User Manual for Vivaan-Armor Security Manager Brought to you by Aan Systems

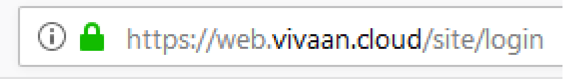
VIVAAN-ARMOR
train, engage, secure, comply

How-To Manual ©Vivaan-Armor and Aan Systems, v1.0, 10-24-2018

Purpose: The purpose of this How-To manual is to make the ease of navigation through the Vivaan-Armor Security Manager a little easier. There are also video tutorials to supplement your learning that will be available throughout the Vivaan-Armor. Vivaan-Armor Makes it easy to build and track your company's Cyber Resiliency. The portal allows companies to maintain its Information Security (IS) and Cybersecurity policy documents and technical controls (such as patch management, anti-virus software and firewall information etc.). A historical index of learning analytics, process readiness and control effectiveness are also tracked. The portal also offers various templates for policies that any company can modify and adapt for its own purpose.

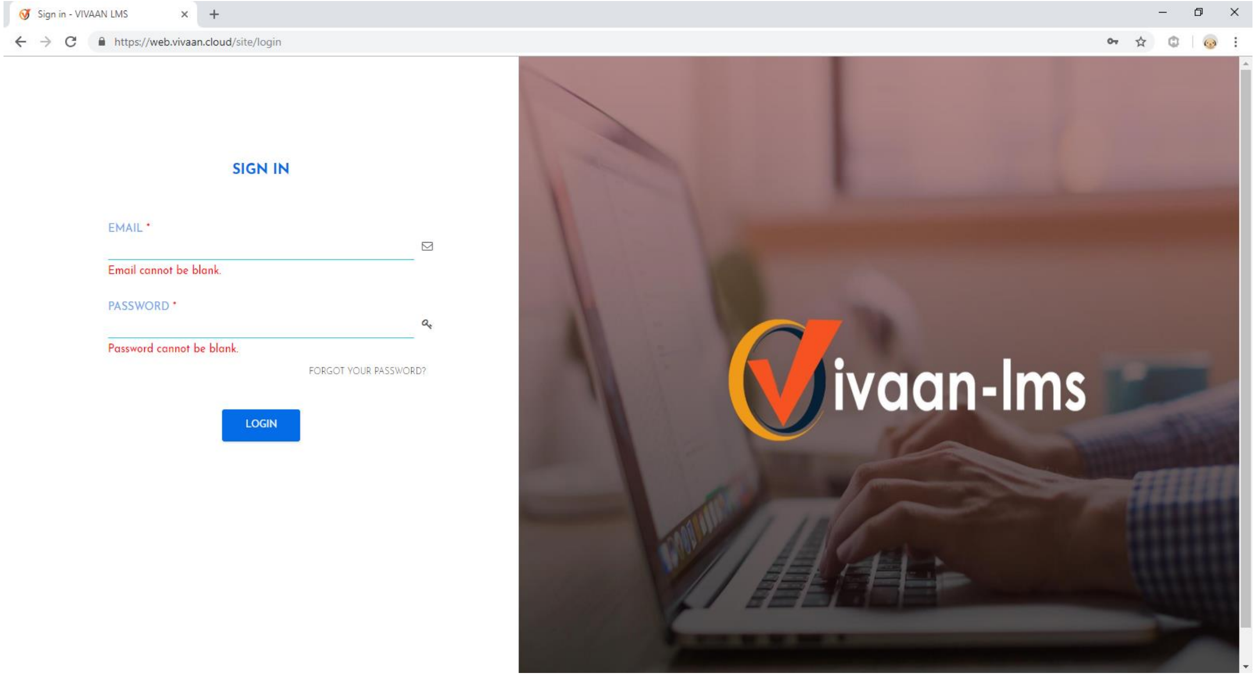
Step-By-Step Process:

1) Pull up a new browser and enter the following in the URL: https://web.vivaan.cloud



https://web.vivaan.cloud/site/login

2) This is the first screen you will see after inputting the URL above:

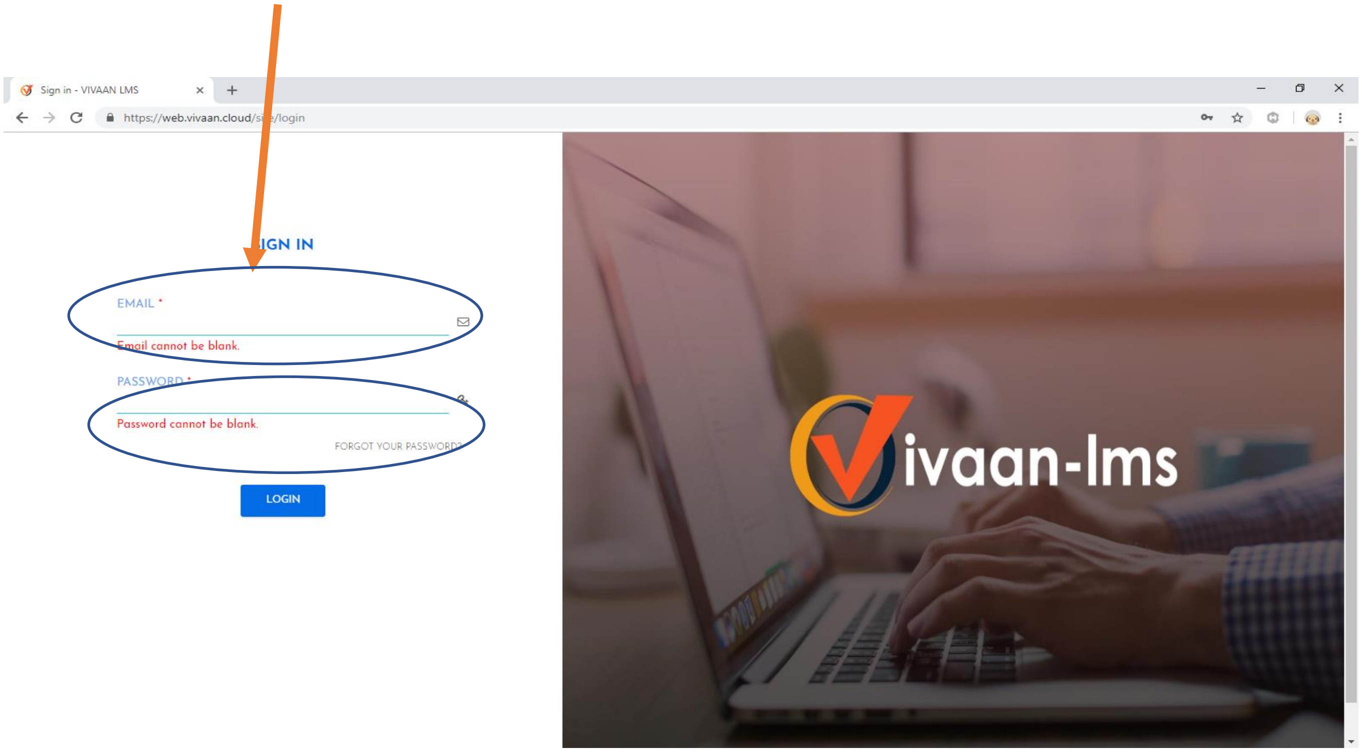


https://web.vivaan.cloud/site/login

Email cannot be blank.

Password cannot be blank.

3) Enter in the email address and password that your admin or corporate leader has provided to you.



Sign in - VIVAAN LMS

https://web.vivaan.cloud/s /login

IGN IN

EMAIL *

Email cannot be blank.

PASSWORD *

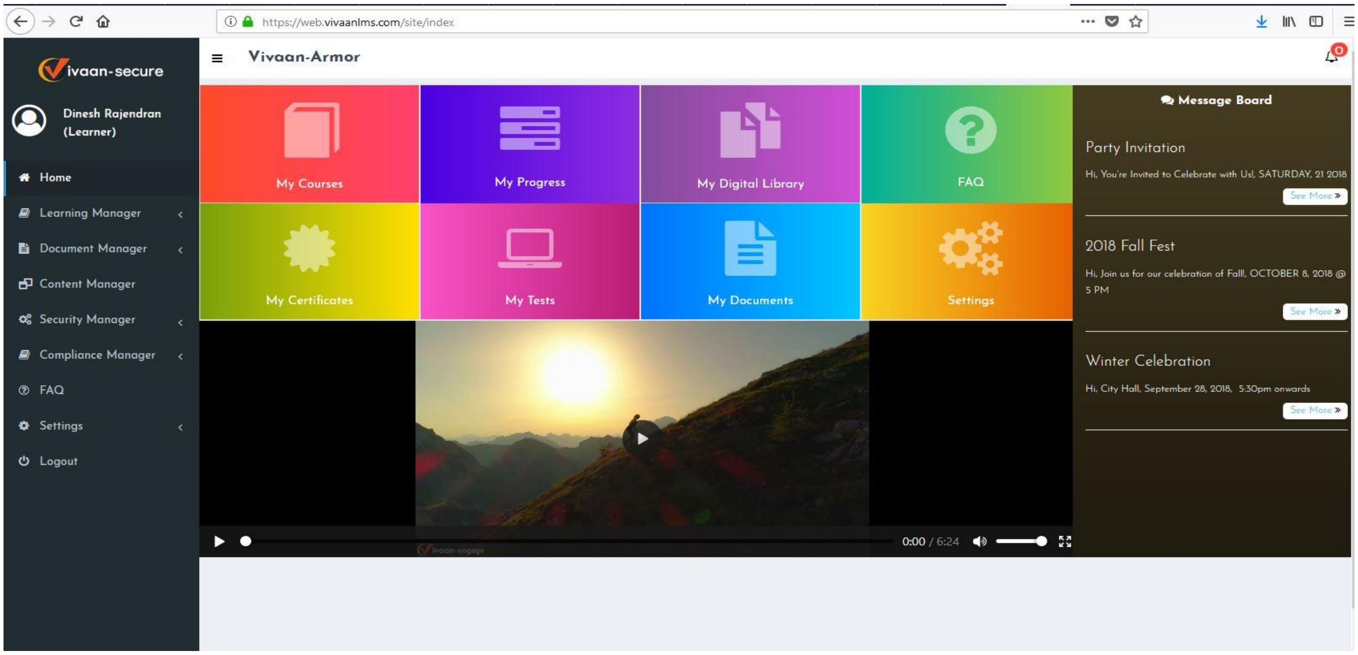
Password cannot be blank.

FORGOT YOUR PASSWORD?

LOGIN

Each learner or super admin, branch manager, etc., will have their own login and password. Each level of management will have different privileges in terms of being able to create classes, accounts, learners depending on the level of power that they have in the hierarchy of the LMS. This hierarchical assignment is determined by your company and the individual learners, and admin are assigned responsibilities and/classes accordingly.

