Table of Contents

TPN+ Platform Process
Supporting TPN Service Provider Members

Completes onboard info

Completes TPN+ Profile
👁 Visible upon payment

Uploads non-TPN Security Certs eg: ISO, SOC2 Type2
👁 Visible upon payment
TPN spot checks non-TPN Certs

Completes TPN Questionnaire per Site or App

SELF-REPORTED
Valid for 1 year from publication

👁 TPN Blue Shield is visible and available for download

Completes TPN Membership Agreement

Pays TPN Annual Membership Fee

Payment unlocks TPN+ visibility and ability to perform a TPN Gold Assessment

GATE

Selects accredited TPN Assessor

👁 Company is visible in TPN+ Registry & to Content Owners

Collaboration between Service Provider and TPN Assessor

Pre-assessment Phase per Site or App

Assessment Phase per Site or App

TPN performs final QC

PUBLISH

ASSESSED
Valid for 2 years from publication

Self-serve Remediation

Content Owners are able to flag priority remediation items

👁 TPN assessment report is published

Legend
👁 Content Owner Visibility
🟠 TPN Team
🔵 Service Provider
⚫ 3rd party TPN Assessor

Content Owner Visibility

Note: Visibility to Content Owners is enabled only after Service Provider has paid their TPN membership fee

Content Owner TPN+ visibility as follows:

- ✓ Dashboard Metrics
- ✓ Company & Application Registries
- ✓ Service Provider Profile
- ✓ Completed Self-Reported Site or App TPN Questionnaire
- ✓ Final 3rd party Assessed Site or App TPN Assessment
- ✓ Final TPN Assessment Report
- ✓ Assessor Findings
- ✓ Remediation Items & Updates
- ✓ In-platform "comments" with Service Providers & TPN

Content Owner functionality:

- ✓ Ability to download watermarked TPN Assessment Reports
- ✓ Ability to flag priority remediation items (Gold members only)

Content Owner does not have visibility of:

- X Service Provider TPN membership tier or annual gross revenue
- X In-platform "comments" between Service Providers & Assessors
- X Uploaded evidence

TPN+ Platform Process
Supporting TPN Service Provider Members
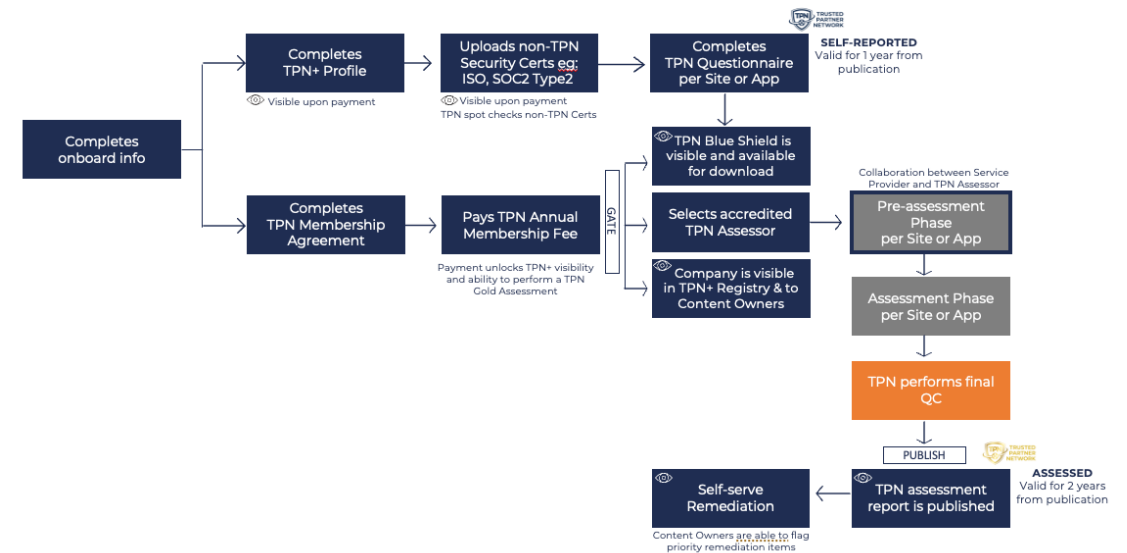
Account Signup & Creation

TPN+ TRUSTED PARTNER NETWORK

Welcome To The Trusted Partner Network

Email

Enter your Email

Password

Enter your Password 👁

Sign in

Forgot your password?

Are you a new Service Provider?   If you are a new Content owner or Assessor

SIGN UP NOW   **CLICK HERE**

❓ **NEED SUPPORT?**

Copyright © Trusted Partner Network 2023.

As a returning user, click Login and enter your credentials to login to TPN+

To join TPN as a new Service Provider, click here to create your user and company account

If you are a new Content Owner or Assessor and would like to join TPN click here.

Welcome To The Trusted Partner Network

Complete the signup process below

Service Provider Signup

First Name
Last Name

Email
Phone

Password

Confirm Password

Create Account

Copyright © Trusted Partner Network 2023.

Not a Service Provider?   BACK

Already a user? Login

The first step in creating a new account is providing your details to create your user account

You must provide:
- First and Last Name
- Business e-mail address
- Phone number
- Desired password
  - Minimum length - 12 characters
  - Minimum of 3 of the following:
    Uppercase
    Lowercase
    Numeric or Special Characters

Microsoft Authenticator Setup

1. Download Microsoft Authenticator via link on Slide 9
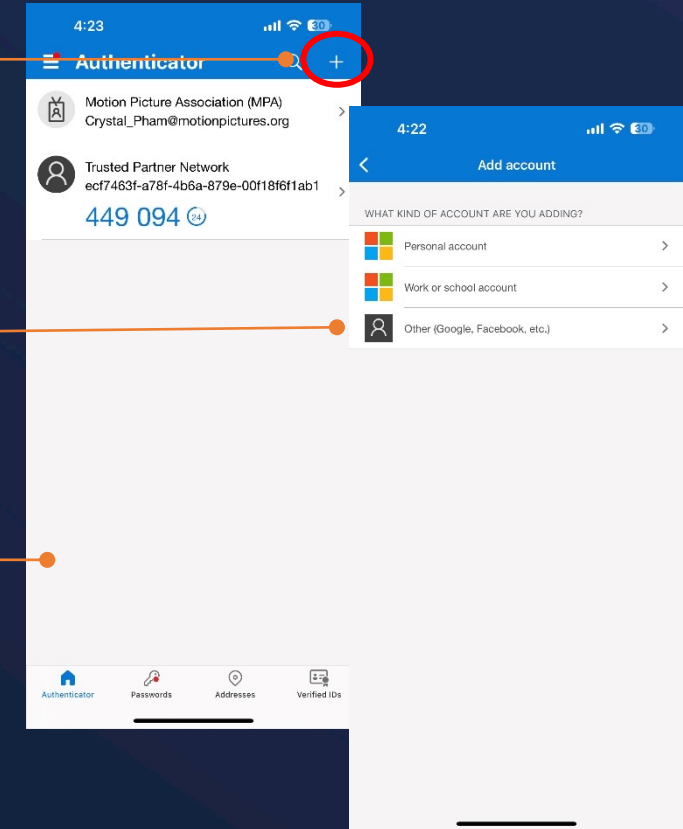
2. Open Application

3. Click "+" symbol in upper right corner

- Select Other (Google, Facebook)
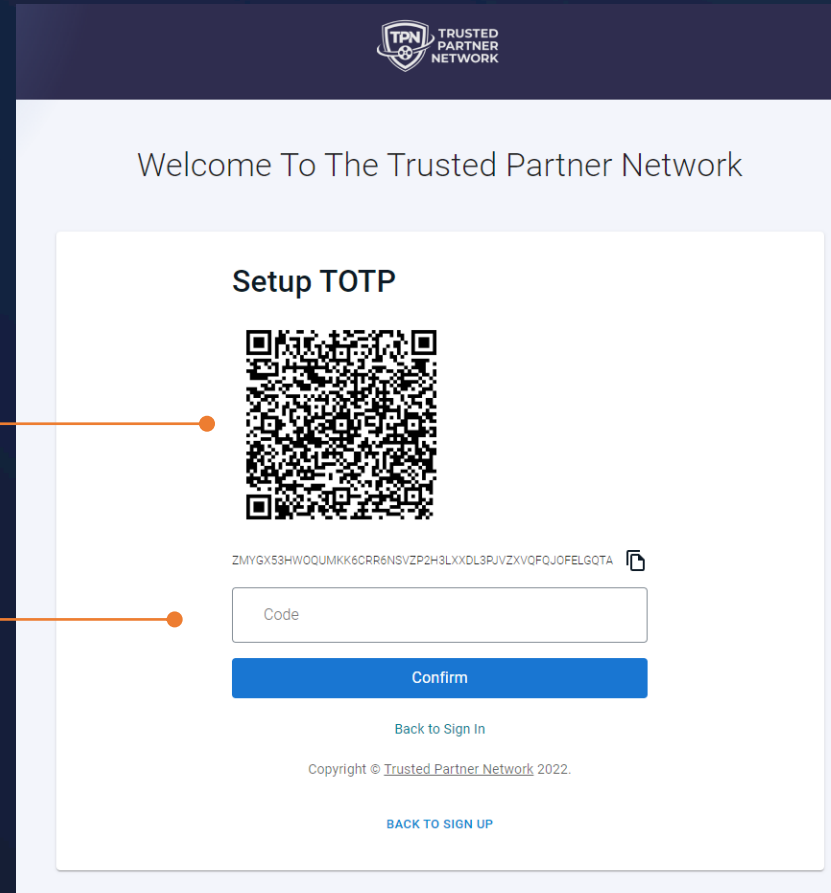
4. Point your camera at the QR code

5. Your new account should appear in your Authenticator app

6. Use the one-time code to sign in to the TPN+ Platform

Welcome To The Trusted Partner Network

Setup TOTP

ZMYGX53HWOQUMKK6CRR6NSVZP2H3LXXDL3PJVZXVQFQJOFELGQTA

Code

Confirm

Back to Sign In

Copyright © Trusted Partner Network 2022.

