



Cyber Guru Enterprise

Onboarding Procedure

How to turn employees and contractors into your organization's first line of defense

www.cyberguru.io

CG Awareness Overview

- Phishing
- Password
- Social media
- Privacy & GDPR
- Mobile Device & APP
- Fake News
- USB Device
- Email Security
- Malware & Ransomware
- Web Browsing
- Critical Scenarios
- Social Engineering

- Clean Desk
- Smart working
- Social collaboration e video conferencing
- Smishing & Vishing
- Spear Phishing
- Ransomware
- Multi-factor authentication
- IoT Device
- Bluetooth & WIFI
- Information Classification
- Data Protection
- Social Engineering 2

- Real Scam
- Phone Scam
- Social & Cyberbullying
- Privacy
- Legal Aspect
- Physical Security
- E-commerce
- Holiday & Business trip
- Cyber Hygiene
- Backup & Restore
- Best practice
- Social Engineering 3



**UPON
COMPLETION
OF THE 3
LEVELS**



CAMPUS
Knowledge
updating

CGA level 1
1st year

CGA level 2
2nd year

CGA level 3
3rd year

Certificate

Campus

CG Awareness Overview - School

Breakdown of individual years

12 MODULES

The standard release of modules is: **one module per month** over the course of a year; the module is available in both video and pdf format

36 LESSONS

Each module consists of 3 lessons lasting from 5-7 minutes each

36 LEARNING TESTS

After each lesson there is a test, 3 out of 4 questions must be answered correctly in order to access the next lesson, tests can be repeated

4 REINFORCEMENT TESTS

For every 3 modules there is a reinforcement test, 10 out of 10 questions must be answered correctly, tests cannot be repeated; a negative result does not block access to the next module

1 COURSE CERTIFICATE

Upon completion of the modules for each year, the user can download the certificate



Gamification

Medals are obtained by passing the learning tests at the end of the lesson
<4 correct answers out of 4>

Cups are obtained by passing the reinforcement test after every 3 modules
< 10 correct answers out of 10>



Extra content in the platform:

Micro-pills (video)



Special sections:

Internal Area

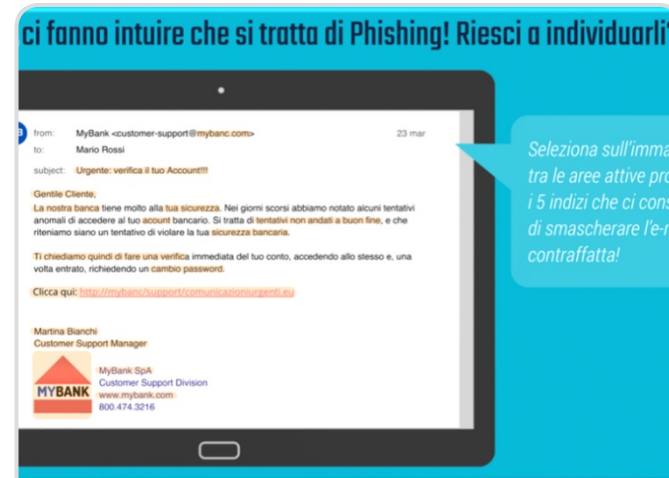
Campus - Maintenance & Update



Lifelong Learning



Warm-Up



DidActive



Serious Game



Cyber Insights

MAINTENANCE

UPDATING

Overview CG Awareness - Campus Awareness

- Context
- Clean & Secure
- E-Commerce
- Cyber Hygiene
- Backup
- Travel
- Mobile
- Email Investigate
- Phishing recap
- Malware recap
- Email Investigate
- Personal data
- Ramsonware
- Password Recap
- Social Media
- Social Engineering
- Difficult travelling
- Kalasya conspiracy
- Cyber «Risk it all»
- The art of deception
- SMS Spoofing
- Password Manager
- Juice Jacking
- Keylogger
- Unconscious Testimonial (AI)
- Deep Fake (AI)
- Privacy Risk (AI)
- Targeted Attacks (AI)

WARM UP

DIDACTIVE

SERIOUS GAME

CYBER INSIGHTS

Overview CG Awareness - Campus



Breakdown of individual years

8 WARM UP

Learning situational objects that include 5 interactions for each of which feedback and 'shields' are obtained for the following conditions: correct interaction, partially correct, or incorrect.