4) After successful login, you should see the main home screen of the Vivaan-Armor.



https://web.vivaanlms.com/site/index

Vivaan-Armor

Dinesh Rajendran (Learner)

Message Board

Party Invitation

Hi, You're Invited to Celebrate with Us!, SATURDAY, 21 2018

See More »

2018 Fall Fest

Hi, Join us for our celebration of Fall!, OCTOBER 8, 2018 @ 5 PM

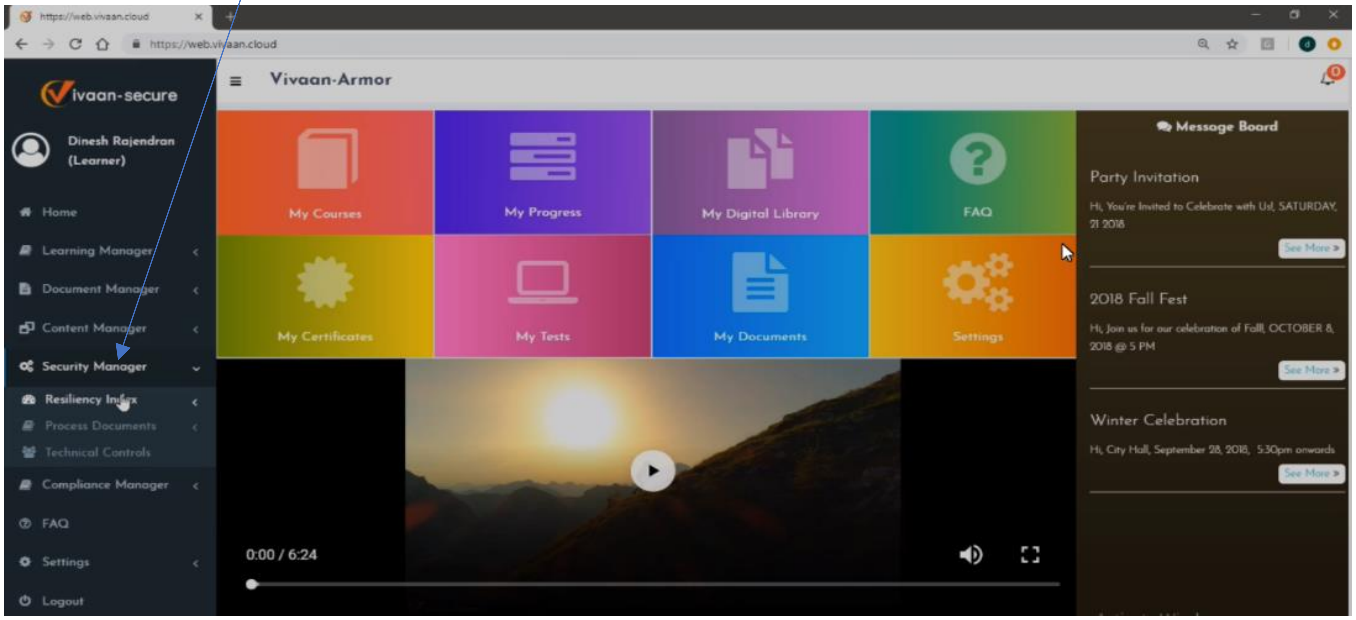
See More »

Winter Celebration

Hi, City Hall, September 28, 2018, 5:30pm onwards

See More »

5) Click on Security Manager and notice that the menu expands to show: Resiliency Index, Process Documents, and Technical Controls.



Party Invitation

Hi, You're Invited to Celebrate with Us!, SATURDAY, 21 2018

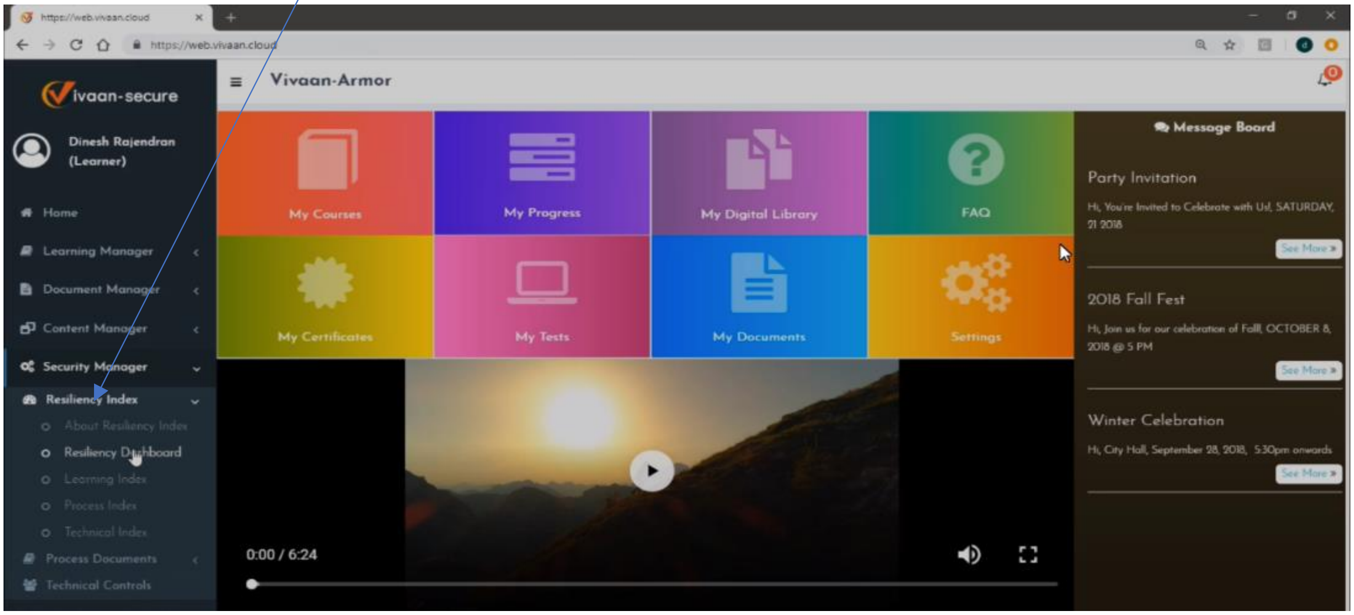
2018 Fall Fest

Hi, Join us for our celebration of Fall!, OCTOBER 8, 2018 @ 5 PM

Winter Celebration

Hi, City Hall, September 28, 2018, 5:30pm onwards

6) Click on the Resiliency Index to expand the menu to show: About Resiliency Index, Resiliency Dashboard, Learning Index, Process Index, and Technical Index.



Party Invitation

Hi, You're Invited to Celebrate with Us!, SATURDAY, 21 2018

2018 Fall Fest

Hi, Join us for our celebration of Fall!, OCTOBER 8, 2018 @ 5 PM

Winter Celebration

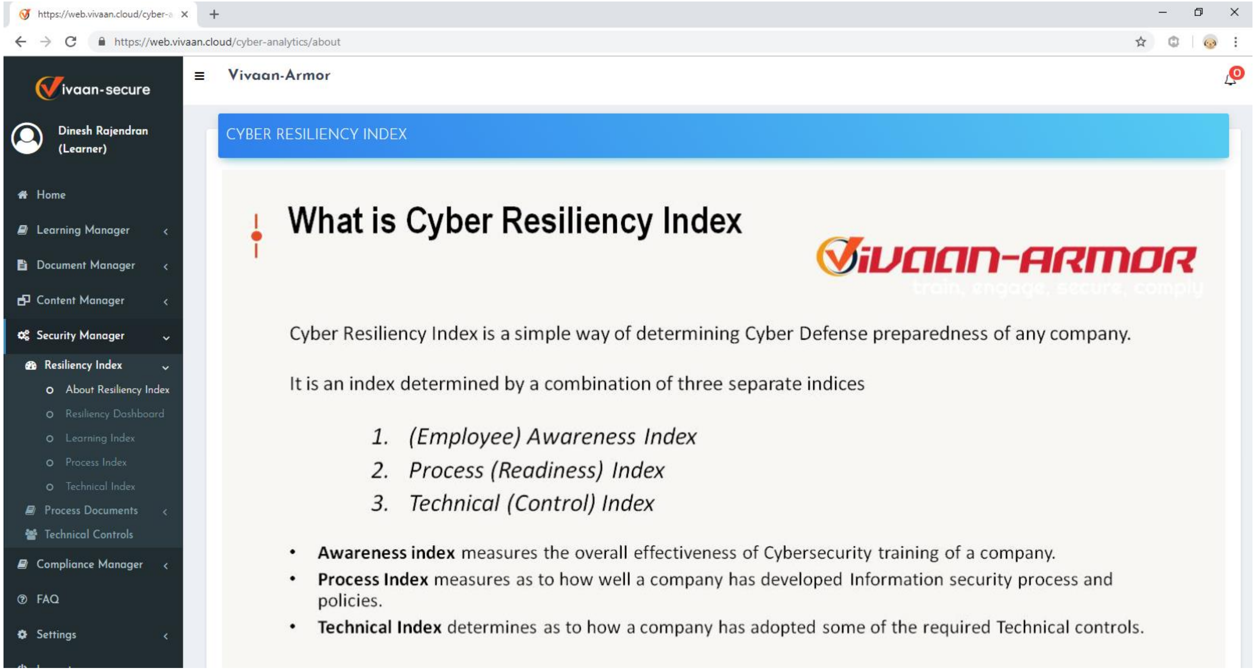
Hi, City Hall, September 28, 2018, 5:30pm onwards

7) Click on “About Resiliency Index” to learn more about Resiliency Index. Cyber Resiliency Index is a simple way of determining Cyber Defense preparedness of any company. It is an index determined by a combination of three separate indices:

   a. (Employee) Awareness Index – measures the overall effectiveness of Cybersecurity training of a company – This is the Learning Index

   b. Process (Readiness) Index – measures as to how well a company has developed Information security processes and policies.

   c. Technical (Control) Index – determines as to how a company has adopted some of the required Technical controls.



CYBER RESILIENCY INDEX

What is Cyber Resiliency Index

Cyber Resiliency Index is a simple way of determining Cyber Defense preparedness of any company.

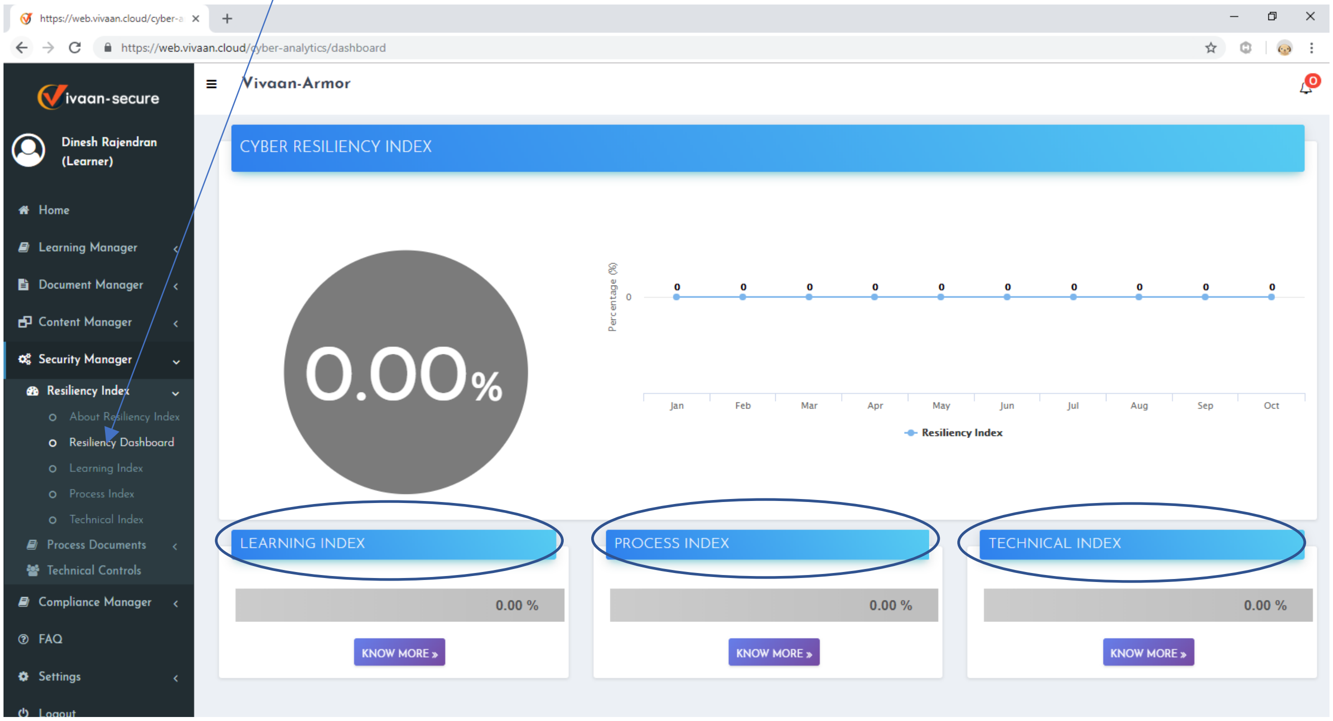
It is an index determined by a combination of three separate indices