BACK TO SIGN UP

Once you have Microsoft Authenticator installed on your smartphone, using the camera on your phone, you can scan the QR code on the screen to pair the authenticator to your TPN+ user account and receive your two-factor authentication (2FA) number.

Enter the 6-digit number that appears in your Microsoft Authenticator app and press confirm to validate your secure login session.

TPN+ requires two-factor authentication (2FA). TPN+ only supports Microsoft Authenticator for 2FA validation.

Microsoft Authenticator

Links to Microsoft Authenticator

iPhone

Android

Important: You will need to open the Microsoft Authenticator app on your smartphone every time you log in. You will not receive a notification or text.

Search Companies

After successfully authenticating, you will be brought to this page to search for your Company.

If your Company is listed and you select it, a request will be sent to your Company's administrator to add you as a user.

If the Company doesn't exist, choose **Add New Company** and you will be taken to a screen to create the Company in the system

Request Access To Existing Company

Welcome To The Trusted Partner Network

Complete the signup process below

Join TMT Insights ✕

By clicking join, a request will be sent to an admin of TMT Insights to allow you to join. Are you sure you want to do this?

CANCEL   JOIN

Copyright © Trusted Partner Network 2023.

If you find your Company, select it and click the **Join** button. The primary admin of your Company will then grant permission for you to access the system.

TPN+ TRUSTED PARTNER NETWORK

Your request has been submitted to an admin for TMT Insights. You will be granted access upon approval.

Initial Company Setup

TPN+ TRUSTED PARTNER NETWORK

Welcome To The Trusted Partner Network

Complete the signup process below

Create a new Company

Business Name *
AES

Website Domain

Billing PO Number

VAT Number

Gross Revenue *
Self-Employed

Employee Count *
1 person only with no other employees

Primary Contact

Address *

Address 2

Address 3

Country

State / Province

City

Postal Code *

Phone Number *
+1

Billing Contact

☐ Same as primary contact

To create a new Company, add all requested information.

All fields with * are required to continue.

If your billing contact and information are different from your Company information - unselecting this checkbox will provide additional fields of data to complete.

The gross revenue selection is tied directly to the TPN Membership levels.

Please report accurately to reflect the membership level reported in the TPN membership agreement and in accordance with the terms of the agreement.

If you are a parent Company and owner of **subsidiary companies** who will have their own TPN+ Company accounts please click "**NEED SUPPORT**" in the navigation pane for TPN Admin to assist with linking the accounts.

Initial Company Setup

Membership Agreement

After you have created your Company and completed the sign-up process, you will be prompted to sign the TPN membership agreement via DocuSign and you will receive an email from DocuSign for signature.

If someone else in your organization should be the signatory you can reassign to them in the "Other Actions" menu in the top right corner of DocuSign.

Please update the required fields and sign. TPN will then be prompted to sign, and upon completion you will receive a copy of the signed agreement via DocuSign email.

Completion of the agreement will trigger the invoice process.

Service Provider: Adding & Managing Users

Granting User Access

As your Company's user admin, you will be notified of any users who have requested accounts for your company.

You can **Approve** or **Reject** their requests here granting or denying access to the system.

Adding and Managing Users

An existing list of users will display once the Users section has been expanded

Clicking the **+ USER** button allows you to add new users

Clicking the User Settings icon will display a dropdown that allows for resending the email invite or resetting the user's password

Clicking the trash or pencil icons provide the ability to delete or edit the user account

This toggle is used to enable Admin privileges for your Company's user.

Only a User Admin can enable or revoke admin privileges for other users. Only User Admins receive TPN+ notifications (eg: assessment published).

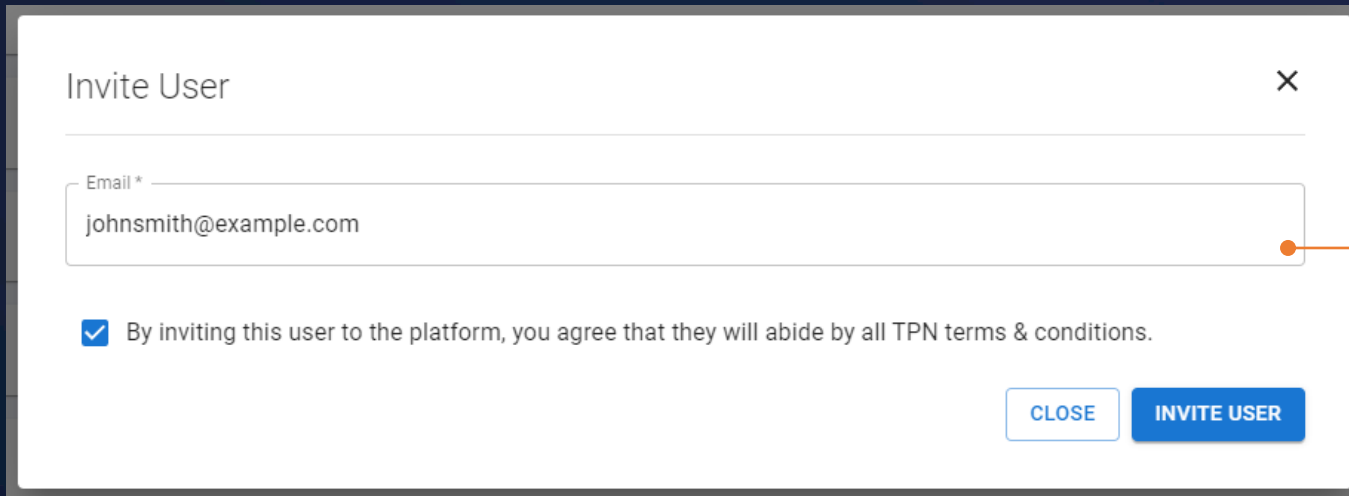This toggle is used to identify a user as a Consultant.

Users (6)

+ USER

Email	First	Last	Last Login	Admin	Consultant	
niemeyerbilly+123@gmail.com			N/A			⋮
ryan+vendor@giantsource.com	Gina	Gajewski	05/15/2023 4:02:36 pm			⋮
kyle+qavendor@giantsource.com	Melody	Giambastiani	07/07/2023 4:59:11 am			

Edit

Delete

Resend Invite

Reset

Adding and Managing Users

Invite User

Email *

johnsmith@example.com

☑ By inviting this user to the platform, you agree that they will abide by all TPN terms & conditions.

CLOSE   **INVITE USER**

When adding a new user, and clicking the **Invite User** button, an invitation will be sent to the email address you provide on this screen. The email address will be used to register the new user and will be pre-associated with your Company account.

Please note: only enter one email address at a time

Adding and Managing Users

An email will then be sent to the user from membership@ttpn.org with their temporary password

Trusted Partner Network - Welcome to TPN+!

M   ○ membership@ttpn.org <membership@ttpn.org>
To: 🕐 Giambastiani, Melody

Hello,

Welcome to the Trusted Partner Network (TPN+) Platform! For your convenience, please use this LINK to the TPN+ how-to guide for more detailed instructions.

Please use the username and temporary password below to login to TPN+ HERE and set up your TPN+ Platform account.

The user can then log in to the system by clicking on this hyperlink and using their temporary password

Adding and Managing Users

You can now log in to the system by using your email and temporary password sent to you in the welcome email.

Service Provider: Profile Overview

Service Provider Profile

Your Profile is the landing page that upon login allows you to set up and manage your **Users** as well as update your **Company Details.**
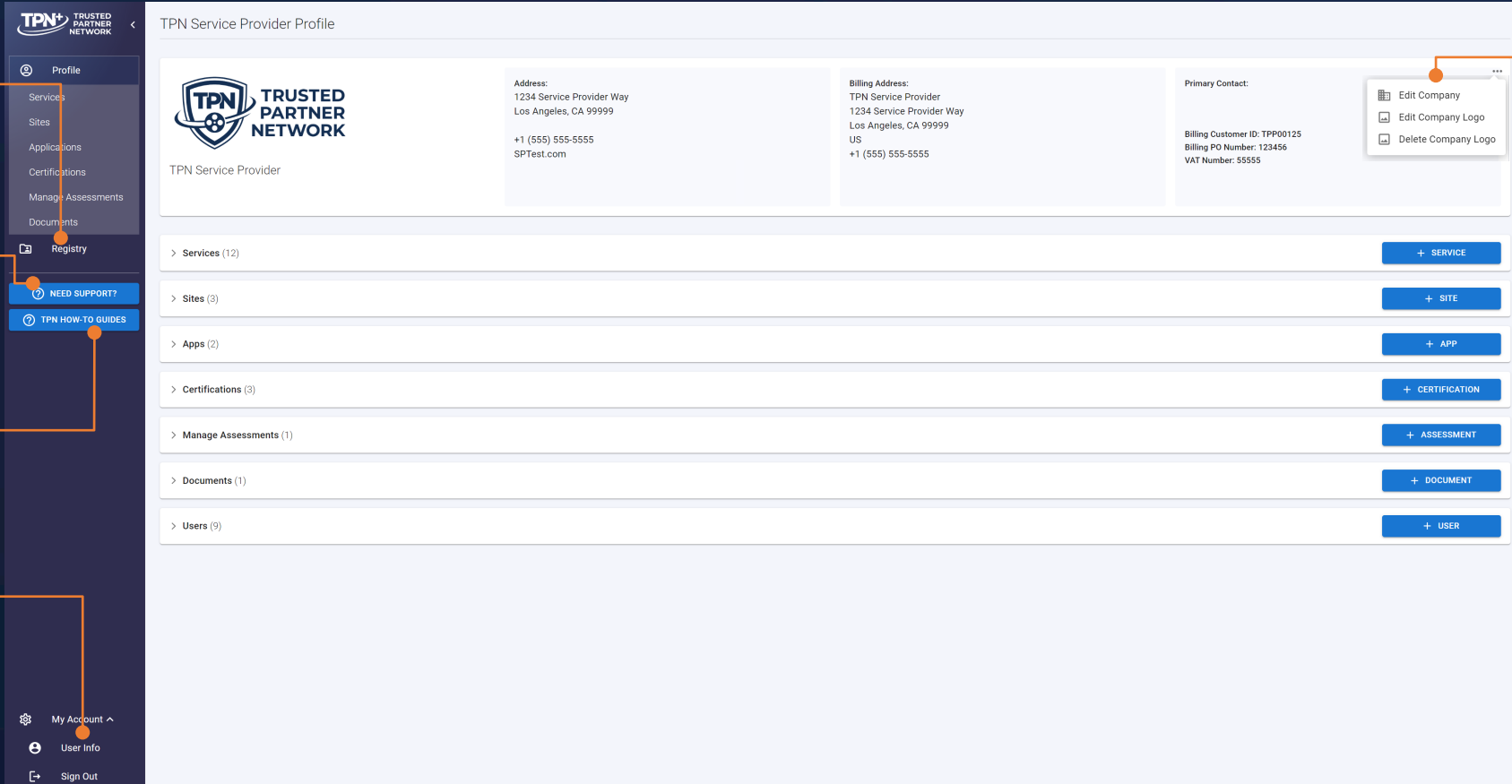
Registry: view list of all Service Providers and their shield status

