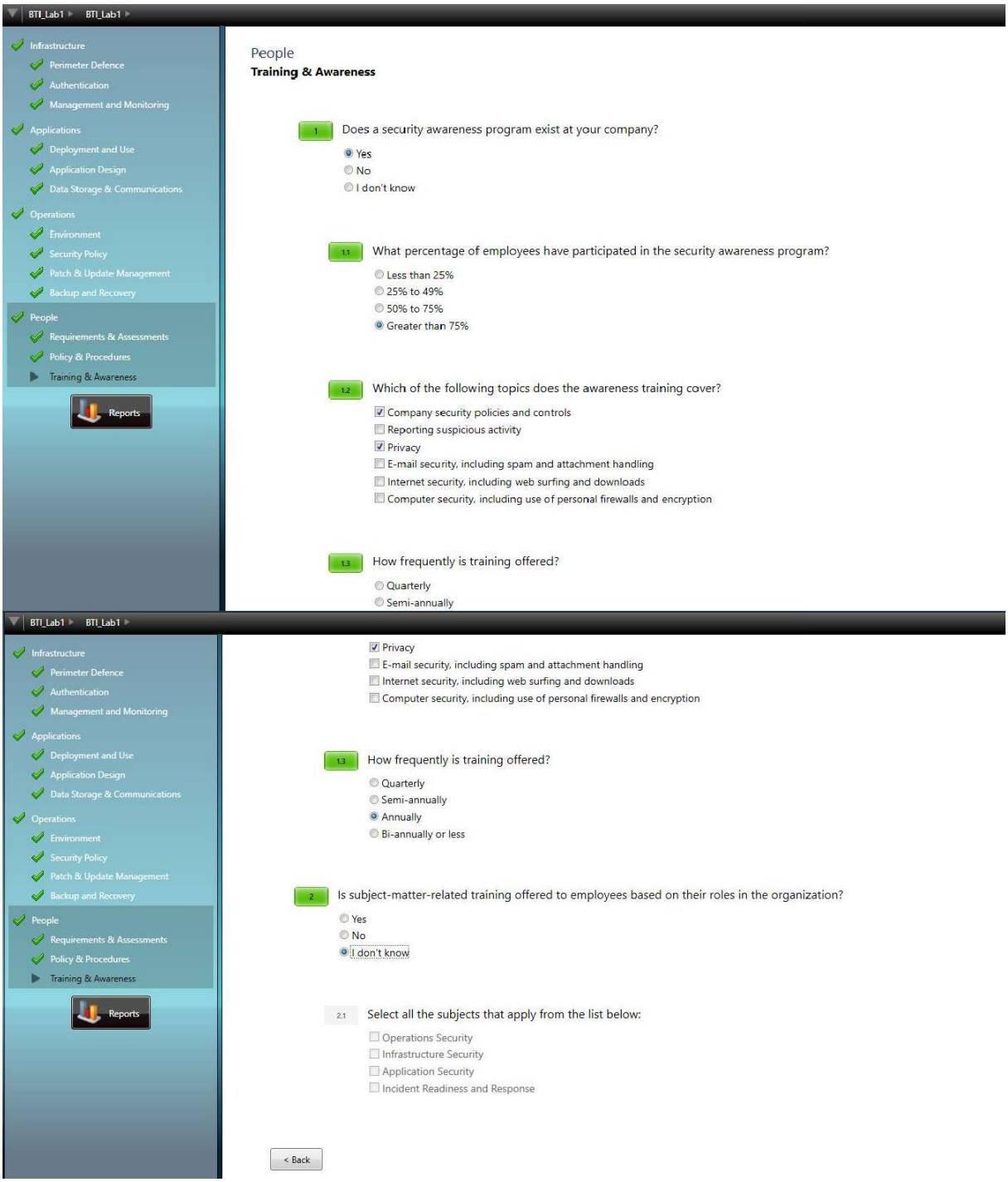

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
Operations
Backup and Recovery
1 Is logging enabled in the environment to record events on hosts and devices?
Yes
No
I don't know
1.1 Does the organization take measures to protect the information contained within logs?
Operating system and applications are configured to not overwrite events
Log files are rotated frequently to ensure sufficient space is available
Access to log files is restricted to administrator-level accounts
Logs are written to a centralized log server
1.2 Does the organization review log files regularly?
Yes
No
I don't know
1.2.1 How often are log files reviewed?
Daily
Weekly
Monthly
As needed
I do not know


BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
2 Is critical and sensitive data backed up on a regular basis?
Yes
No
I don't know
2.1 Do policies and procedures exist for storage and handling of backup media?
Yes
No
I don't know
2.1.1 Which of the following policies and procedures are followed:
Offsite storage
Storage in locked fireproof cabinets
Restricted personnel access to backup media
Rotation and lifecycle of backup media
2.2 Do policies exist for regular testing of backup and restore procedures? Are these policies documented?
Yes, and they are documented
Yes, but they are not documented
No
I don't know


BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
People
Requirements & Assessments
1 Do you have an individual or group in your company that is responsible for security?
Yes
No
I don't know
1.1 Does this individual or team have security subject matter expertise?
Yes
No
I don't know
1.2 Is this individual or group involved in defining security requirements for new and existing technologies?
Yes
No
I don't know
1.3 At what stages of the technology lifecycle is this security team or individual involved?
Planning and Design
Implementation
Testing
Deployment