1. *(Employee) Awareness Index*
2. *Process (Readiness) Index*
3. *Technical (Control) Index*

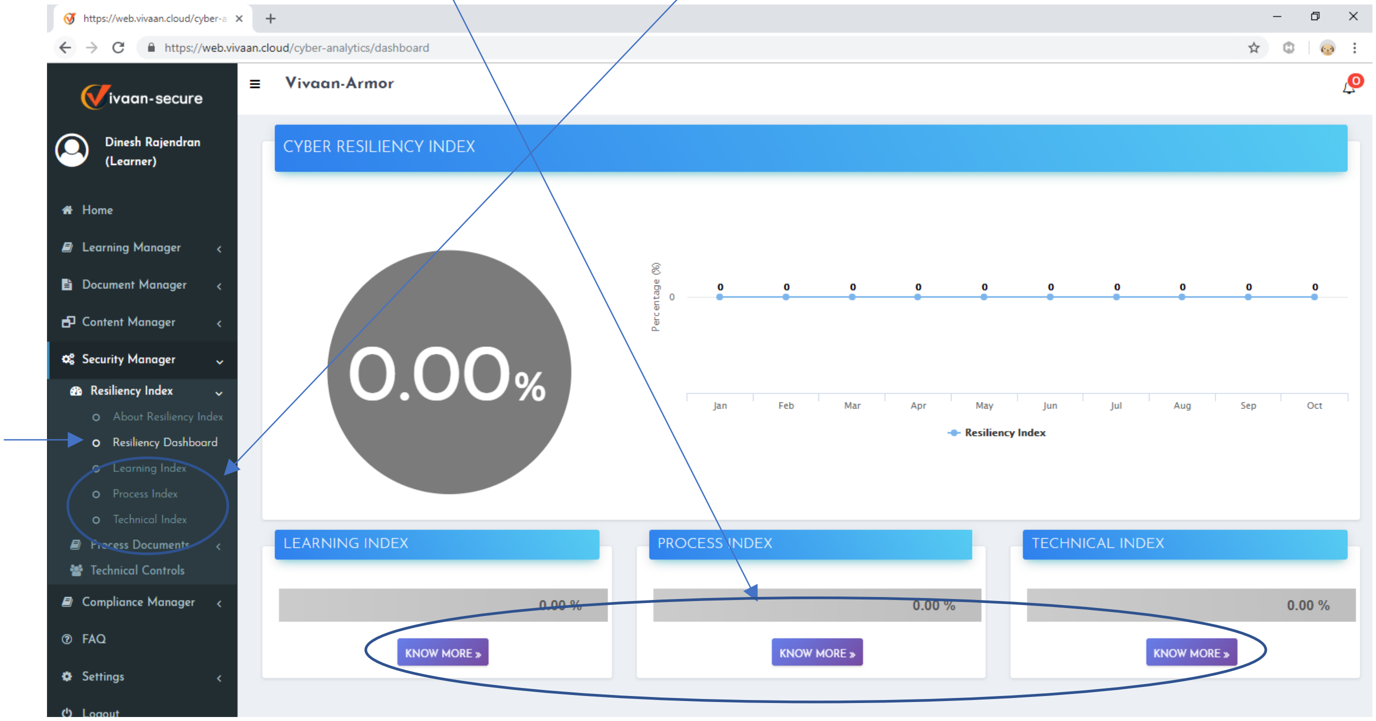
- **Awareness index** measures the overall effectiveness of Cybersecurity training of a company.
- **Process Index** measures as to how well a company has developed Information security process and policies.
- **Technical Index** determines as to how a company has adopted some of the required Technical controls.

8) Click on the Resiliency Dashboard (<Security Manager <Resiliency Index <Resiliency Dashboard) to see the Cyber Resiliency Index which depends on three individual indices Learning Index, Process Index, and Technical Index.

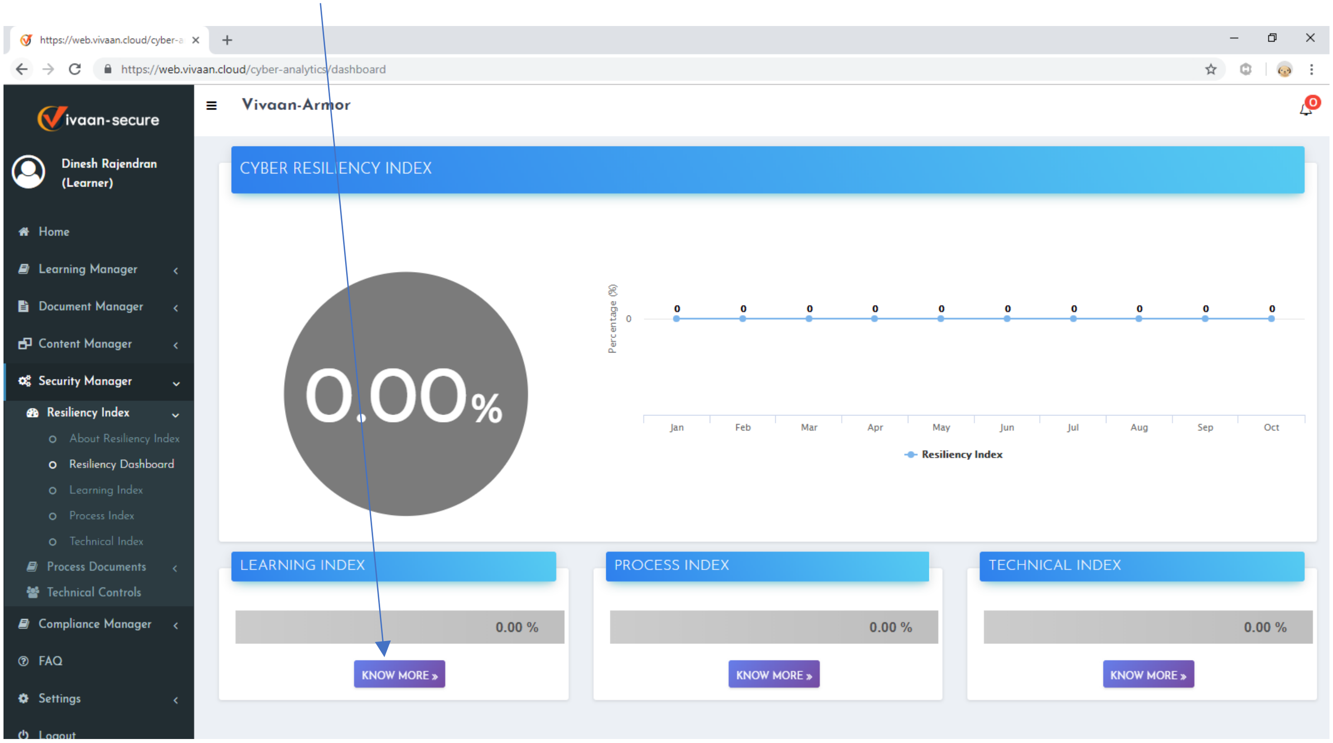
Cyber Resiliency Index = Learning Index + Process Index + Technical Index



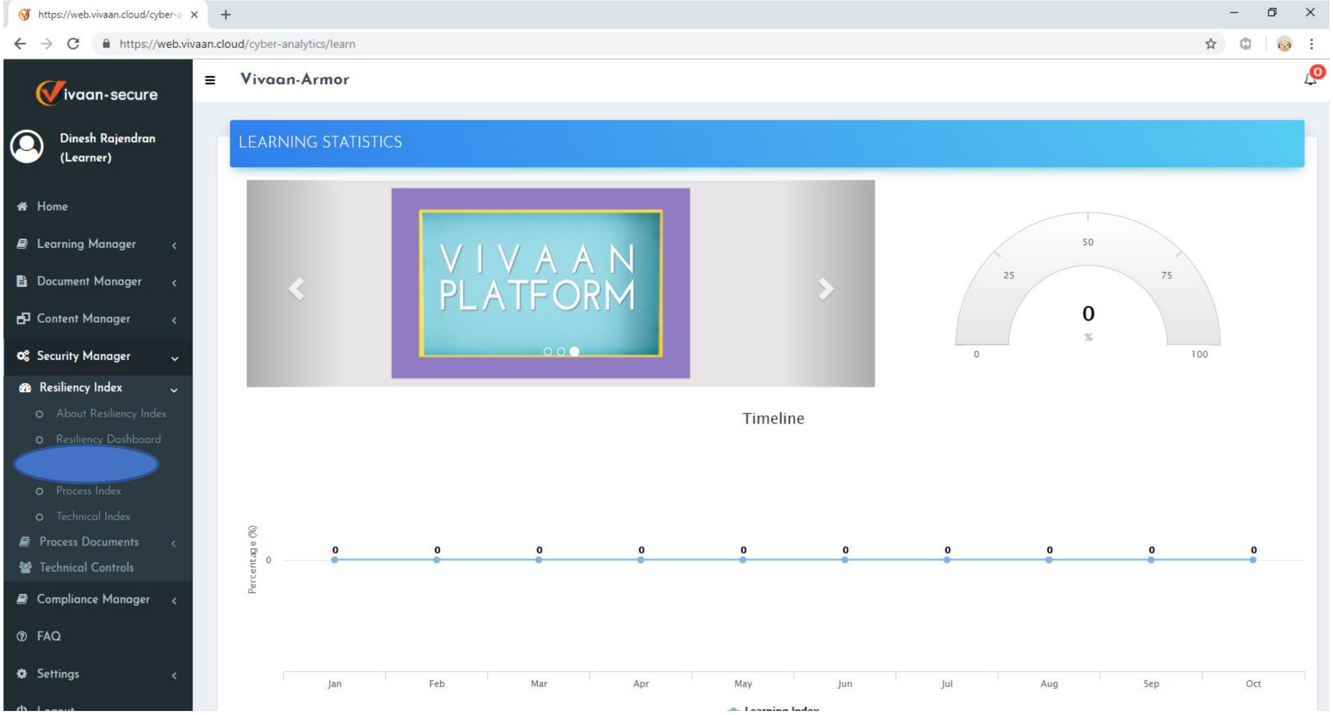
9) The know more buttons in the Resiliency Dashboard under each of the learning indices will take the user to the same page as if they were to click on the links in the grey area that say "Learning Index", "Process Index", and "Technical Index.