Need Support: create support tickets for assistance from TPN Support Team

How-To Guides: view support guides for Assessors and Service Providers

User Info: change or update your individual account details

Company Details: change or update address, primary contact information, or logo

---

TPN Service Provider Profile

TRUSTED PARTNER NETWORK

TPN Service Provider

Address:
1234 Service Provider Way
Los Angeles, CA 99999

+1 (555) 555-5555
SPTest.com

Billing Address:
TPN Service Provider
1234 Service Provider Way
Los Angeles, CA 99999
US
+1 (555) 555-5555

Primary Contact:

Billing Customer ID: TPP00125
Billing PO Number: 123456
VAT Number: 55555

Edit Company
Edit Company Logo
Delete Company Logo

- Profile
- Services
- Sites
- Applications
- Certifications
- Manage Assessments
- Documents
- Registry

NEED SUPPORT?
TPN HOW-TO GUIDES

My Account
User Info
Sign Out

- Services (12)   + SERVICE
- Sites (3)   + SITE
- Apps (2)   + APP
- Certifications (3)   + CERTIFICATION
- Manage Assessments (1) + ASSESSMENT
- Documents (1)   + DOCUMENT
- Users (9)   + USER

Service Provider Profile Continued

Your Profile also allows you to set up and manage your **Services, Sites, Applications, Documents, non-TPN Certifications,** and **Users** and manage ongoing **Assessments.**

- **Services:** Types of services provided

- **Sites:** Service Provider's physical locations where services are performed

- **Apps:** In-house developed or 3rd party application software used to provide services

- **Certifications:** non-TPN security certifications (ISO27001, AICPA Soc2 Type 2, CSA STAR Level 1 & 2)

- **Manage Assessments**: This is where you will be able to manage your TPN+ assessments

- **Documents:** Legacy TPN and other assessments; white papers; process maps

- **Users:** Add and manage Users

Adding Services

Services (3)

+ SERVICE

Service	Category
Color	A/V Post
DCP Replication	Digital Cinema
Animation	Visual Effects (VFX)

Clicking the **+ SERVICE** button allows you to add and manage which **Services** you currently provide.

Adding Services

Visual Effects (VFX)

Edit Services   ✕

- ☑ A/V Post   ☐ Content Transfer Networks   ☐ Data Center

- ☑ Digital Cinema   ☐ Film Lab   ☐ Home Entertainment

- ☐ Localization   ☐ Marketing   ☐ Non-Theatrical

- ☐ On-Set Production   ☐ Onboard   ☐ Screening Room

- ☐ Transportation & Storage   ☐ Video Game Services   ☑ Visual Effects (VFX)

CLOSE   SET SERVICE CATEGORIES

Upon clicking **+ Service** a new window will appear prompting you to select one or more service categories.

After choosing the various service categories click the **Set Service Categories** button to further define more detailed services for each Service Category.

Adding Services

Visual Effects (VFX)

Edit Services ✕

A/V Post

Digital Intermediate (DI) ⊗   Color ⊗ ▾

Digital Cinema

DCP Replication ⊗   Digital Cinema Mastering ⊗ ▾

Visual Effects (VFX)

3D Effects ⊗   Rotoscoping ⊗ ▾

CLOSE   **SAVE SERVICES**

Each of your selected high level service categories are now displayed as separate groupings. Clicking on the dropdowns will provide a list of more detailed services to add to each high-level service category.

After selecting the detailed service selections for each high-level category, click **Save Services** to return to the profile page where the selected services will now be displayed. Please note you must select at least one Service inside of each Service Category selected.

Adding Sites

Clicking the **+ SITE** button allows you to add and manage the Physical location of each site and identify which services are performed at that location.

Shield	Name	Applications	Services	Status	Actions	
[TPN]	ⓘ Blue Shield - London	Custom TPN Application	Music Composition Music Editing Music Recording	Self-Reporting Complete	Ⓑ VIEW QUESTIONNAIRE	

Sites (3)

The Shield area of the Site listing will populate the most advanced stage of recognition for that Site.

The three display stages are:

1. Non-TPN certificate if this is the only security status reported.

2. Blue TPN Shield upon completion of the self-reported TPN Best Practice questionnaire.

3. Gold TPN Shield upon publication of a TPN assessment by an accredited TPN Assessor.

This **Action** button will change based on the different phases the Site is currently in.

The next step after creating the Site will be completion of a short Baseline Questionnaire. This baseline information will be used to filter the Best Practice questions you need to answer when you start to complete the TPN Best Practice Questionnaire.

Adding Sites

Location Name is where you can create a familiar name for your Site as opposed to just the address to help easily distinguish and identify.

This dropdown allows you to associate the various **Services** performed at this location. These services must already be selected in the **Services** section of the profile in order to appear here.

Upon clicking **+Site** you will be asked to provide information related to the location of the Site you are adding.

The creation of a Site is the first step in completing the Best Practice Questionnaire and initiating an assessment.

Primary Contact is selectable from a list of users invited by the administrator to the account under the **USERS** section of the company profile.

When complete, click **Add Site**.

Add New Site ✕

Location Name *
Burbank Facility

Address *

Country ▼   State / Province ▼

City ▼   Postal Code *

Phone Number *
🇺🇸 +1   Primary Contact ▼

Services
▲

Color
Digital Intermediate (DI)
DCP Replication
Digital Cinema Mastering
3D Effects
Rotoscoping

CLOSE   ADD SITE >

Best
Practices
Version
5.0:
3/67

Adding Applications – Overview

The **Applications** that you add to your profile are either **In-house Developed** or **3rd Party Applications**.

Note you can only respond to the TPN Best Practice questionnaire for **In-House Developed Applications**.

Apps (0)   + APP

In-house Developed Application

Shield	Name	Sites	Services	

3rd Party Licensed Application

Shield	Name	Version	Sites	Services	Hardening Guidelines	

Versions

Shield	Version	Hardening Guidelines	Status	Actions
📋	1		Pending	BEGIN APPLICATION BASELINE
📋	2		Pending	BEGIN APPLICATION BASELINE
(TPN)	3	3 TPN In-house App hardening guidelines	Self-Reporting Complete	ⓑ SCHEDULE ASSESSMENT / VIEW QUESTIONNAIRE
	4		Pending	ⓑ BEGIN TPN BEST PRACTICES QUESTIONNAIRE

Just like Sites, the process to begin the TPN Best Practice questionnaire and Assessments follows the same workflow.

Adding Applications – Overview

The **Shield** column will populate the current TPN Shield status for the Application. If you have added a 3ʳᵈ party Licensed Application that is a TPN member, your profile will display the associated TPN Shield status.

This **Actions** column will reflect the different actions related to the Application.

For example: Begin Baseline Questionnaire, Begin Best Practices Questionnaire, Continue Questionnaire, etc.

Versions

Shield	Version	Hardening Guidelines	Status	Actions
	1		Pending	BEGIN APPLICATION BASELINE
	2		Pending	BEGIN APPLICATION BASELINE
TPN	3	3 TPN In-house App hardening guidelines	Self-Reporting Complete	SCHEDULE ASSESSMENT / VIEW QUESTIONNAIRE
	4		Pending	BEGIN TPN BEST PRACTICES QUESTIONNAIRE

In the **Versions** drop-down, you will see the various versions of the App, one per row.

If you have uploaded Hardening Guidelines (per Version), they will be displayed in the **Hardening Guidelines** column and are downloadable by Content Owners and by the Assessor selected to perform the App Assessment.

This **Status** column will change based on the different phases the Application is currently in.

If the Best Practices Questionnaire is in progress, for example, it will show how many questions have been answered.

Adding Applications - Overview

You can add and manage both **In-house Developed** Applications and also **3rd-party Licensed** Applications (eg: SaaS, PaaS, etc.) to your TPN+ Profile

∨ **Apps** (0)   [**+ APP**]

In-house Developed Application			
Shield	Name	Sites	Services

3rd Party Licensed Application					
Shield	Name	Version	Sites	Services	Hardening Guidelines

Clicking the **+ APP** button allows you to add and manage your in-house developed and 3rd-party Licensed Applications.

You can add new Applications or select pre-registered Applications from the TPN+ Registry.

Both in-house and 3rd party Apps will require you to select the Application type (eg: cloud services, transfer services etc.) and the versions that you provide or are licensing.

In-house developed apps will also indicate whether the app is licensable and/or used "as a service".