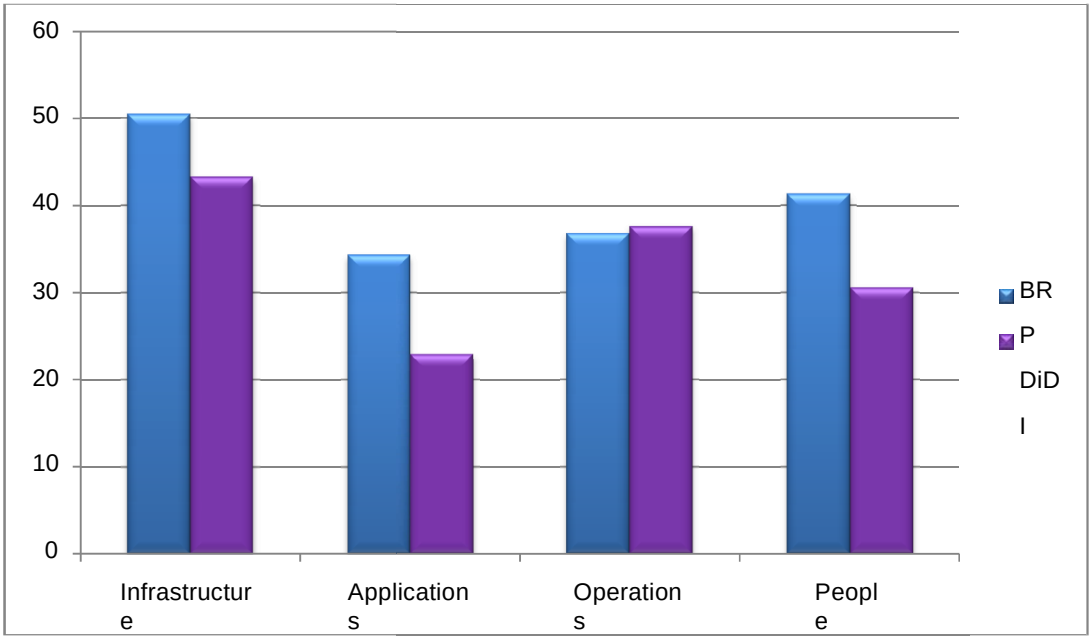

BTI_Lab1 ▸ BTI_Lab1 ▸
Infrastructure
Perimeter Defence
Authentication
Management and Monitoring
Applications
Deployment and Use
Application Design
Data Storage & Communications
Operations
Environment
Security Policy
Patch & Update Management
Backup and Recovery
People
Requirements & Assessments
Policy & Procedures
Training & Awareness
2 Does your organization perform security assessments of the environment through independent third-parties?
Yes
No
I don't know
2.1 How often are these assessments performed?
Quarterly
Semi-Annually
Annually
Bi-Annually or less
2.2 Select the areas of analysis that are being covered by these assessments:
Infrastructure
Application
Policy
Audit
3 Does your organization perform security assessments of the environment internally?
Yes
No
I don't know
3.1 How often are these assessments performed?
Quarterly


BTI_Lab1 ▸ BTI_Lab1 ▸
People
Policy & Procedures
1 Does the organization perform background checks as a component of the hiring process?
Yes
No
I don't know
1.1 Please select the option that is most appropriate:
Background checks are performed for all positions
Background checks are performed only for positions deemed sensitive or critical
2 Does a formal employee exit procedure exist?
Yes
No
I don't know
2.1 Select the options for which a formal employee exit policy exists:
Hostile exits
Friendly exits
3 Does a formal policy exist to govern third-party relationships?
Yes



Po odpowiedzeniu na wszystkie pytania zostanie wygenerowany dokument z oceną ryzyka w naszej firmie wraz z wytłumaczeniem poszczególnych oznaczeń.

Business Risk Profile vs. Defense-in-Depth Index Summary Report



Interpreting the Graphs

- BRP ranges from 0 to 100, where a higher score implies a greater amount of potential business risk for that specific AoA. It is important to note that a score of zero is not possible here; conducting business in itself implies some level of risk. It is also important to understand that there are some aspects of running a business that have no direct mitigation strategy.
    - **Business Risk Profile (BRP)** - A measurement of the risk to which an organization is exposed, based on the business environment and industry in which it competes.
    - **AoAs** - Areas of Analysis which are infrastructure, applications, operations, and people.
- DiDI also ranges from 0 to 100. A high score indicates an environment where a greater number of measures have been taken to deploy defense-in-depth strategies in a particular AoA. The DiDI score does not reflect overall security efficacy or even resources spent on security, rather it is a reflection of the overall strategy used to defend the environment.
    - **Defence-in-Depth Index (DiDI)** - A measurement of the security defences used across people, process and technology to help to mitigate the risks identified for a business.
- Intuitively, it may seem that a low BRP score and a high DiDI score are good outcome, but this is not always the case. The scope of this self-assessment does not allow for all factors to be taken into consideration. Significant disparity between BRP and DiDI scores in a particular AoA suggests that further examination of this AoA is recomm nded. When analyzing your results it is important to consider the individual scores, both BRP and DiDI, in relation to one another. A stable environment will probably be represented by relatively equal scores across all areas. Disparities between DiDI scores are a strong indicator that overall security strategy is focused on a single mitigation technique. If the security strategy does not balance people, process and technology aspects, the environment will probably be more vulnerable to attack.

2. Podsumowanie

Według przeprowadzonej oceny ryzyka w firmie ‘XXX’ poziom ryzyka w firmie jest wysoki. Ilość środków przeznaczonych na wgłębienie się w lepszą ochronę firmy jest zbyt mała co może spowodować utratę ważnych danych i utratę wielu klientów.
Powinny zostać wprowadzone nowe procedury ochronne, poziom zabezpieczeń infrastruktury firmy powinnien zostać zwiększony poprzez dodanie odpowiednich uprawnień poszczególnym