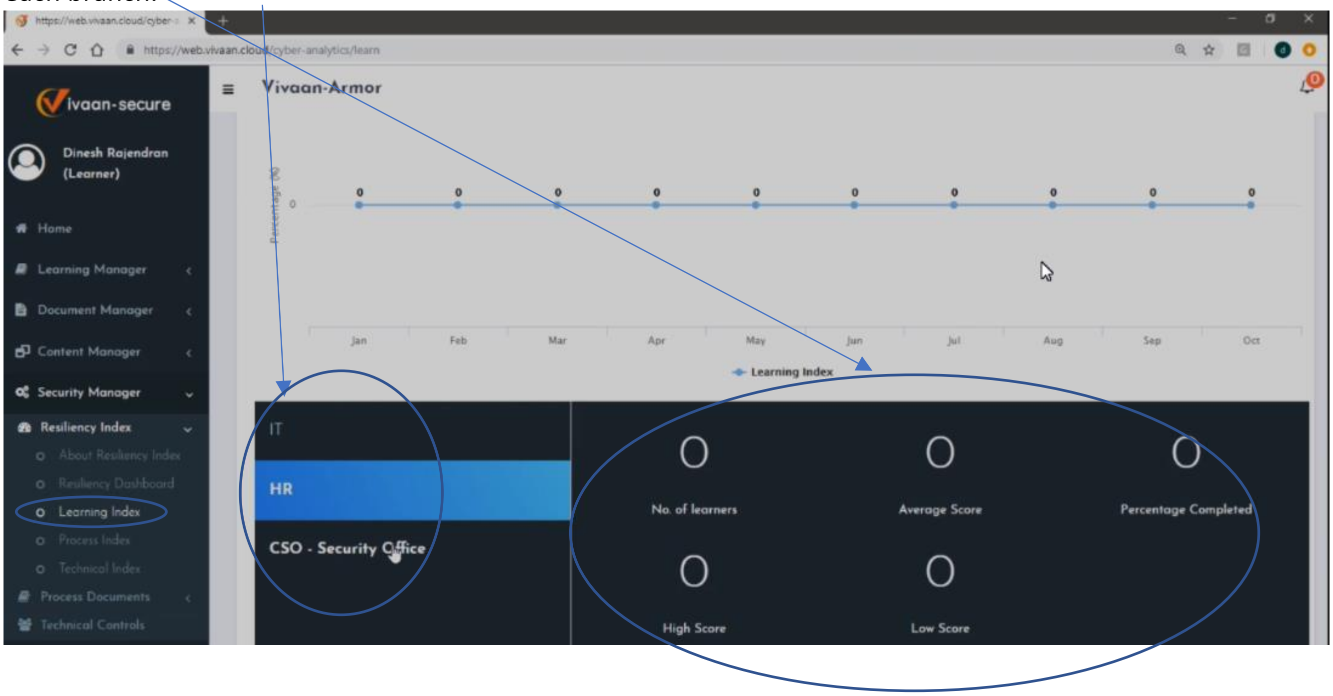
10) Click on the “Know More” button under the Learning Index:



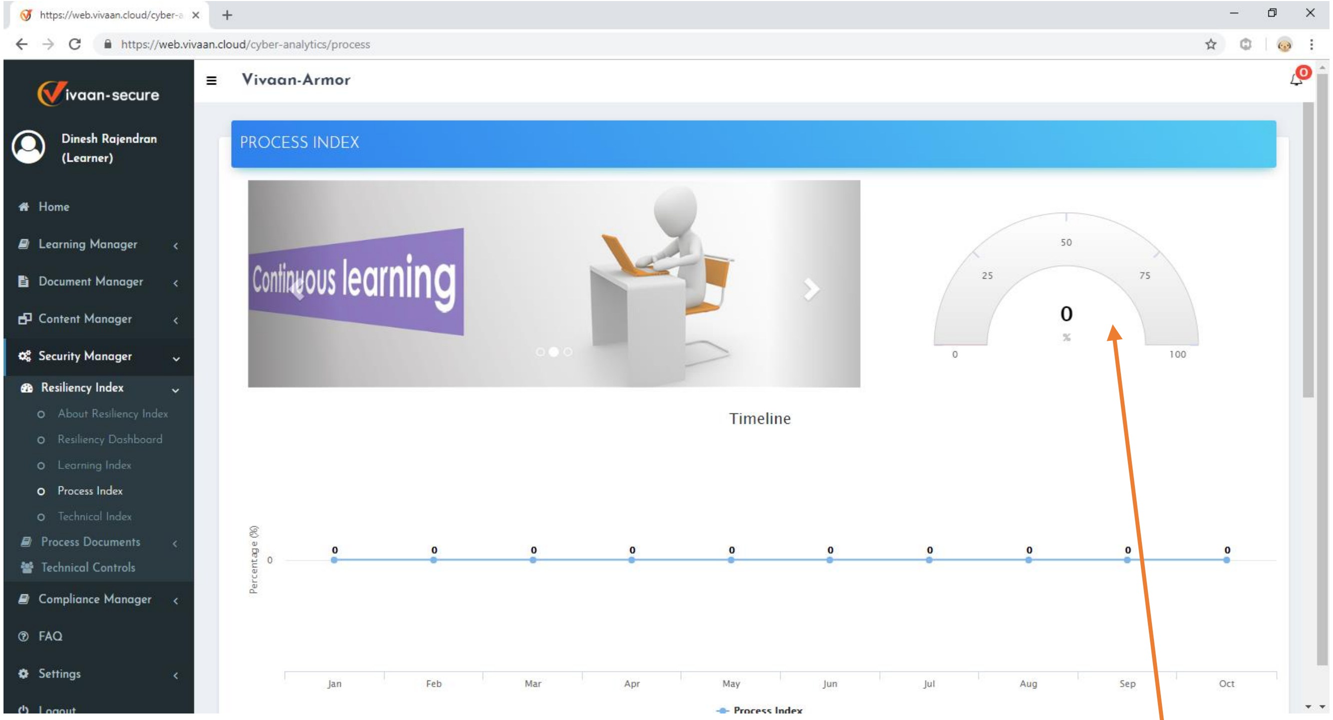
11) Learning Index – we will be able to see the learning index where it’s mainly taken from the percentage completed in a particular branch. The Learning Index is also known as the (Employee) Awareness Index, which measures the overall effectiveness of Cybersecurity training of a company.



12) So, for each branch, percentage completed is considered for the learning index. We are also showing the statistics for the number of learners, high score, average score, low score, and percentage completed for each branch.

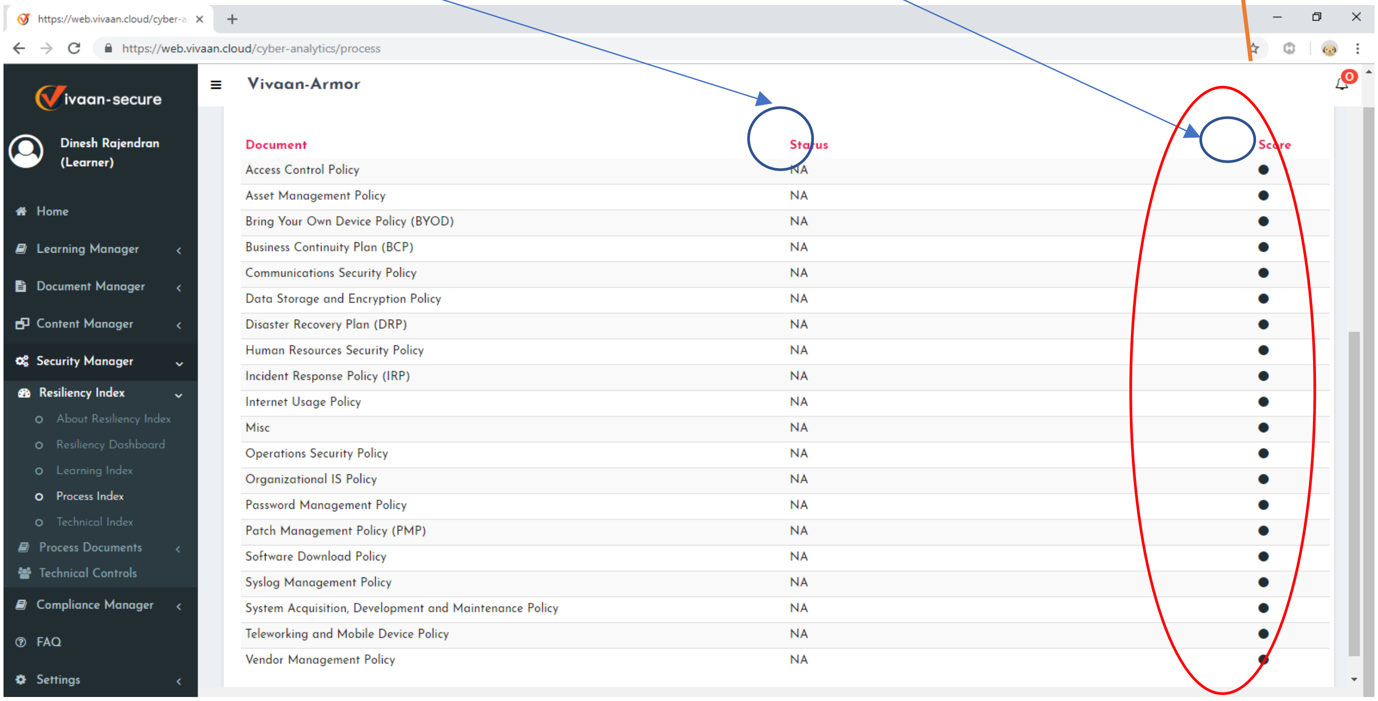


13) Process (Readiness) Index – the process implemented by the company – measures how well a company has developed Information security processes and policies.



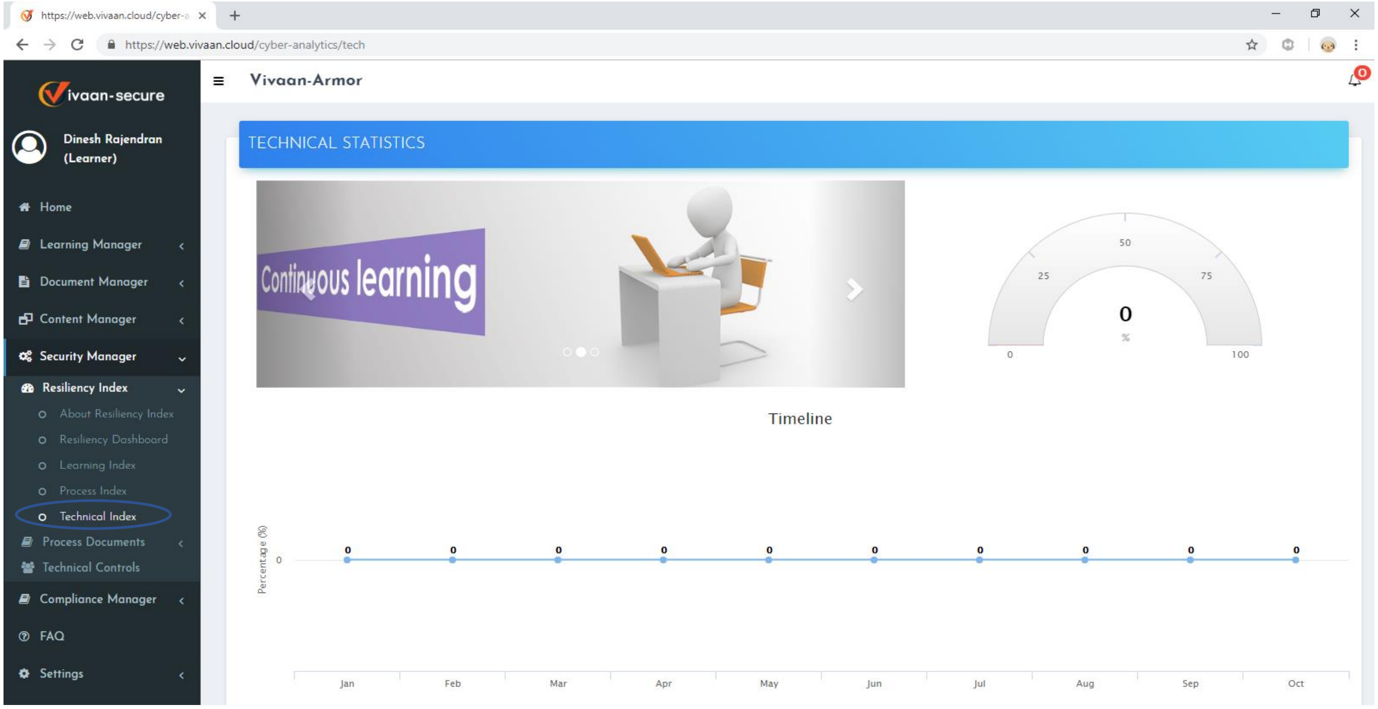
Average of these scores = Process Index

The Status column would display information on whether the policy has been implemented or is required for the company, and based on the response, Vivaan-Armor would assign a score for the particular policy. When you take the average of the scores from these policies, we would be calculating the process index based on that.