You will also identify which Service and Site is using that Application and Version if applicable.

Adding Applications

To add Applications that were developed in-house by
your Company, please click **+ In-House Developed Application** to add it to the TPN+ registry

To add a licensed Application, please click **+ 3rd Party Licensed Application** and either select the Application from the TPN+ registry, or if it is new to TPN+, please add it to the TPN+ registry.

Add Application ✕

Would you like to create a new in-house application developed by you or add a licensed application?

An "in-house developed application" is developed and owned by your business. If you would like to add a version to your existing in-house developed application please close this box and choose the edit icon for the desired application in your profile.

A 3rd-Party Licensed Application application is developed by a 3rd party and licensed by your company for use. Prior to adding a new licensed application, please first check the TPN+ directory to select it if available. If it is not available, please add it to the TPN+ directory.

    + IN-HOUSE DEVELOPED APPLICATION

    + 3RD PARTY LICENSED APPLICATION

Adding In-house Developed Applications

First, provide the **Application Name**, then select from the **Application Types** dropdown.

Add a **brief description** of your Application. Please be aware that this will be visible to Content Owners and other Service Providers if it is licensable.

Select the **Application Type** from the dropdown list. You can make multiple selections here.

If you do not see the Application Type you need, please contact support@ttpn.org.

Create New Application ✕

Please provide the following details about your in-house developed application.

Application Name *

Application Types*

Cloud Services

Digital Supply Chain

Editing Software

Transfer Services

Description

Please be aware that this description will be visible to Content Owners and

Indicate any/all deployed versions of the application.

Is your application available "As a Service"? Please note that "As a Service" is considered a version.   ◯ Yes   ⦿ No

Type below and hit ⎾ENTER⏌ to add a version or versions

Versions*

Is this application licensable to other Service Providers?   Yes   No
Please note that "Licensable Apps" will be visible for other Service Providers to select   ⦿   ◯
when filling out this form.

List any 3rd party application integrations (eg: API integration to your customized app) by searching the TPN+ directory or adding new.

＋ Add New

Indicate which Site locations operate or host this application. (i.e. do not include cloud instances)

Sites ▼

Services* ▼

‹ BACK   CANCEL   **CREATE APPLICATION**

Adding In-house Developed Applications

If your Application is available as a service, click **Yes**. "**As a Service**" will then appear in the **Versions** list.

Please add all other available Application **Versions**.

Note that you must hit ENTER to add a version.

Click **Yes** if your Application is licensable to other Companies. Note that it will then be available to other TPN member Service Providers to select in their TPN profile as their licensed Application.

If your Application is integrated with any other 3rd-party Applications, click **Add New** and search in the TPN+ registry or add a new Application. *See the next slide for instructions.*

Use these dropdowns to list which of your **Sites** and **Services** use this Application.

Create New Application

Please provide the following details about your in-house developed application.

Application Name *

Application Types*

- Cloud Services
- Digital Supply Chain
- Editing Software
- Transfer Services

Description

Please be aware that this description will be visible to Content Owners and

Indicate any/all deployed versions of the application.

Is your application available "As a Service"? Please note that "As a Service" is considered a version.   ○ Yes   ● No

Type below and hit ENTER to add a version or versions

Versions*

Is this application licensable to other Service Providers?   Yes ●   No ○
Please note that "Licensable Apps" will be visible for other Service Providers to select when filling out this form.

List any 3rd party application integrations (eg: API integration to your customized app) by searching the TPN+ directory or adding new.
+ Add New

Indicate which Site locations operate or host this application. (i.e. do not include cloud instances)

Sites

Services*

BACK   CANCEL   CREATE APPLICATION

Adding In-house Developed Applications – 3rd Party Integrations

After clicking **Add New** you will search in the TPN+ registry or add a new Application.

If you are selecting your 3rd party integrated Application from the TPN+ Registry, the **Company** and **Application** boxes will assist your search of the TPN+ Registry. Once the Company and Application are selected, please **select version/s** and **save** to list in your Application profile.

If the **version** you are using does not already exist in the TPN+ Registry, please click **+Add New Version** and TPN will contact the Application Owner to verify and add the requested version. TPN will advise you when available for your selection.

To add a new Application to the TPN+ Registry, please click **Add It To Our Directory,** add the Company and Application name and type, and Version/s and click Save. You may then select the new Application and save to your Profile.

Search the TPN+ Registry & Add 3rd party Applications ✕

Search the directory to find 3rd party applications. You can search by the name of the company (e.g. Adobe), or the application itself (e.g. Premiere).

★ This star denotes a TPN+ member Company

Company	Application	Application Types ▾
Company	Application	+

Melody SP3	Melody Application	Select Version ▲
		4 + ADD
		+ Add New Version
★ Melody Service Provider	Melody standalone app 1	
★ Melody Service Provider	Melody standalone app 2	Select Version ▾
★ Melody Service Provider	Melody standalone app 3	Select Version ▾
Davids VFX	My App	Select Version ▾

|◄ ◄ 1 2 3 **4** 5 … 8 ► ►|

Selected Applications:

None

CANCEL SAVE

Add new 3rd Party Licensed Application ✕

Company Name * 🔍	Application Name *	Application Types* ▾

Indicate any/all deployed versions of the application.

Is your application available "As a Service"? Please note that "As a Service" is considered a version.   ○ Yes   ● No

Type below and hit ⌷ENTER⌷ to add a version or versions

Versions*

CANCEL SAVE

Adding In-house Developed Applications

Congratulations on adding your new in-house developed application ✕

You can now edit your application and hardening guidelines.

CLOSE

After you have saved your In-house Developed App, you will see this confirmation message.

To add **Hardening Guidelines**, see next slides.

Adding In-house Developed Applications – Hardening Guidelines & Edits

In-house Developed Application

Shield	Name	Sites	Services	
📑	Cloud Services App	Blade House Melody Ruby Lane Melody Main Street	Dubbing Subtitling/Captioning	✏️

> Versions

To add **Hardening Guidelines**, **add a new Version** or **make other changes** to your Application, first click this pencil icon to Edit.

Indicate any/all deployed versions of the application.

Is your application available "As a Service"? Please note that "As a Service" is considered a version.   ⦿ Yes   ◯ No

Type below and hit ⎵ENTER⎵ to add a version or versions

Versions*
| 4.5 | As a Service |

Hardening Guidelines

[+ Add New]

In the Edit screen, you can make edits or click **Add New** to upload **Hardening Guidelines**.

Add new Hardening Guidelines to TPN Cloud Services App   ✕

Hardening Guidelines Name *
TPN Cloud Services App Hardening Guidelines

Version
4.5

Maximum File size is 50MB

Upload or Drop file here

Preview	Name	User	Uploaded	-
📄	Hardening Guidelines Test Doc.docx	Melody Giambastiani	07/07/2023 05:26	🗑️

CANCEL   UPLOAD

Enter the **name** and **version** of the Hardening Guidelines, upload the file by clicking to upload or drag and drop the file here.

Once the **Hardening Guidelines** file shows here, click **Upload** then **Save Application**.

Note that **Content Owners** and any **Service Provider** who has listed your licensable Application in their own TPN+ profile will be able to **download** the Hardening Guidelines

Adding 3rd Party Licensed Apps

Add Application

Would you like to create a new in-house application developed by you or add a licensed application?

An "in-house developed application" is developed and owned by your business. If you would like to add a version to your existing in-house developed application please close this box and choose the edit icon for the desired application in your profile.

A 3rd-Party Licensed Application application is developed by a 3rd party and licensed by your company for use. Prior to adding a new licensed application, please first check the TPN+ directory to select it if available. If it is not available, please add it to the TPN+ directory.

+ IN-HOUSE DEVELOPED APPLICATION

+ 3RD PARTY LICENSED APPLICATION

⭐ This star denotes a TPN member Company

A blue star next to the Company name means it is a TPN Member who has either self-reported their security status or been assessed on TPN+. The TPN Blue or Gold Shield will be displayed in your TPN+ profile if you select this one of these Applications.

To add licensed **Applications**, you will first search by **Company**, **Application** and/or **Application Types** in the existing TPN+ registry.

Once located and selected, please also select the **Version** that you are using. You cannot **Save** until you have done this.

See next slide for more instructions regarding Versions.

Search the TPN+ Registry & Add 3rd party Applications

Search the directory to find 3rd party applications. You can search by the name of the company (e.g. Adobe), or the application itself (e.g. Premiere).

⭐ This star denotes a TPN member Company

Company	Application	Application Types
Company	Application	+

⭐ Crystal Test June 2023	melody	Select Version
⭐ Crystal Test June 2023	Melody	Select Version
⭐ Melody Service Provider	Melody App	Select Version
Melody SP3	Melody Application	Select Version
⭐ Melody Service Provider	Melody standalone app 1	Select Version

|< < 1 ... 6 7 8 ... 13 > >|

< BACK   **CANCEL**

Adding 3rd Party Licensed Apps

You will select the Version of the App here or click **+Request New Version** to add a version not yet in the TPN+ registry.

If a New Version is requested for an owned Application (with Blue Star), TPN will contact the App Owner to verify and add the requested version and will let you know when it is available for you to select.

Use these drop downs to list where you use this App and for which Services.

If you are adding more than one Version, you will have to repeat this for each Version. (Go back to **+ 3rd Party Licensed Application**.)

Search the TPN+ Registry & Add Licensed Applications

Search the directory to find licensed applications. You can search by the name of the company (e.g. Adobe), or the application itself (e.g. Premiere).

- Company: TMT
- Application
- Application Types
- Company
- Application

★ TMT Insights — testing custom — Select Version

1	+ ADD
2	+ ADD
3	+ ADD
+ Request New Version	

Not finding the application you are looking for? ADD IT TO OU...