8 DIDACTIVE

Educational learning objects that include 5 interactions, for each of which feedback and 'shields' are obtained for the following conditions: correct interaction, partially correct, or incorrect

8 CYBER INSIGHTS

Dedicated update sessions on a single topic, consisting of a video clip and a four-question test.

4 SERIOUS GAMES

Every 3 contents, an interactive 'serious game' is introduced that employs the technique of 'game-based learning' to develop understanding regarding Cybersecurity topics.

1 COURSE CERTIFICATE

Upon completion of the modules for each year, the user can download the certificate



Gamification

The medal will be obtained by excellently surpassing all interactions.



Extra contents in the platform:

Micro-pills (video)



Special session:

Internal Area

CG Channel Overview

Breakdown of individual year

12 EPISODES

The standard release of Channel episodes is: **one episode each month** over the course of a year; once they are released, the episodes will remain visible on the platform.

STORYTELLING

The episodes are characterized by a **captivating storytelling**, which captivates the users, giving them an immersive experience of the content in the video, similar to a TV series.

DURATION OF EPISODES

The duration of the individual episodes is limited and follows the same approach as the duration of the video lessons in the Awareness Program; on average, the episodes last about 5 minutes each.

ACCESS TO CHANNEL

Access is enabled using the same platform interface as the Awareness Program

CG Channel Overview

CGC Episodes

- CEO FRAUD – From heaven to hell in one click
- SMART WORKING – The perfect storm
- PASSWORD – It's just a game!
- USB DEVICE – A fistful of songs
- PUBLIC WIFI – Caught in the net
- SOCIAL ENGINEERING – The worst deal ever
- DEEPFAKE – Scammers work in mysterious ways
- RANSOMWARE – Learn how to read!
- SIM SWAP – The unbearable lightness of bank accounts
- IDENTITY THEFT – Don't let hackers get in your shoes
- SCAM WEBSITES – The crocodile technique
- SMISHING – Fatal Refund

CGC level 1 – 1st Season

- WATERING HOLE – All mad for the discount
- WHATSAPP SCAMS – A fruitful fishing
- VISHING & DATA THEFT – Call me
- QISHING - “Dangerous” parking
- FAKE WEBSITE – Try, but don't forget
- CEO FRAUD – Copy with too much knowledge
- DATA PROTECTION – A memorable photo...to forget
- SPEAR PHISHING – It all started with an e-mail
- FAKE NEWS – Beyond Appearances
- PHARMING - A “wrong” donation
- PRIVACY – Dangerous Posts
- SHARED DEVICES – A “no low cost” holiday

CGC level 2 – 2nd Season

- CEO FRAUD – Thin connections
- CREDENTIAL STUFFING – An inconvenient truth
- PASSWORD SECURITY – No alternative
- EMAIL SPOOFING – Domino effect
- SPEAR PHISHING – The devil is in the details
- PRIVACY – An incriminating selfie
- SIM SWAP – The cat and the fox 2.0
- WATERING HOLE – The lion and the gazelle
- PUBLIC WIFI – The fish in the net
- USB DEVICE – Lethal USB stick
- KEYLOGGER – Key logger (an invisible enemy)
- CYBERSECURITY – The culprit

CGC livello 3 – 3rd Season

Onboarding Process

Contractual Aspects



SERVICE ACTIVATION LICENSE VALIDITY

The contact person will receive credentials for a first-time login on the Cyber Guru onboarding portal