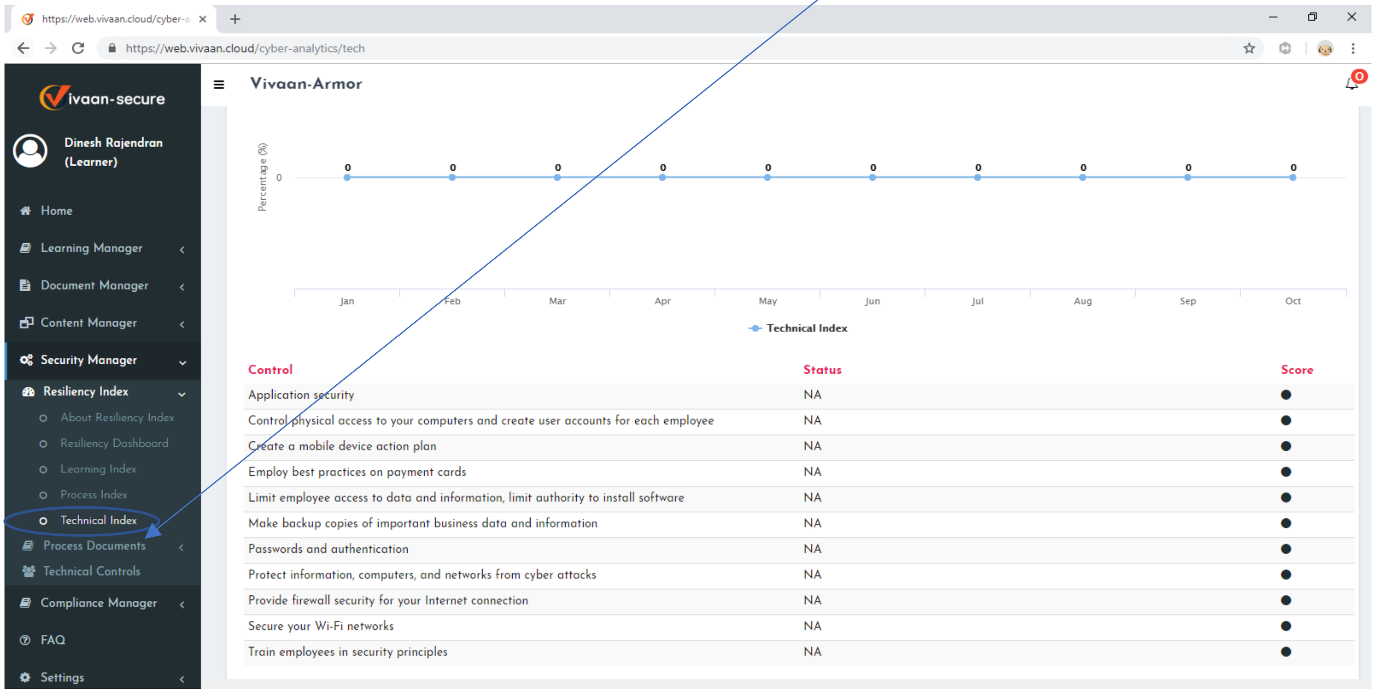


Document	Status	Score
Access Control Policy	NA	●
Asset Management Policy	NA	●
Bring Your Own Device Policy (BYOD)	NA	●
Business Continuity Plan (BCP)	NA	●
Communications Security Policy	NA	●
Data Storage and Encryption Policy	NA	●
Disaster Recovery Plan (DRP)	NA	●
Human Resources Security Policy	NA	●
Incident Response Policy (IRP)	NA	●
Internet Usage Policy	NA	●
Misc	NA	●
Operations Security Policy	NA	●
Organizational IS Policy	NA	●
Password Management Policy	NA	●
Patch Management Policy (PMP)	NA	●
Software Download Policy	NA	●
Syslog Management Policy	NA	●
System Acquisition, Development and Maintenance Policy	NA	●
Teleworking and Mobile Device Policy	NA	●
Vendor Management Policy	NA	●

14) Technical Index – similar to process index. The technical (Control) Index – determines as to how a company has adopted some of the required Technical controls.

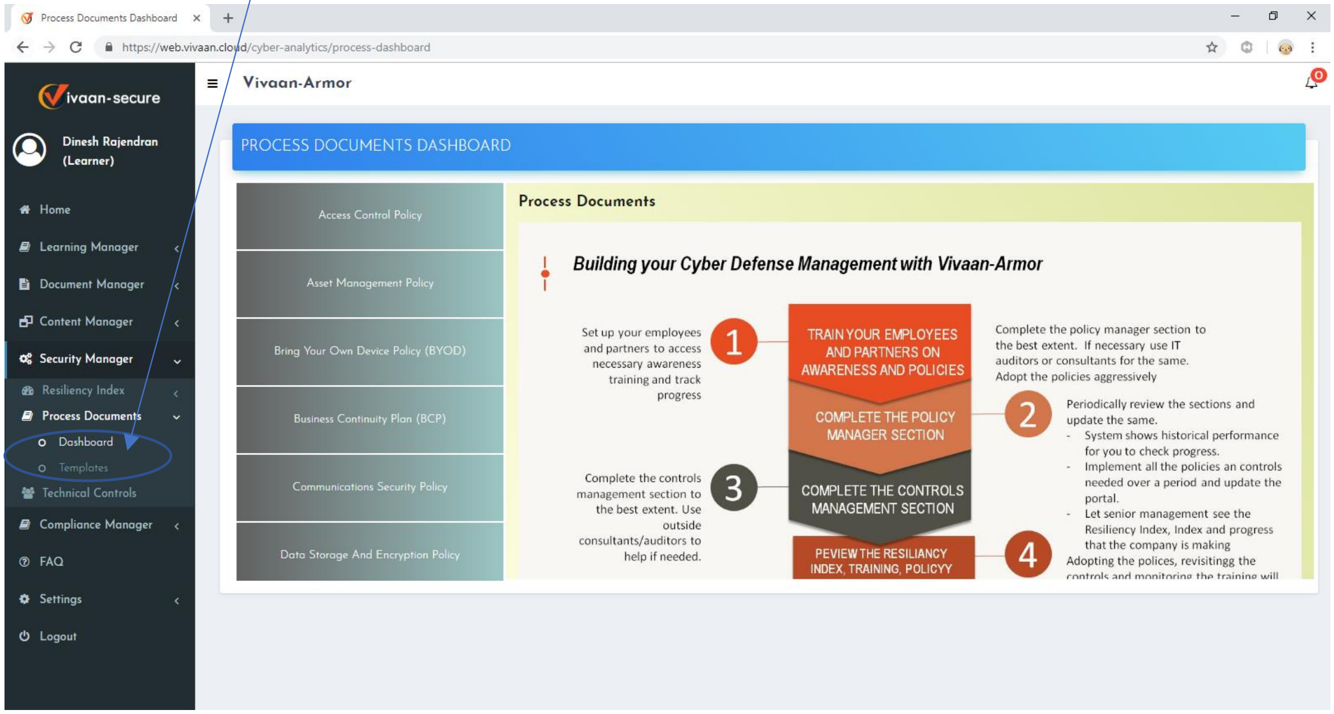


These scores were determined from questions that were answered in the process documents dashboard and depending on the answers that the user gives, the Vivaan-Armor system would calculate a score for each category of questions. The scores will be averaged and a final value for the technical index will be obtained.



Control	Status	Score
Application security	NA	●
Control physical access to your computers and create user accounts for each employee	NA	●
Create a mobile device action plan	NA	●
Employ best practices on payment cards	NA	●
Limit employee access to data and information, limit authority to install software	NA	●
Make backup copies of important business data and information	NA	●
Passwords and authentication	NA	●
Protect information, computers, and networks from cyber attacks	NA	●
Provide firewall security for your Internet connection	NA	●
Secure your Wi-Fi networks	NA	●
Train employees in security principles	NA	●

15) Click on Process Documents to expand the menu (Security Manager<Process Documents) to show Dashboard and Templates.


Process Documents Dashboard
https://web.vivaan.cloud/cyber-analytics/process-dashboard
ivaan-secure
Dinesh Rajendran (Learner)
Home
Learning Manager
Document Manager
Content Manager
Security Manager
Resiliency Index
Process Documents
Dashboard
Templates
Technical Controls
Compliance Manager
FAQ
Settings
Logout
Vivaan-Armor
PROCESS DOCUMENTS DASHBOARD
Access Control Policy
Asset Management Policy
Bring Your Own Device Policy (BYOD)
Business Continuity Plan (BCP)
Communications Security Policy
Data Storage And Encryption Policy
Process Documents

Building your Cyber Defense Management with Vivaan-Armor

1 TRAIN YOUR EMPLOYEES AND PARTNERS ON AWARENESS AND POLICIES: Set up your employees and partners to access necessary awareness training and track progress

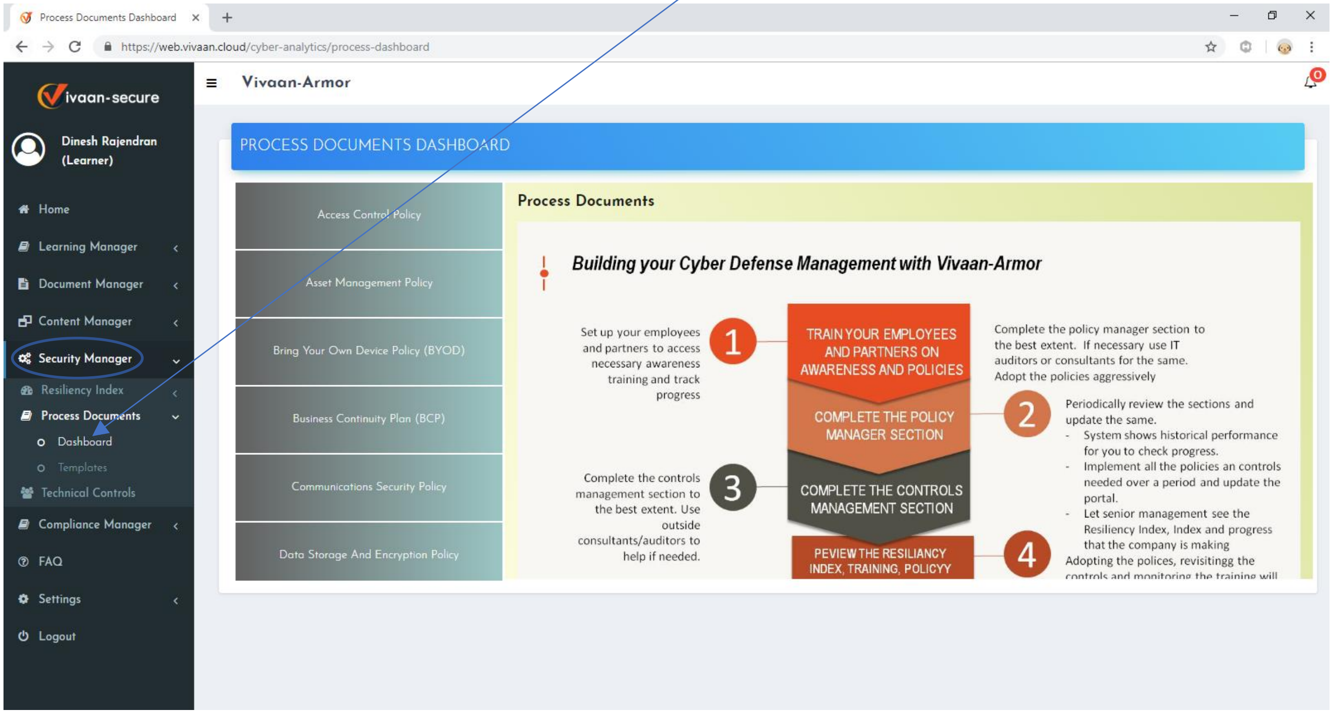
2 COMPLETE THE POLICY MANAGER SECTION: Complete the policy manager section to the best extent. If necessary use IT auditors or consultants for the same. Adopt the policies aggressively

3 COMPLETE THE CONTROLS MANAGEMENT SECTION: Complete the controls management section to the best extent. Use outside consultants/auditors to help if needed.