Selected Applications:

None

BACK CANCEL SAVE

Search the TPN+ Registry & Add 3rd party Applications

Search the directory to find 3rd party applications. You can search by the name of the company (e.g. Adobe), or the application itself (e.g. Premiere).
★ This star denotes a TPN member Company

- Company
- Application
- Application Types
- Company
- Application

New Version Requested

TPN has been notified of your request for:
Crystal Test Adobe: Version 4

CLOSE

| Non-member | App name | Select Version |
| Non-member | App Name | Select Version |

BACK CANCEL

Sites and Services for TMT Insights testing custom 1

Indicate which Site locations operate or host this application. (i.e. do not include cloud instances)

- Sites
- Services

CANCEL SAVE APPLICATION

Note – if you already added Apps before the TPN Release V1.1.0 (7/13/23) you will now need to add Versions

Clicking the pencil button allows you edit an app that you had previously added to TPN+ (prior to the TPN Release v1.1.0 7/13/23).

If you already obtained a Blue or Gold Shield for your in-house developed app, you will be prompted to indicate the version that was self-reported and/or assessed.

The version you select will inherit the Status and Actions you have completed.

Adding Certifications

Non-TPN Certifications accepted:
ISO 27001: 2013 & 2022, AICPA Soc2 Type 2, CSA STAR Level 1 & 2, and TPN Legacy Certificates

Clicking the **+ CERTIFICATION** allows you to upload an accepted non-TPN certificate or a legacy TPN certificate by selecting the control framework from the drop-down list and linking it to the applicable previously registered Site and Application.

Clicking the **Link** button allows you to download the document from the profile.

Clicking the **Trash Can** button will delete the file from the profile.

Adding Certifications

Choose from a list of accepted certifications to upload the evidence against.

Drag the file from your computer or click on the box to bring up a file browser to find the file on your computer.

Provide the start and date of the certificate you uploaded.

Certificates that are not valid will be rejected by TPN.

Select the list of Sites and Applications for which the uploaded certificate or TPN legacy assessment applies.

Remember those Sites and Apps must be selected in your profile prior to making this association.

Certification Upload

Certification
ISO 27002-2022: 2022

Maximum File size is 50MB

Upload or Drop file here

Preview	Name	User	Uploaded	-
📄	ISO_27001_Certificate.png	Melody Giambastiani	07/12/2023 07:23	🗑

Start Date
04/03/2023

End Date
04/03/2026

Sites

Applications

CLOSE   UPLOAD CERTIFICATION

Adding Documents

You may use Documents to upload your TPN legacy assessment and remediation PDFs along with any other document type that will be useful for Content Owners to understand your security status.

Clicking the **+ DOCUMENT** button allows you to upload a new document.

Documents (1)		+ DOCUMENT
Document	Upload Date	
2021 TPN Assessment - Los Angeles	12/28/2022	

Clicking the **Link** button allows you to download the document from the profile.

Clicking the **Trash Can** button will delete the file from the priofile.

Please be advised that documents uploaded to this section, including your Legacy TPN Assessment Reports, will not be watermarked upon user download - this includes Content Owners. **If you require watermarking, please direct Content Owners to the TPN Box account.**

Adding Documents

Upload Document

Description *

2022 TPN Assessment

Maximum File size is 50MB

Upload or Drop file here

Preview	Name	User	Uploaded	-
📄	TPN Assessment.docx	Melody Giambastiani	07/12/2023 07:28	🗑

Please be advised that documents uploaded to this section, including your Legacy TPN Assessment Reports, will not be watermarked upon user download--this includes Content Owners. If you require watermarking, please direct Content Owners to the TPN Box account.

UPLOAD

Enter the name of the document to be uploaded

Drag your file from your computer or click on the box to bring up a file browser to find the file on your computer

A summary of the documents you have prepared for upload will display here

Note that if you have dragged or selected multiple documents to be uploaded, all files will display here

Click the upload button to begin uploading the document(s)

Service Provider:
Answering TPN Best Practices Questionnaire

Baseline Questionnaire

ⓘ Paris Facility	-	Animation	Pending	BEGIN SITE BASELINE	✏️ 🗑️

Once a new Site or App is created, you will be prompted to complete a Baseline Questionnaire.

Site Service Provider Baseline BACK TO COMPANY DETAILS

Site Service Provider Baseline ⋯

BA-1.0 Site Baseline

Number of Employees ☐

Content Types ☐

Select the types of content you handle:

- ☑ Full-length
- ☐ Partial-length
- ☐ Does not handle content

SAVE AND CONTINUE ›

Workflow Timeframes ☐

Work From Home/Remote ☐

The responses in the Baseline Questionnaire are used to scope the questions in the TPN Best Practice Questionnaire.

TPN Best Practices Process Overview

In the top right-hand corner of the TPN Best Practice questionnaire screen you are able to click down and see this progress list as your Site or Application moves through the TPN+ platform to Blue or Gold Shield status including remediation management.

The assigned Assessor has accepted the request

The Assessor has officially begun the assessment

TPN approved the assessment and the **TPN Gold Shield** awarded

---

Current Step: Assessment In Remediation   ⌃

Site/App Baseline In Progress

⌄

Site/App Baseline Complete

⌄

Best Practices Questionnaire In Progress

⌄

Self-Reporting Complete   TPN TRUSTED PARTNER NETWORK

⌄

Assessment Assigned

⌄

Pre-Assessment In Progress

⌄

Assessment In Progress

⌄

Assessment Submitted for Review

⌄

TPN TRUSTED PARTNER NETWORK   **Assessment In Remediation**

⌄

Assessment Complete

Note that if you wish to complete the TPN Questionnaire over time, your progress will always be saved and you may return to it from your profile screen at any time.

The Questionnaire is locked and published and the **TPN Blue Shield** is awarded

The Questionnaire is unlocked for changes and discussions between Assessor and Service Provider begin.

The Assessor has submitted the final assessment to TPN for approval

The Service Provider begins remediation on any open findings.

TPN Best Practices Questionnaire Legend

The following Legend items are applicable when editing or viewing your **Blue Shield Questionnaire**:

This symbol denotes a Best Practice question, all other questions are Implementation Guidance

This answer was pre-populated based on the associated non-TPN certificate you uploaded

Hovering over this icon on a question will explain why the question is being displayed

A response meets Best Practice requirements

A response does not meet the Best Practice requirements and needs review by Content Owner

Legend

- **Best Practice Question**
- ☐ Unanswered Question
- ☑ Answered
- 📄 Satisfied by Certificate
- ☑ For Review
- 👁 Question Visible Due to Logic
- 💬 Question has Comments

TPN Best Practices Questionnaire

Tip : multiple TPN Users can answer the Questionnaire concurrently if needed

Upon completion of the Baseline Questionnaire the profile will now show an action button to **Begin MPA Best Practices.** Click this button to start your TPN Best Practices Questionnaire. You may also click the small "B" icon to review your Site/App Baseline Questionnaire

ⓘ Paris Facility — Animation — Pending — Ⓑ BEGIN TPN BEST PRACTICES QUESTIONNAIRE
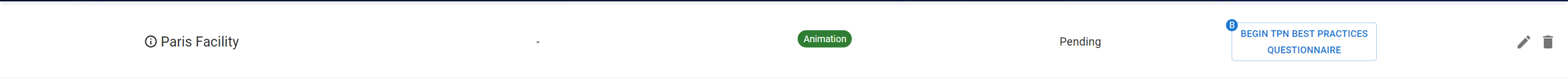
Best Practice questions are illustrated by this icon marking the difference between questions related to Best Practices and Implementation Guidance.

Each question begins as a white background. As you respond the questions will change color for easy reference based on the legend.

Expand this pane to see the overall progress of your Site or Application.

This quick navigation pane allows you to explore and move around the Best Practices without needing to follow a linear order

The Legend is always visible to help remind you what different color and icons represent regarding the various states of your responses and any assessment or remediation states.

TPN Best Practices Questionnaire

If your answers meet all the Best Practice requirements, the screen will turn green when you click **Save and Continue** to illustrate that the answer meets all Best Practices.

🏅 **Do you have a formal, documented Information Security Management System (ISMS), which includes the following?**   ☑

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

☑ Fully Implemented

☐ Overseen by leadership of your organization

☐ Regular reviews of your ISMS

☐ Reviews upon key changes

☐ Control Framework

☐ Governance, Risk, and Compliance (GRC)

☐ Not Implemented

☐ Not Applicable

Provide additional details here:

📎 ATTACHMENTS (0)

SAVE AND CONTINUE ❯

Last Updated By Connor Gartner 03/10/2023 13:30

Each question provides these prompts to assist you.

Each question has an "additional details" box for you to provide context regarding your response (optional).

Please pay attention to the box prompt as some questions may have a particular type of evidence to be provided.

You can attach multiple files of supporting evidence against each question.

A full audit log of all changes are kept, and the last user who modified this response will always be shown with a time and date stamp.

Tip: Including details and context in the "additional details" text box can be helpful to the Content Owners. If you proceed with a TPN Assessment, this info can also make for a smoother and more efficient process.

Please take note of the acceptable types of evidence

Upload attachments to question: Do you have a formal, documented Information Security Management System (ISMS), which includes the following?

✕

Types of Evidence: Documents (Policy, Process, Framework, Handbook/Manual), Diagrams (Data/Workflow), Photographs or Screenshots

Upload or Drop file(s) here

Preview	Name	User	Uploaded	-
📄	Policy_2023.pdf	Quinton Kite	01/23/2023 08:40	🗑

CLOSE   UPLOAD

After clicking **Attach Evidence** on the previous screen, this window will appear.

Simply drag your file from your computer or click on the box to bring up a file browser to find the file on your computer.

A summary of the evidence associated with this question you've uploaded will display here

Note that if you've dragged or selected multiple documents to be uploaded, all files will display here

There is a file size limit of 50MB.

TPN Best Practices Questionnaire

Responses with a yellow screen indicate that the provided answer may need further review by the Content Owner

TPN+ has logic to ensure that where possible you are not asked redundant questions. The **eye icon** illustrates that you are being shown this question based on the response to a previous question.