4 PEVIEW THE RESILIANCY INDEX, TRAINING, POLICYY: Periodically review the sections and update the same.
- System shows historical performance for you to check progress.
- Implement all the policies an controls needed over a period and update the portal.
- Let senior management see the Resiliency Index, Index and progress that the company is making

Adopting the polices, revisitingg the controls and monitoring the training will

16) This is the screen that is shown when you click on Dashboards (Security Manager<Process Documents<Dashboard).


Building your Cyber Defense Management with Vivaan-Armor

1 TRAIN YOUR EMPLOYEES AND PARTNERS ON AWARENESS AND POLICIES: Set up your employees and partners to access necessary awareness training and track progress

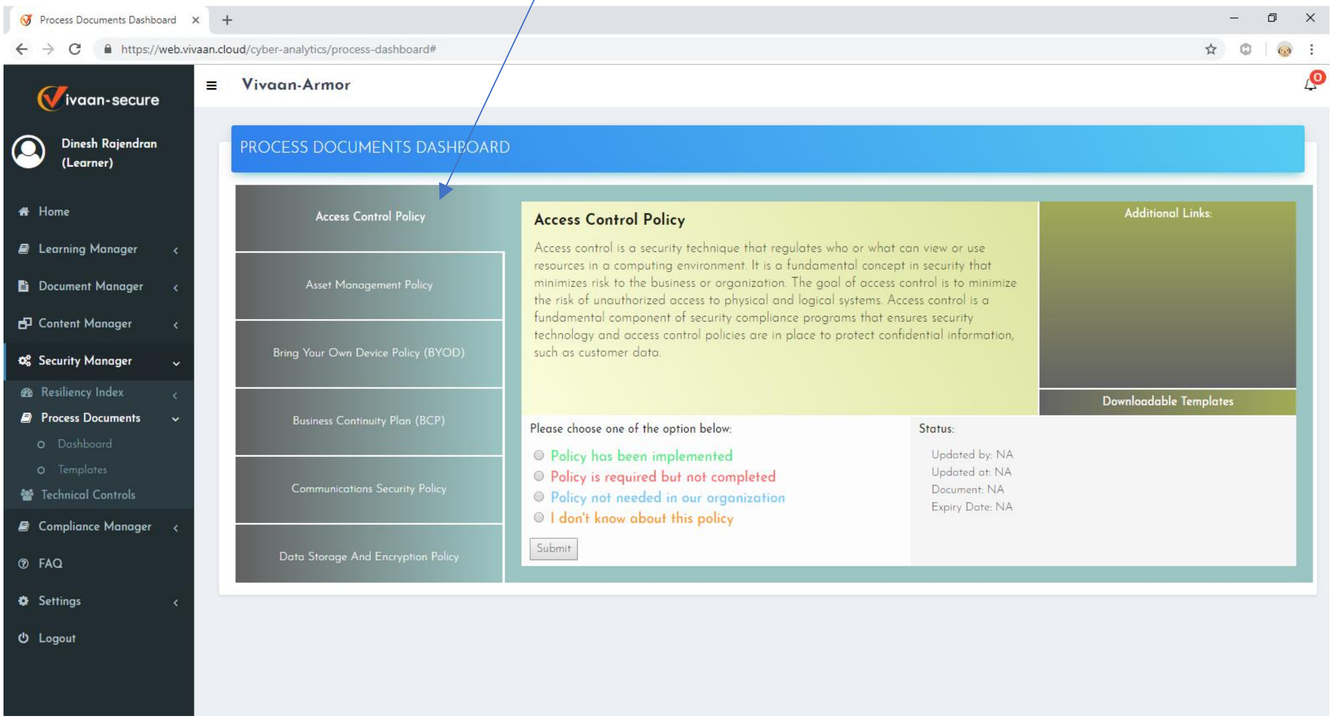
2 COMPLETE THE POLICY MANAGER SECTION: Complete the policy manager section to the best extent. If necessary use IT auditors or consultants for the same. Adopt the policies aggressively

3 COMPLETE THE CONTROLS MANAGEMENT SECTION: Complete the controls management section to the best extent. Use outside consultants/auditors to help if needed.

4 PEVIEW THE RESILIANCY INDEX, TRAINING, POLICYY: Periodically review the sections and update the same.
- System shows historical performance for you to check progress.
- Implement all the policies an controls needed over a period and update the portal.
- Let senior management see the Resiliency Index, Index and progress that the company is making

Adopting the polices, revisitingg the controls and monitoring the training will

17) Click on any one of the policies in the grey area to answer question that are important in generating your process index (step 13).



PROCESS DOCUMENTS DASHBOARD

Access Control Policy
Asset Management Policy
Bring Your Own Device Policy (BYOD)
Business Continuity Plan (BCP)
Communications Security Policy
Data Storage And Encryption Policy

Access Control Policy

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data.

Additional Links:

Downloadable Templates

Please choose one of the option below:

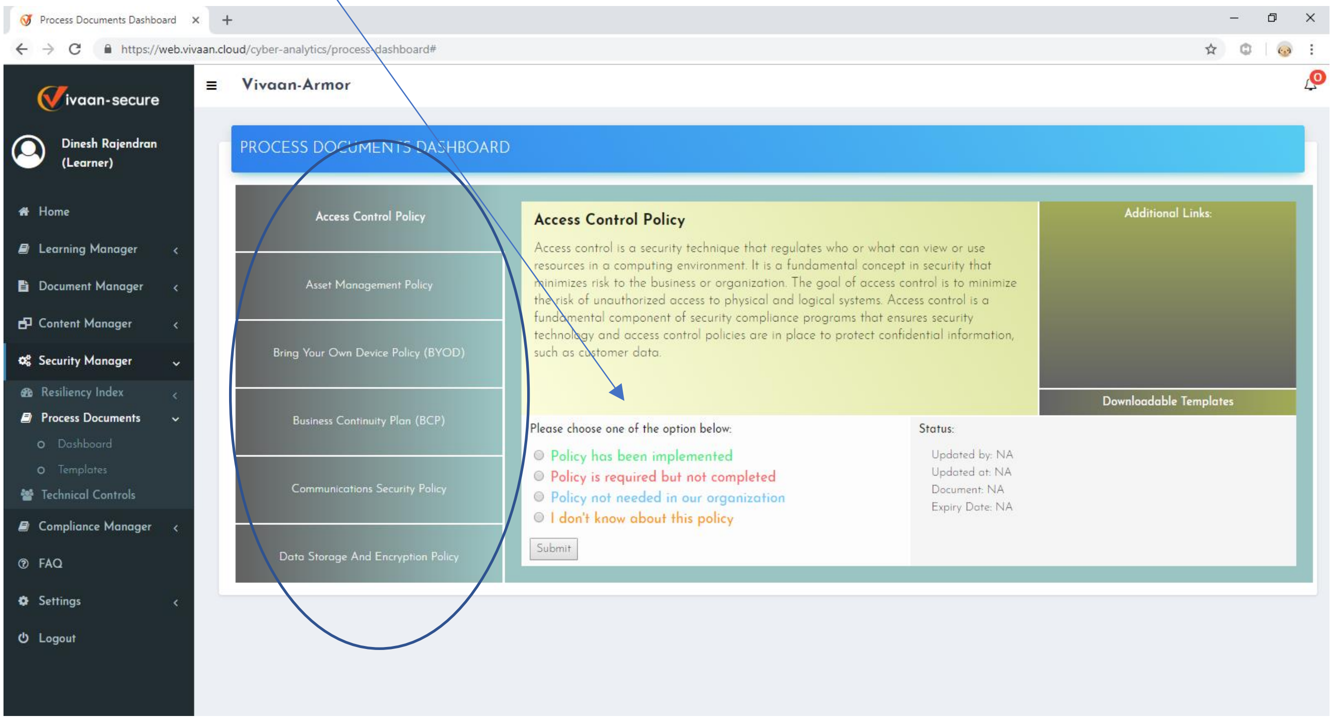
○ Policy has been implemented
○ Policy is required but not completed
○ Policy not needed in our organization
○ I don't know about this policy

Submit

Status:

Updated by: NA
Updated at: NA
Document: NA
Expiry Date: NA

18) Answer the questions for each category. The answers that you provide will be fetched automatically by Vivaan-Armor and will populate into the Resiliency Index section of the Security Manager and used to calculate the process index.



PROCESS DOCUMENTS DASHBOARD

Access Control Policy
Asset Management Policy
Bring Your Own Device Policy (BYOD)
Business Continuity Plan (BCP)
Communications Security Policy
Data Storage And Encryption Policy

Access Control Policy

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data.

Additional Links:

Downloadable Templates

Please choose one of the option below:

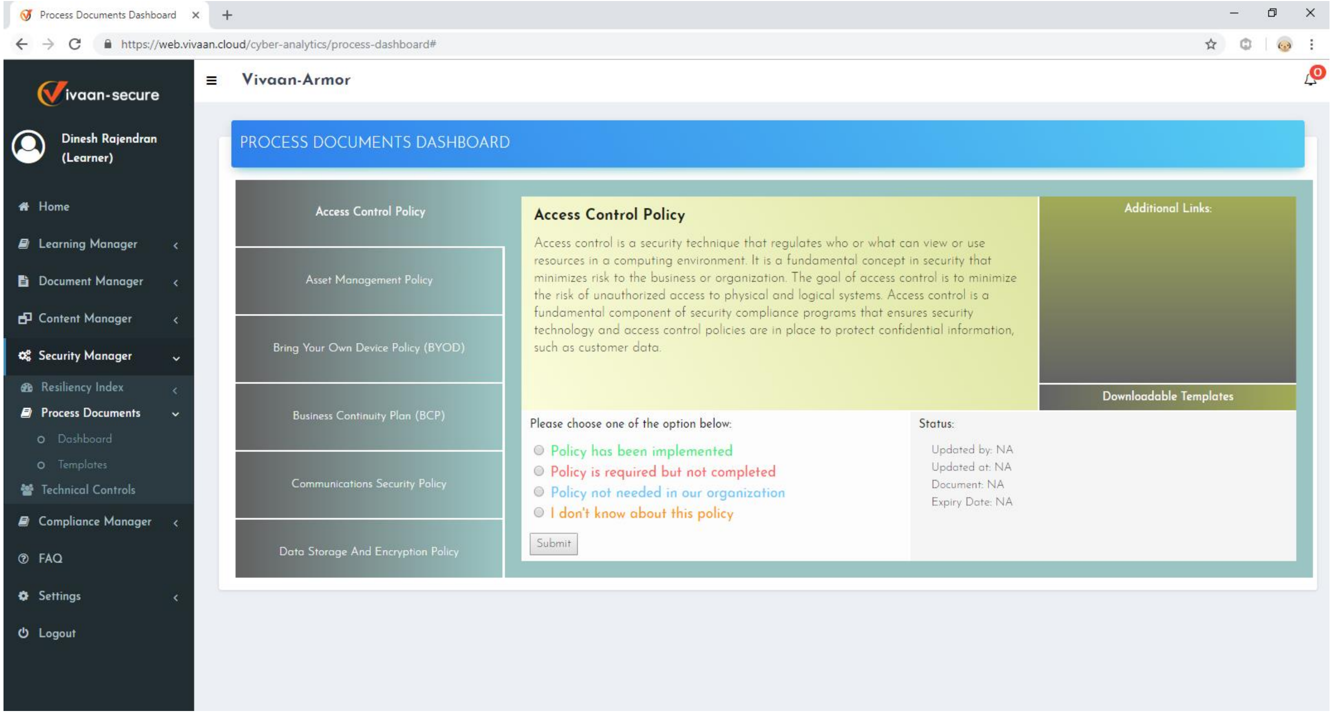
○ Policy has been implemented
○ Policy is required but not completed
○ Policy not needed in our organization
○ I don't know about this policy

Submit

Status:

Updated by: NA
Updated at: NA
Document: NA
Expiry Date: NA

The user can select the correct answer that corresponds to their company situation for each set of questions presented under each of the policy categories. This score will be fetched and brought back into the index screen as shown in step 13, averaged, and then used to calculate the process index. A description of the particular policy is also provided in this section.



Access Control Policy

Access control is a security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. The goal of access control is to minimize the risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data.

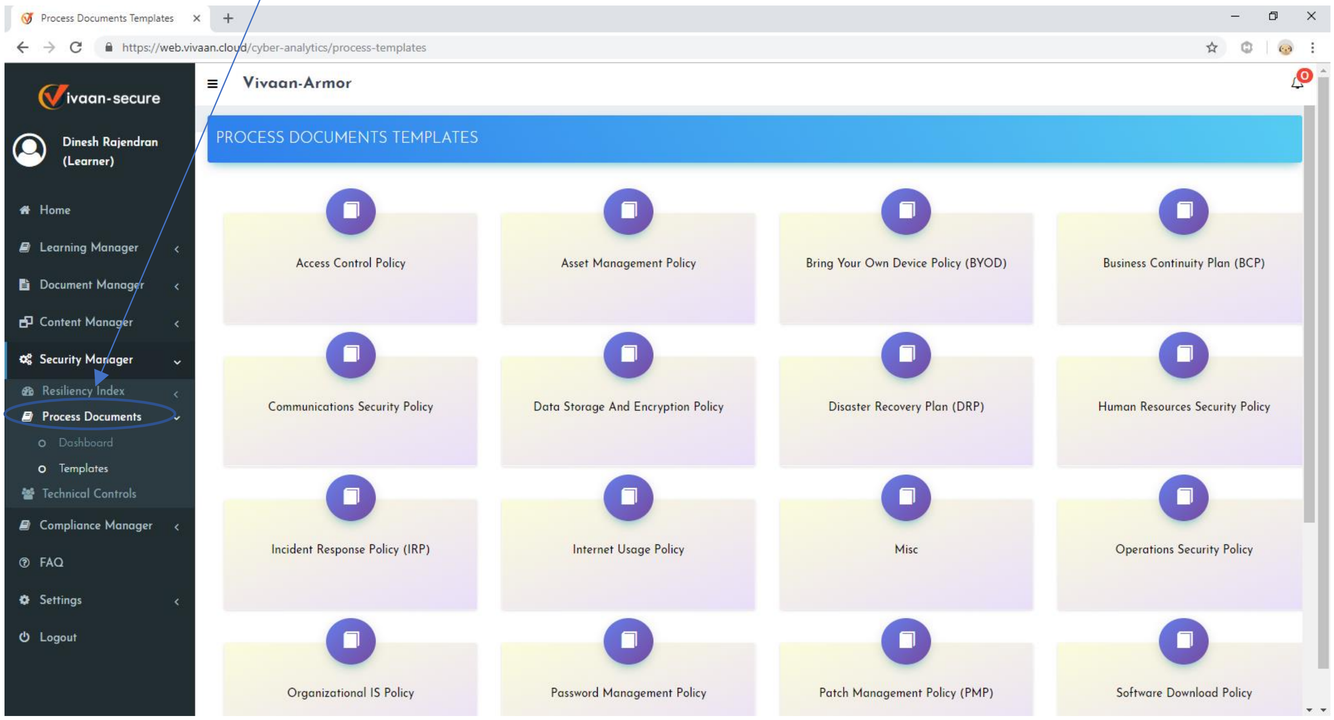
Please choose one of the option below:

○ Policy has been implemented
○ Policy is required but not completed
○ Policy not needed in our organization
○ I don't know about this policy

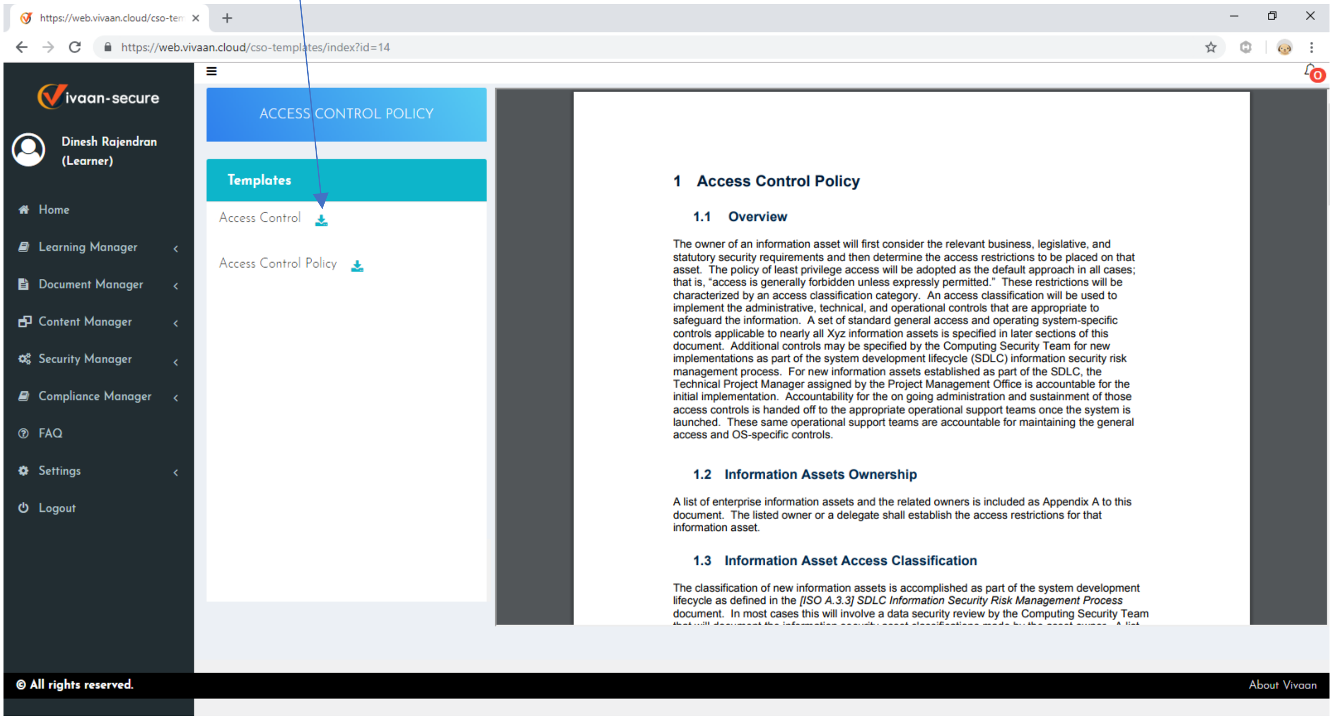
Status:

Updated by: NA
Updated at: NA
Document: NA
Expiry Date: NA

19) This is the template page of the Process Documents under Security Manager (Security Manager <Process Documents<Templates). Click on any one of these templates to view or download and customize your own company policy.


Process Documents Templates
https://web.vivaan.cloud/cyber-analytics/process-templates
ivaan-secure
Vivaan-Armor
Dinesh Rajendran (Learner)
Home
Learning Manager
Document Manager
Content Manager
Security Manager
Resiliency Index
Process Documents
Dashboard
Templates
Technical Controls
Compliance Manager
FAQ
Settings
Logout
PROCESS DOCUMENTS TEMPLATES
Access Control Policy
Asset Management Policy
Bring Your Own Device Policy (BYOD)
Business Continuity Plan (BCP)
Communications Security Policy
Data Storage And Encryption Policy
Disaster Recovery Plan (DRP)
Human Resources Security Policy
Incident Response Policy (IRP)
Internet Usage Policy
Misc
Operations Security Policy
Organizational IS Policy
Password Management Policy
Patch Management Policy (PMP)
Software Download Policy

20) You can download an editable word copy of the template to customize as your own document. Then reload the finished document back into Vivaan-Armor using the Document Manager if you want the document to be approved or the Content Manager if approval is not required.



1 Access Control Policy

1.1 Overview

The owner of an information asset will first consider the relevant business, legislative, and statutory security requirements and then determine the access restrictions to be placed on that asset. The policy of least privilege access will be adopted as the default approach in all cases; that is, "access is generally forbidden unless expressly permitted." These restrictions will be characterized by an access classification category. An access classification will be used to implement the administrative, technical, and operational controls that are appropriate to safeguard the information. A set of standard general access and operating system-specific controls applicable to nearly all Xyz information assets is specified in later sections of this document. Additional controls may be specified by the Computing Security Team for new implementations as part of the system development lifecycle (SDLC) information security risk management process. For new information assets established as part of the SDLC, the Technical Project Manager assigned by the Project Management Office is accountable for the initial implementation. Accountability for the on going administration and sustainment of those access controls is handed off to the appropriate operational support teams once the system is launched. These same operational support teams are accountable for maintaining the general access and OS-specific controls.