Moving the mouse over this icon will display the reason a particular question is being asked.

Do you include the following as part of your Information Security Management System (ISMS)?   👁 ☑

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

☐ Fully Implemented

☑ Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.

☐ Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.

☐ Organization charts and job descriptions are prepared to facilitate the designation of roles and responsibilities as it pertains to security

☐ Not Implemented

☐ Not Applicable

Provide additional details here:

📎 ATTACHMENTS (0)

SAVE AND CONTINUE ›

Last Updated By Connor Gartner 03/10/2023 13:41

Tip: If you select **Not Applicable** or **Not Implemented**, you may not see subsequent questions due to Questionnaire logic. Please make sure that you only select Not Applicable if you are sure this is the correct indication.

TPN Best Practices Questionnaire

Current Step: MPA Best Practice In Progres ⌄

OR. Organizational Security ⌃

   1. Policies & Procedures ⌄

   2. Risk Management ⌄

   3. Personnel Security ⌄

   4. Incident Management ⌄

OP. Operational Security ⌄

PS. Physical Security ⌄

TS. Technical Security ⌄

Certifications: Expiration:

⬆ UPLOAD CERTIFICATION

Before beginning any Site or App TPN Best Practice questionnaire, we recommend that you upload accepted non-TPN certificates if available. That way, your answers can be pre-populated in the event that your pre-existing non-TPN certificate satisfies the question.

You are able to upload non-TPN certificates in your Profile screens, and we also provide the opportunity to **upload certification** here on the TPN Best Practice questionnaire screen.

TPN Best Practices Questionnaire

Choose from a list of accepted certifications to upload the evidence against.

To upload a non-TPN certificate, drag the file from your computer or click on the box to bring up a file browser to find the file on your computer.

Provide the date the certificate you uploaded was issued and when it expires.

Select the list of Sites and Applications for which the uploaded certificate applies.

Remember those Sites and Apps must be selected in your profile prior to making this association.

Certification Upload

Certification
ISO 27002-2022

Upload or Drop file(s) here

Preview	Name	User	Uploaded
📄	ISO_27002_Certificate.docx	Andy S	12/27/2022 10:02

Issue Date
12/01/2022

Expiration Date
11/30/2023

Sites
Dallas ⊗

Applications

CLOSE   UPLOAD CERTIFICATION

TPN Best Practices Questionnaire

Any answers that are mapped to an acceptable **uploaded non-TPN certificate** associated to this Site or Application questionnaire will be pre-answered and illustrated by the blue screen.

You are able to over-ride this auto-answer if you wish. However, if you are satisfied that this accurately answers the question, then no further action is required from you.

Do you have a formal, documented Acceptable Use Policy (AUP), which includes the following?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- [ ] **Fully Implemented**
- [ ] Regular reviews of your policy
- [ ] Use of Internet (e.g. social media and communication activities)
- [ ] Use of mobile devices (e.g. phones, tablets, laptops, etc.)
- [ ] Language detailing the restriction for sharing any pre-release content, unless expressed written consent from client
- [ ] Not Implemented
- [ ] Not Applicable

Provide additional details here:

🔗 **ATTACHMENTS (0)**

SAVE AND CONTINUE >

TPN Best Practices Questionnaire

When you have completed all Best Practice questions, you will be able to **SUBMIT AND COMPLETE** to finalize your answers and earn the TPN Blue Shield for that Site or App.

Please note that once you click this button the Questionnaire becomes locked and you cannot update your answers until an assessment process is initiated. Content Owners are also able to see your Questionnaire answers once submitted.

TPN Best Practices Questionnaire Complete ✕

You have answered all questions on the TPN Best Practices Questionnaire. Save to continue editing later or submit and complete to finalize. Once submitted, you will no longer be able to edit your responses. Are you sure you want to submit and complete?

CONTINUE EDITING   SUBMIT

TPN Best Practices Questionnaire Submit Confirmation ✕

Are you sure you want to submit your TPN Best Practices Questionnaire? Once submitted, you will receive your TPN Blue Shield and you can no longer update your answers, add additional information, or upload evidence until you proceed with a TPN Gold Assessment.

CONTINUE EDITING   SUBMIT AND COMPLETE

The TPN Blue Shield will be displayed on the profile page denoting the status of the Site.

You are now able to click on the Blue Shield icon to download a copy of the Shield for your promotional use.

Sites (12)   **+ SITE**

Shield	Name	Applications	Services	Status	Actions	
🛡	ⓘ Paris Facility	-	Animation	Self-Reporting Complete	Ⓑ SCHEDULE ASSESSMENT VIEW QUESTIONNAIRE	

Service Provider:
Scheduling a TPN Assessment

Service Provider – Site/App Assessment Scheduling

After you have **completed and submitted** your TPN Best Practices Questionnaire your TPN Shield status turns to **Blue** in your profile and you are able to download the Blue Shield logo for your **promotional use by clicking on the logo** and also schedule a TPN Gold Assessment.

Clicking on **Schedule Assessment** will allow you to send a request to your selected TPN accredited Assessor who will perform the assessment.

We recommend that you negotiate cost and terms directly with the 3rd party TPN accredited Assessor prior to scheduling an assessment on TPN+. **Once the Assessor accepts the request, the 15-business day SLA begins.**

Service Provider – Multiple Assessment Scheduling

By clicking **+Assessment** in your profile section, you are able to schedule single or multiple Sites and Apps to one assessment request.

Allows completed assessments to be filtered out of view

Manage Assessments (1)   Show Completed   + ASSESSMENT

Assessor	Questionnaire Count	Status	Action	
> TPN Assessor	1	Assessment Submitted for Review	-	-

Choose the various Sites and Apps to be bundled in the assessment request.

Create New Assessment   ✕

Search Sites and Applications

Paris Facility ✕   Test App 3.9.23 2 ✕

Site/Application	Scope	Type	
Test App 3.9.23 2	On-Prem ⬤ Cloud ⬤	On Site ⬤	🗑
Paris Facility	Site ⬤ Cloud ⬤	On Site ⬤	🗑

TPN Assessor Training - Level 1   🔍 ▾

TPN Assessor   🔍 ▾

CANCEL   SAVE

Scope: An assessment scope can be on-prem and/or cloud depending on scope.

Type: Defines if the actual 3rd party assessment is on-site or remote.

Choose the name of the Assessor to send the request to. All Assessors are individuals, so company names will be represented by the Assessor's name.

Service Provider: Pre-Assessment

Pre-Assessment

Your selected **Assessor** must **accept** your assessment request in their own TPN+ profile. Once accepted they will have access to your TPN Best Practice Questionnaire and associated documentation.

If the **Assessor** rejects your assessment request you will be notified.

Note that once the Assessor clicks **ACCEPT** this starts the 15-business day turnaround SLA

Pre-Assessment

Once accepted, the **Assessor** will click **Review and Comment** to start the Pre-assessment phase where you and your selected Assessor can collaborate and review your questionnaire answers, evidence and other information such as non-TPN certs.

During the pre-assessment phase you can update your Questionnaire answers and upload evidence prior to beginning the formal assessment.

You can manage all pre-assessment and assessment activity in the **Manage Assessments** section in your profile.

Note that the pre-assessment phase is part of the 15-business day turnaround SLA

Pre-Assessment - Commenting

TPN Best Practices Questionnaire for Paris Facility **BACK TO COMPANY DETAILS**

TPN Best Practices Questionnaire

OR-1.0 Information Security Management System
Best Practice:
Establish, regularly review, and update upon key changes, an Information Security Management System (ISMS), which is approved by leadership of the organization, to include the following:...

Show More

Do you have a formal, documented Information Security Management System (ISMS), which includes the following?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- ☑ Fully Implemented
- ☐ Overseen by leadership of your organization
- ☐ Regular reviews of your ISMS
- ☐ Reviews upon key changes
- ☐ Control Framework
- ☐ Governance, Risk, and Compliance (GRC)
- ☐ Not Implemented
- ☐ Not Applicable

Provide additional details here:

COMMENTS (0)   **ATTACHMENTS (0)**

SAVE AND CONTINUE
Last Updated By Connor Gartner 03/10/2023 13:30

Do you include the following as part of your Information Security Management System (ISMS)?

Current Step: Pre-Assessment In Progress

Current Best Practice: Information Security Management System

Certifications: End Date:
🔍 ISO 27002-2022   03/10/2024

UPLOAD CERTIFICATION

Legend
- 🏅 **Best Practice Question**
- ☐ Unanswered Question
- ☑ Answered
- 📄 Satisfied by Certificate
- ☑ For Review
- 👁 Question Visible Due to Logic
- 💬 Question has Comments

To begin or continue a dialogue with the Assessor during pre-assessment or the assessment phase click the **Comments** button

Pre-Assessment - Commenting

Comments for Question: Do you have a formal, documented Information Security Management System (ISMS), which includes the following?

TA

Please upload relevant evidence to show this control is fully implemented
TPN Assessor | Assessor | 03/13/2023 12:00

Please see the attached documents
Connor Gartner | Service Provider | 03/13/2023 12:02

CG

New Comment *

ADD COMMENT

CLOSE

During Pre-Assessment, the Assessor may contact you via the **Comments** button to request additional information.

Once the full assessment phase begins, the ability to provide additional evidence or modify your responses to the best practices is no longer available.

You can provide responses and upload requested documents within the **Comments** window.

Recent Activity Notifications

When any change is made during the assessment process, a notification will appear on the profile to notify that there have been changes since the questionnaire was last opened.

Recent Activity Notifications

The recent activity section displays a list of all questions that have updated information since the questionnaire was last opened.

Under each question will be a list of items that have changed so you can easily identify what to look for when reviewing.

TPN Best Practices Questionnaire for Paris Facility BACK TO COMPANY DETAILS

TPN Best Practices Questionnaire

OR-1.0 Information Security Management System
Best Practice:
Establish, regularly review, and update upon key changes, an Information Security Management System (ISMS), which is approved by leadership of the organization, to include the following:...