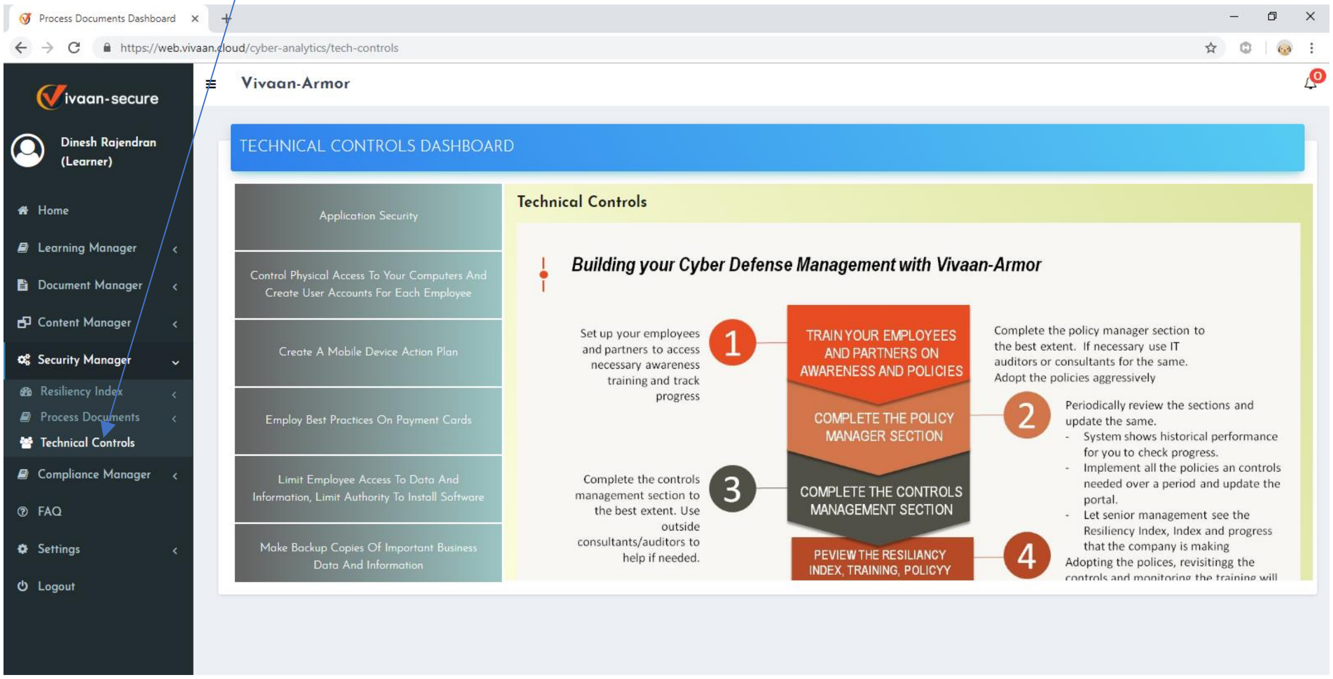
1.2 Information Assets Ownership

A list of enterprise information assets and the related owners is included as Appendix A to this document. The listed owner or a delegate shall establish the access restrictions for that information asset.

1.3 Information Asset Access Classification

The classification of new information assets is accomplished as part of the system development lifecycle as defined in the *[ISO A.3.3] SDLC Information Security Risk Management Process* document. In most cases this will involve a data security review by the Computing Security Team

21) Technical Controls (Security Manager<Technical Controls) – Similar to Process controls.


Process Documents Dashboard
https://web.vivaan.cloud/cyber-analytics/tech-controls
ivaan-secure
Vivaan-Armor
Dinesh Rajendran (Learner)
Home
Learning Manager
Document Manager
Content Manager
Security Manager
Resiliency Index
Process Documents
Technical Controls
Compliance Manager
FAQ
Settings
Logout
TECHNICAL CONTROLS DASHBOARD
Application Security
Control Physical Access To Your Computers And Create User Accounts For Each Employee
Create A Mobile Device Action Plan
Employ Best Practices On Payment Cards
Limit Employee Access To Data And Information, Limit Authority To Install Software
Make Backup Copies Of Important Business Data And Information
Technical Controls
1
TRAIN YOUR EMPLOYEES AND PARTNERS ON AWARENESS AND POLICIES
2
COMPLETE THE POLICY MANAGER SECTION
3
COMPLETE THE CONTROLS MANAGEMENT SECTION
4
PEVIEW THE RESILIANCY INDEX, TRAINING, POLICYY

Building your Cyber Defense Management with Vivaan-Armor

1 Set up your employees and partners to access necessary awareness training and track progress

Complete the policy manager section to the best extent. If necessary use IT auditors or consultants for the same. Adopt the policies aggressively

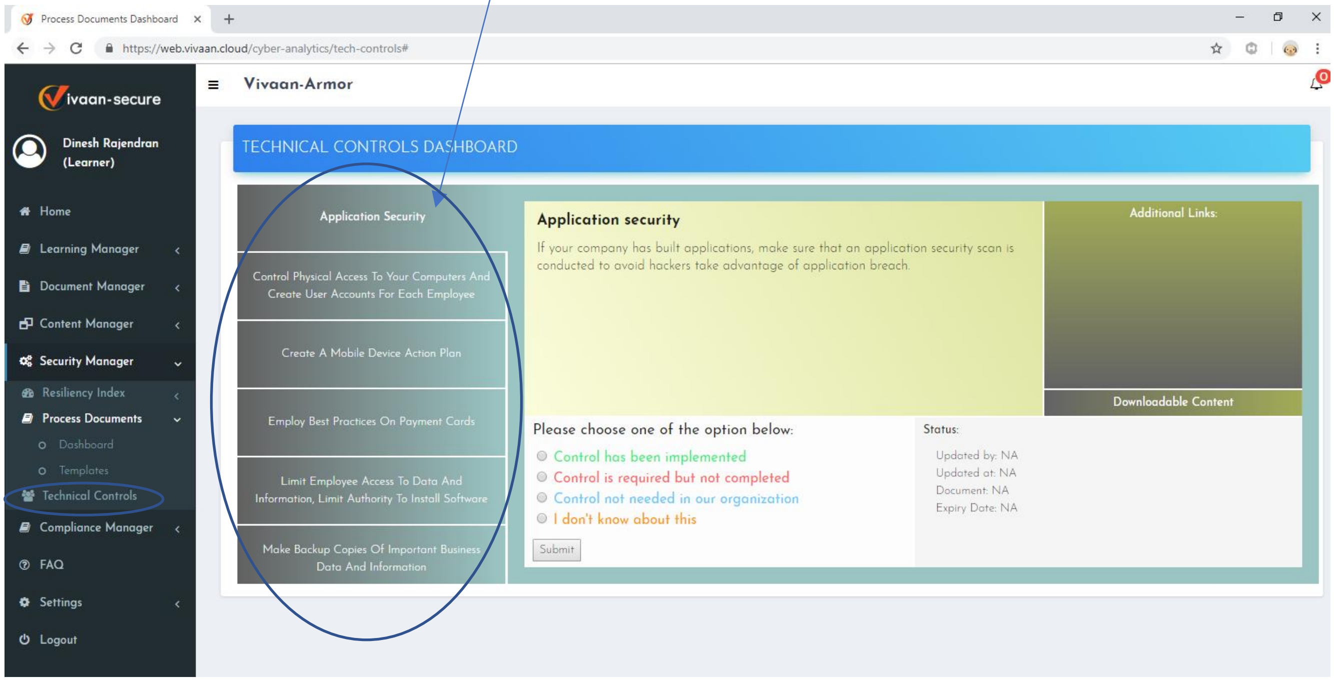
2 Periodically review the sections and update the same.

- System shows historical performance for you to check progress.
- Implement all the policies an controls needed over a period and update the portal.
- Let senior management see the Resiliency Index, Index and progress that the company is making

3 Complete the controls management section to the best extent. Use outside consultants/auditors to help if needed.

4 Adopting the polices, revisitingg the controls and monitoring the training will

22) Clicking on any of the policies in the grey box will populate the description of the policy as well as a question that the user needs to answer. This answer will be fetched automatically and used to calculate the technical index as described in step 14.



Process Documents Dashboard

https://web.vivaan.cloud/cyber-analytics/tech-controls#

Vivaan-secure

Dinesh Rajendran (Learner)

Vivaan-Armor

TECHNICAL CONTROLS DASHBOARD

Application Security

Control Physical Access To Your Computers And Create User Accounts For Each Employee

Create A Mobile Device Action Plan

Employ Best Practices On Payment Cards

Limit Employee Access To Data And Information, Limit Authority To Install Software

Make Backup Copies Of Important Business Data And Information

Application security

If your company has built applications, make sure that an application security scan is conducted to avoid hackers take advantage of application breach.

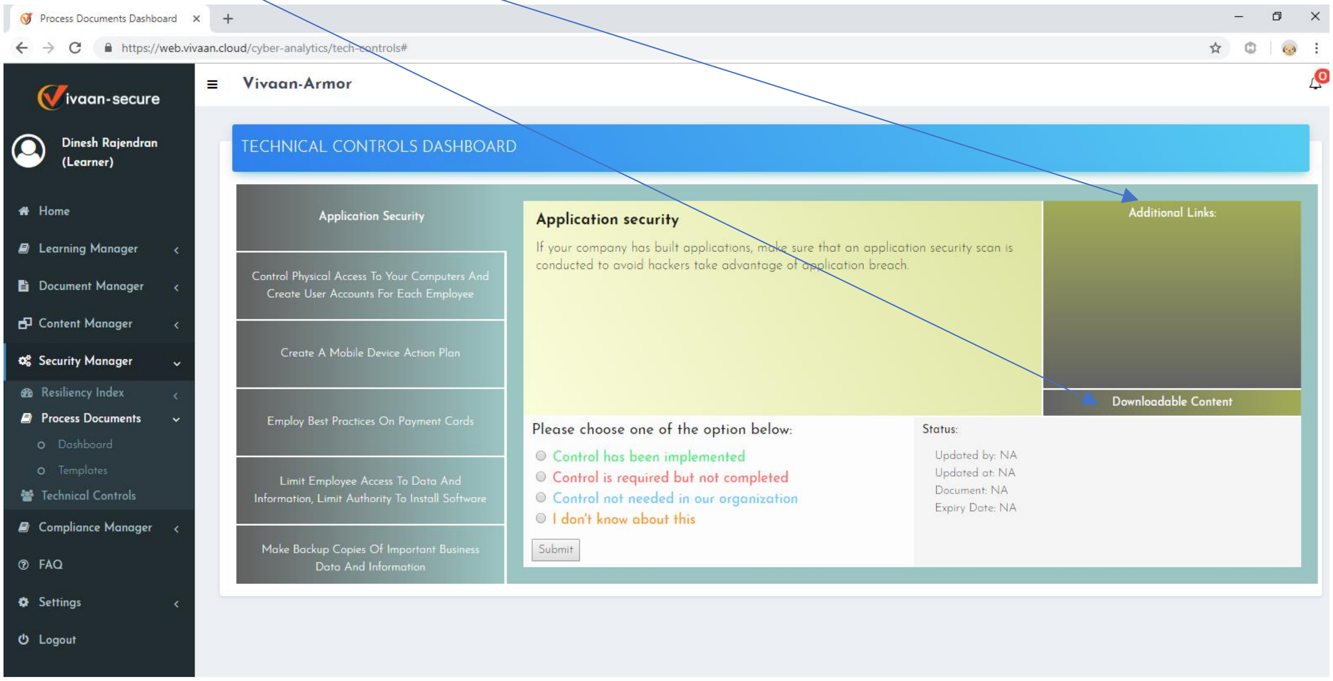
Please choose one of the option below:

○ Control has been implemented
○ Control is required but not completed
○ Control not needed in our organization
○ I don't know about this

Status:

Updated by: NA
Updated at: NA
Document: NA
Expiry Date: NA

Downloadable content and additional links may appear here.



Process Documents Dashboard

https://web.vivaan.cloud/cyber-analytics/tech-controls#

Vivaan-secure

Dinesh Rajendran (Learner)

Vivaan-Armor

TECHNICAL CONTROLS DASHBOARD

Application Security

Control Physical Access To Your Computers And Create User Accounts For Each Employee

Create A Mobile Device Action Plan

Employ Best Practices On Payment Cards

Limit Employee Access To Data And Information, Limit Authority To Install Software

Make Backup Copies Of Important Business Data And Information

Application security

If your company has built applications, make sure that an application security scan is conducted to avoid hackers take advantage of application breach.

Please choose one of the option below:

○ Control has been implemented
○ Control is required but not completed
○ Control not needed in our organization
○ I don't know about this

Status:

Updated by: NA
Updated at: NA
Document: NA
Expiry Date: NA

Conclusion: Vivaan-Armor Makes it easy to build and track your company's Cyber Resiliency. The portal allows companies to maintain its Information Security (IS) and Cybersecurity policy documents and technical controls (such as patch management, anti-virus software and firewall information etc.). A historical index of learning analytics, process readiness and control effectiveness are also tracked. The portal also offers various templates for policies that any company can modify and adapt for its own purpose.