˅ Show More

Do you have a formal, documented Information Security Management System (ISMS), which includes the following?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- ☑ Fully Implemented
- ☐ Overseen by leadership of your organization
- ☐ Regular reviews of your ISMS
- ☐ Reviews upon key changes
- ☐ Control Framework
- ☐ Governance, Risk, and Compliance (GRC)
- ☐ Not Implemented
- ☐ Not Applicable

Provide additional details here:

COMMENTS (2)   ATTACHMENTS (0)

SAVE AND CONTINUE ›
Last Updated By Connor Gartner 03/13/2023 12:02

Do you include the following as part of your Information Security Management System (ISMS)?

Recent Activity

Since Last view of Assessment

OR-1.0 Information Security Management System
Do you have a formal, documented Information Security Management System (ISMS), which inclu...
| Comment |

Current Step: Pre-Assessment In Progress

Current Best Practice: Information Security Management System

Certifications: End Date:
🔍 ISO 27002-2022   03/10/2024

📄 UPLOAD CERTIFICATION

Legend   ˄

🎖 **Best Practice Question**
☐ Unanswered Question
☑ Answered
📄 Satisfied by Certificate
◻ For Review
👁 Question Visible Due to Logic
💬 Question has Comments

Service Provider: Assessment

Service Provider – Assessment

After the Assessor completes Pre-Assessment and moves to the **Assessment** phase, you are no longer able to update your answers or upload any documentation.

You are able to continue communicating with the Assessor through the Comments function if needed.

The Assessor will click the Assess Button to open the **Assessor Findings Window**.

The **Assessor** will select the appropriate response related to the Site or Application being assessed and add Finding comments.

Service Provider – Assessment

The Assessor will complete the selections for Best Practice and Implementation Guidance as follows:

When **Fully Implemented** is selected no additional info is required and the answer will be marked green.

When **Partially** or **Not Implemented** is selected, and findings are provided in the comment box the Questionnaire answer will be marked red for Remediation.

If **Not Applicable** was selected by you and the Assessor disagrees, they will select **Not Implemented,** add comments and the answer will be marked red for Remediation

Selections reflect Service Provider Questionnaire answers. The red screen status shows that the item has now been placed in a remediation state.

The Assessor Findings selection and text for anything **Partially** or **Not Implemented** will show up in the final assessment report.

Do you include the following as part of your Information Security Management System (ISMS)?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented and provide additional details
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- [ ] Fully Implemented
- [x] Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.
- [ ] Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.
- [ ] Organization charts and job descriptions are prepared to facilitate the designation of roles and responsibilities as it pertains to security
- [ ] Not Implemented
- [ ] Not Applicable

Provide additional details here:

ASSESSORS FINDINGS   COMMENTS (0)   ATTACHMENTS (0)

⚠ UPDATE REMEDIATION

Last Updated By John Doe 01/20/2023 13:10

Assessor Finding for Do you include the following as part of your Information Security Management System (ISMS)? ✕

- ( ) Fully Implemented
- (•) **Partially Implemented**
- ( ) Not Implemented
- ( ) Not Applicable

Assessor Finding
Please upload evidence.

CANCEL   UPDATE FINDING

Service Provider – Completed Assessment

TPN+ Platform Process
Supporting TPN Service Provider Members

The Assessor submits the completed assessment to TPN for review. If TPN has questions, they will contact you or the Assessor via TPN+ comments for information.
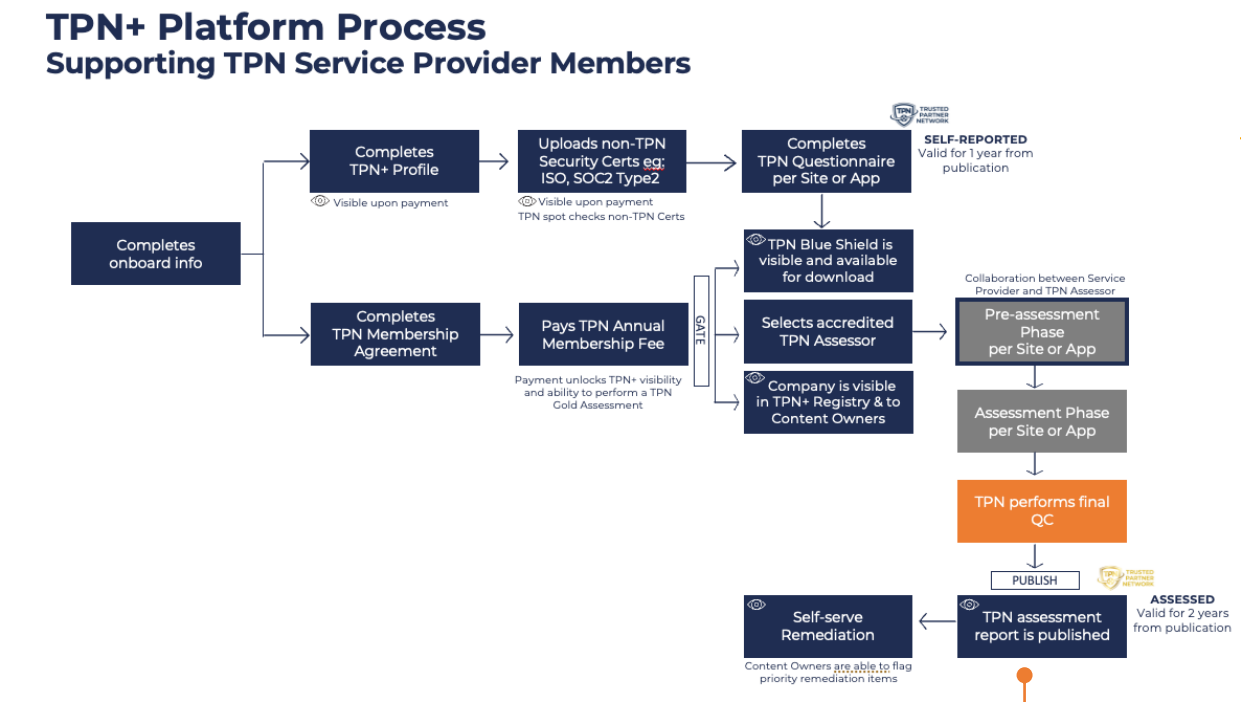
Once the assessment has been approved by TPN, the status is marked as **Complete** and the **TPN Gold Shield** is awarded to the Site or Application.

You now have **3 business days** to add your Remediation plan, with comments and dates to the remediation items.

You are now able to click on the **Gold Shield icon** to download a copy of the Gold Shield for your promotional use.

Service Provider – Generate Report

Once the assessment has been completed, you can click the **Generate Report** button to create the **TPN Assessment report** . It is provided as a visually watermarked PDF containing the username/email and date of the download.

TPN+ Sample Generated Report

Overview

Assessment Scope: On Premise
Assessment Type: , In Person
Related Facility: Approved Phase Test
Services: Mastering, Mixing, Sound Effects / Design
Number of Employees: 11 to 20 employees
Owned Applications:

Security Domains	Best Practice				Implementation Guidance				Legend
	FI	PI	NI	NA	FI	PI	NI	NA	
Organizational Security	8	1	1	1	5	2	2	0	FI: Fully Implemented
Operational Security	5	2	1	1	5	1	1	0	PI: Partially Implemented
Physical Security	7	1	1	0	7	1	0	0	NI: Not Implemented
Technical Security	22	1	8	4	22	1	2	0	NA: Not Applicable
Totals	42	5	11	6	39	5	5	0	

OR: Organizational Security - Policies & Procedures
0. Information Security Management System

Best Practice:
Establish, regularly review, and update upon key changes, an Information Security Management System (ISMS), which is approved by leadership of the organization, to include the following:
• Control framework
• Governance, Risk, and Compliance (GRC)

Implementation Guidance:
Recommend implementing the following:
• Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.
• Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.
• Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to security

Implementation Guidance

Do you include the following as part of your Information Security Management System (ISMS)?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented and provide additional details
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

x Fully Implemented
√ Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.
√ Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.
x Organization charts and job descriptions are prepared to facilitate the designation of roles and responsibilities as it pertains to security
x Not Implemented
x Not Applicable
Service Provider Comment: Working to incorporate org charts into this process

Partially Implemented

Assessor Finding:
Agreed, org charts will need to be implemented

OR: Organizational Security - Policies & Procedures
1. Acceptable Use Policy

Best Practice:
Establish and regularly review an Acceptable Use Policy (AUP) governing the use of Internet (e.g. social media and communication activities) and mobile devices (e.g. phones, tablets, laptops, etc.), to include the following:
• Do not share on any social media platform, forum, blog post, or website: information related to pre-release content and related project activities, unless expressed written consent from the client is obtained

Implementation Guidance:
Recommend implementing the following:
• Use dedicated accounts for marketing purposes

Implementation Guidance

Do you use a dedicated account for marketing purposes?

Select from the following:

x Yes
√ No
x Not Applicable
Service Provider Comment: We use the same account for marketing

Not Implemented

Assessor Finding:
No separate account for marketing purposes

Service Provider: Remediation Management

Remediation Management

TPN Service Provider Profile

TRUSTED PARTNER NETWORK

TPN Service Provider

Address:
1234 Service Provider Way
Los Angeles, CA 99999

+1 (555) 555-5555
SPTest.com

Annual Gross Revenue: $200M+
Employee Count: 21 or more employees

Billing Address:
TPN Service Provider
1234 Service Provider Way
Los Angeles, CA 99999
US
+1 (555) 555-5555

Primary Contact:

Billing Customer ID: TPP00125
Billing PO Number: 123456
VAT Number: 55555

Services (12)

+ SERVICE

Sites (3)

+ SITE

Shield	Name	Applications	Services	Status	Actions	
	ⓘ Blue Shield - London	Custom TPN Application	Music Composition, Music Editing, Music Recording	Self-Reporting Complete	SCHEDULE ASSESSMENT, VIEW QUESTIONNAIRE	
	ⓘ Service Provider Test	TPN Licensed App	Music Composition, Music Editing, Music Recording	1 5	REMEDIATE, GENERATE REPORT	
	ⓘ Test Site - Paris	-	ADR	Self-Attested	BEGIN TPN BEST PRACTICES QUESTIONNAIRE	✎ 🗑

Click the **REMEDIATE** button to address remediation items. Once all remediation items have been addressed, this button will revert to **View Assessment**.

In your TPN+ Profile, these symbols indicate the **number** of remediation items that need your attention. **Red** represents **Best Practice** items and **Yellow** represents I**mplementation Guidance** items that are unresolved.

Remediation Management

TPN Best Practices Questionnaire for Service Provider Test BACK TO COMPANY DETAILS

TPN Best Practices Questionnaire

OR-1.-1 Risk Management Program
Best Practice:
Establish a formal, documented security Risk Management Program, to include the following:...

⌄ Show More

Do you have a formal, documented security Risk Management Program, which includes the following?

Does your security Risk Management program include the following?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- ☑ Fully Implemented
- ☐ Clearly defined scope for the security risk assessment and modified as necessary
- ☐ A systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g. Business Impact Assessment (BIA))
- ☐ Risks identification ties into the Business Continuity (BCP) and Disaster Recovery (DR) Plans
- ☐ Inclusion of risks to cloud infrastructure
- ☐ Regular meetings with management and key stakeholders to identify and document risks
- ☐ A formal exception policy
- ☐ Maintained documentation of a Threat Modeling and Analysis process
- ☐ Documentation of risks associated with WFH/remote access regarding content workflow
- ☐ Leveraged NISTIR 8286, FAIR frameworks, or ISO 3100:2018
- ☐ Not Implemented
- ☐ Not Applicable

Provide additional details here:

ASSESSORS FINDINGS   COMMENTS (0)   📎 ATTACHMENTS (0)

✓ REMEDIATE

Current Step: Assessment In Remediation ⌄

View 6 Controls in Remediation ⌃

OR-1.0 Information Security Management System — 1
OR-4.0 Incident Management — 1
OR-2.0 Risk Management Program — 1
OP-1.0 Receiving
OP-1.1 Packaging — 1
OP-2.0 Data & Assets — 1

Current Best Practice: Risk Management Program ⌄

Certifications: End Date:
🔍 ISO/IEC 27001   02/04/2024

Legend ⌃

🏅 **Best Practice Question**
☐ Unassessed Question
☑ Assessor Reviewed
⚠ Remediation
⚠ Remediation: Content Owner Priority
☑ Remediation Complete
👁 Question Visible Due to Logic
💬 Question has Comments

Using this navigation bar gives a quick reference to all the items that are marked for remediation

Items marked as a priority from Content Owners will be denoted by their purple color.

Remediation Management

TPN Best Practices Questionnaire for Service Provider Test BACK TO COMPANY DETAILS

TPN Best Practices Questionnaire

OR-1.-1 Risk Management Program
Best Practice:
Establish a formal, documented security Risk Management Program, to include the following:...

⌄ Show More

📍 **Do you have a formal, documented security Risk Management Program, which includes the following?**

Does your security Risk Management program include the following?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

- ☑ Fully Implemented
- ☐ Clearly defined scope for the security risk assessment and modified as necessary
- ☐ A systematic approach that uses likelihood of risk occurrence, impact to business objectives/content protection, and asset classification for assigning priority (e.g. Business Impact Assessment (BIA))
- ☐ Risks identification ties into the Business Continuity (BCP) and Disaster Recovery (DR) Plans
- ☐ Inclusion of risks to cloud infrastructure
- ☐ Regular meetings with management and key stakeholders to identify and document risks
- ☐ A formal exception policy
- ☐ Maintained documentation of a Threat Modeling and Analysis process
- ☐ Documentation of risks associated with WFH/remote access regarding content workflow
- ☐ Leveraged NISTIR 8286, FAIR frameworks, or ISO 3100:2018
- ☐ Not Implemented
- ☐ Not Applicable

Provide additional details here:

ASSESSORS FINDINGS   COMMENTS (0)   ⧉ ATTACHMENTS (0)

✓ REMEDIATE

Clicking **Assessor Findings** brings up a window displaying the findings and the Assessor's related comments.

Assessor Finding for Does your security Risk Management program include the following?   ✕

- ◯ Fully Implemented
- ◯ Partially Implemented
- ⦿ Not Implemented
- ◯ Not Applicable

Finding required if answer is "Partially Implemented" or "Not Implemented"

Assessor Finding *
Test Finding

CLOSE

When ready to respond to a remediation, click this button.

Remediation Management

You will be required to provide an update using one of the three selections on this screen.

Will not Remediate requires comments to be added.

Will Remediate Later requires a target date by which the finding will be remediated, and comments outlining the plan.

When either of these options are chosen, the question will turn **yellow** to indicate that Remediation is complete.

Please note that following the assessment completion date, you have 3 business days to either remediate or provide a remediation plan.

When **Remediated** is chosen you will be provided areas for more information to be added.

We recommend that you use TPN+ to share evidence of remediation.

Please use the comment box to describe the intended plan to remediate, or the actual action taken.

Remediation Management

Do you include the following as part of your Information Security Management System (ISMS)? 👁 ⚠

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented, provide additional details, and upload relevant evidence
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

☑ Fully Implemented

☐ Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.

☐ Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.

☐ Organization charts and job descriptions are prepared to facilitate the designation of roles and responsibilities as it pertains to security

☐ Not Implemented

☐ Not Applicable

Provide additional details here:
Testing: Please review the uploaded evidence

ASSESSORS FINDINGS   COMMENTS (0)   📎 ATTACHMENTS (0)

✓ UPDATE REMEDIATION

When choosing **Will Remediate Later**, the remediation stays marked as red as it has not been completed. The button changes to **Update Remediation**.

Remediate Do you include the following as part of your Information Security Management System (ISMS)? ✕

○ Will not Remediate

● **Will Remediate Later**

○ Remediated

Remediation Date
02/11/2023 📅

Remediation Comment
Waiting on system to update

CANCEL   UPDATE REMEDIATION

Service Provider: Generating a Report

Content Owner – Generate Report

Once the assessment has been completed, you can click the **Generate Report** button to create the **TPN Assessment report** . It is provided as a visually watermarked PDF containing the username/email and date of the download.

TPN+ Sample Generated Report

Overview

Assessment Scope: On Premise
Assessment Type: , In Person
Related Facility: Approved Phase Test
Services: Mastering, Mixing, Sound Effects / Design
Number of Employees: 11 to 20 employees
Owned Applications:

Security Domains	Best Practice				Implementation Guidance				Legend
	FI	PI	NI	NA	FI	PI	NI	NA	
Organizational Security	8	1	1	1	5	2	2	0	FI: Fully Implemented
Operational Security	5	2	1	1	5	1	1	0	PI: Partially Implemented
Physical Security	7	1	1	0	7	1	0	0	NI: Not Implemented
Technical Security	22	1	8	4	22	1	2	0	NA: Not Applicable
Totals	42	5	11	6	39	5	5	0	

OR: Organizational Security - Policies & Procedures
0. Information Security Management System

Best Practice:
Establish, regularly review, and update upon key changes, an Information Security Management System (ISMS), which is approved by leadership of the organization, to include the following:
• Control framework
• Governance, Risk, and Compliance (GRC)

Implementation Guidance:
Recommend implementing the following:
• Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.
• Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.
• Prepare organization charts and job descriptions to facilitate the designation of roles and responsibilities as it pertains to security

Implementation Guidance

Do you include the following as part of your Information Security Management System (ISMS)?

Select which of the below apply:
If ALL requirements are met: choose Fully Implemented and upload relevant evidence
If SOME of the requirements are met: choose the line items that are implemented and provide additional details
If NONE of the requirements are met: choose Not Implemented and provide additional details
If this control does NOT APPLY to your Site or Application: choose Not Applicable and provide additional details

x Fully Implemented
√ Reference established Information and Content Security frameworks e.g. MPA Best Practices, ISO 27001, NIST 800-53, SANS, CoBIT, CSA, CIS, etc.
√ Establish an independent team for Information Security, including a Governance Committee, to develop policies addressing threats, incidents, risks, etc.
x Organization charts and job descriptions are prepared to facilitate the designation of roles and responsibilities as it pertains to security
x Not Implemented
x Not Applicable
Service Provider Comment: Working to incorporate org charts into this process

Partially Implemented

Assessor Finding:
Agreed, org charts will need to be implemented

OR: Organizational Security - Policies & Procedures
1. Acceptable Use Policy

Best Practice:
Establish and regularly review an Acceptable Use Policy (AUP) governing the use of Internet (e.g. social media and communication activities) and mobile devices (e.g. phones, tablets, laptops, etc.), to include the following:
• Do not share on any social media platform, forum, blog post, or website: information related to pre-release content and related project activities, unless expressed written consent from the client is obtained

Implementation Guidance:
Recommend implementing the following:
• Use dedicated accounts for marketing purposes

Implementation Guidance

Do you use a dedicated account for marketing purposes?

Select from the following:

x Yes
√ No
x Not Applicable
Service Provider Comment: We use the same account for marketing

Not Implemented

Assessor Finding:
No separate account for marketing purposes

Change Log

TPN+ v1.1.0 Updates 07/13/2023:

- **Slides 3-4: Process maps updated**
- **Slide 9: Important note regarding Microsoft Authenticator**
- **Slide 16: User management now includes Consultant toggle option**
- **Slides 28-39: Updated App Flow**
- **Slide 49: Tip about adding details in Questionnaire**
- **Slide 51: Tip about Not Applicable selection**