Licenses are valid from the day of service activation until the contract expires



ACCEPTANCE OF T&C

Access to onboarding portal and acceptance of T&C

- **EULA**
- **Appointment of data controller**
- **Privacy policy**

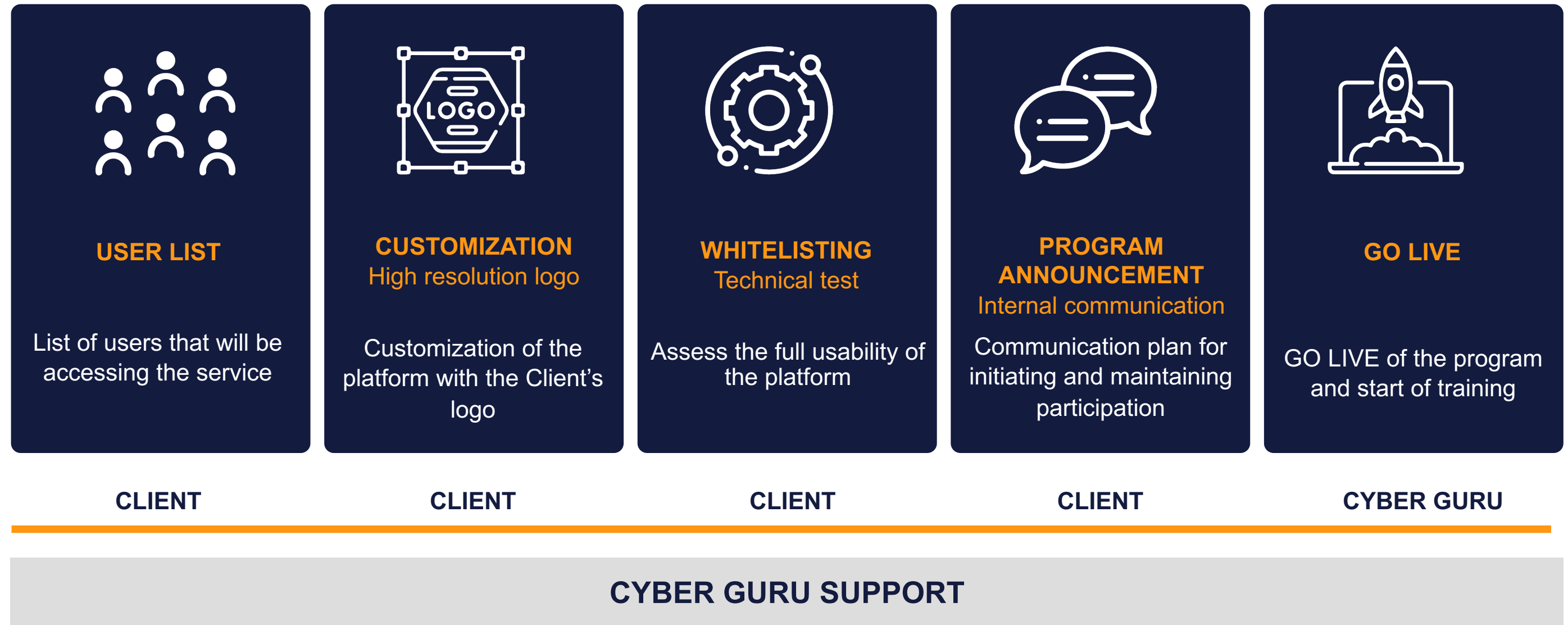


KNOWLEDGE BASE DOCUMENTATION

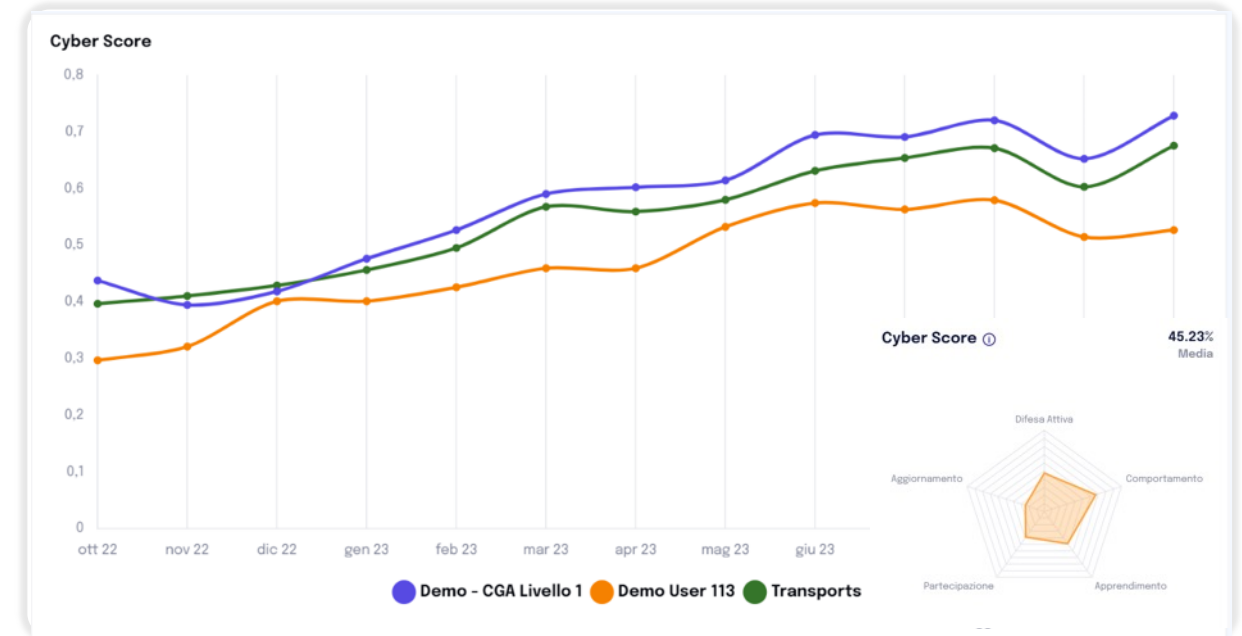
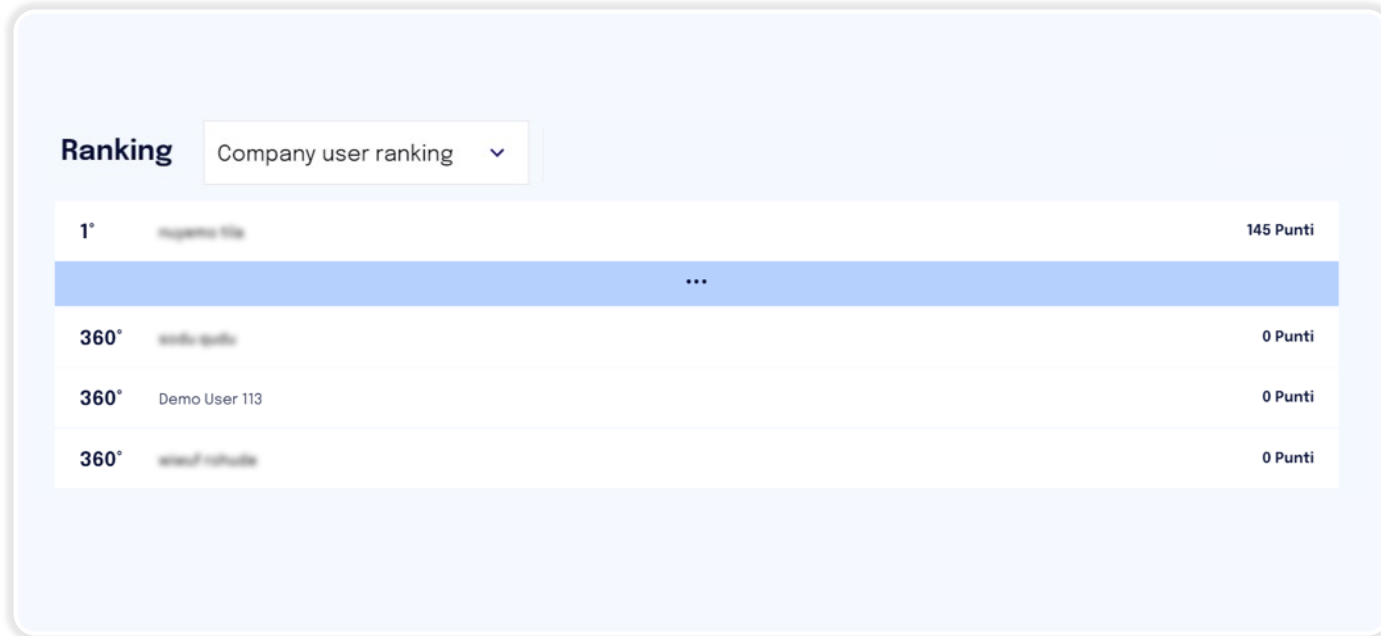
It will be possible to access and download process and product documentation, upload logos and the user list required for GO LIVE, within the shared repository

Onboarding Process

Operational Aspects



Gamification



TEAM-BASED GAMIFICATION (Strongly recommended)

INDIVIDUAL GAMIFICATION



User Engagement



Reward



Achievement



Motivation



Learning



Challenge

Student Caring



Internal communication by the Client



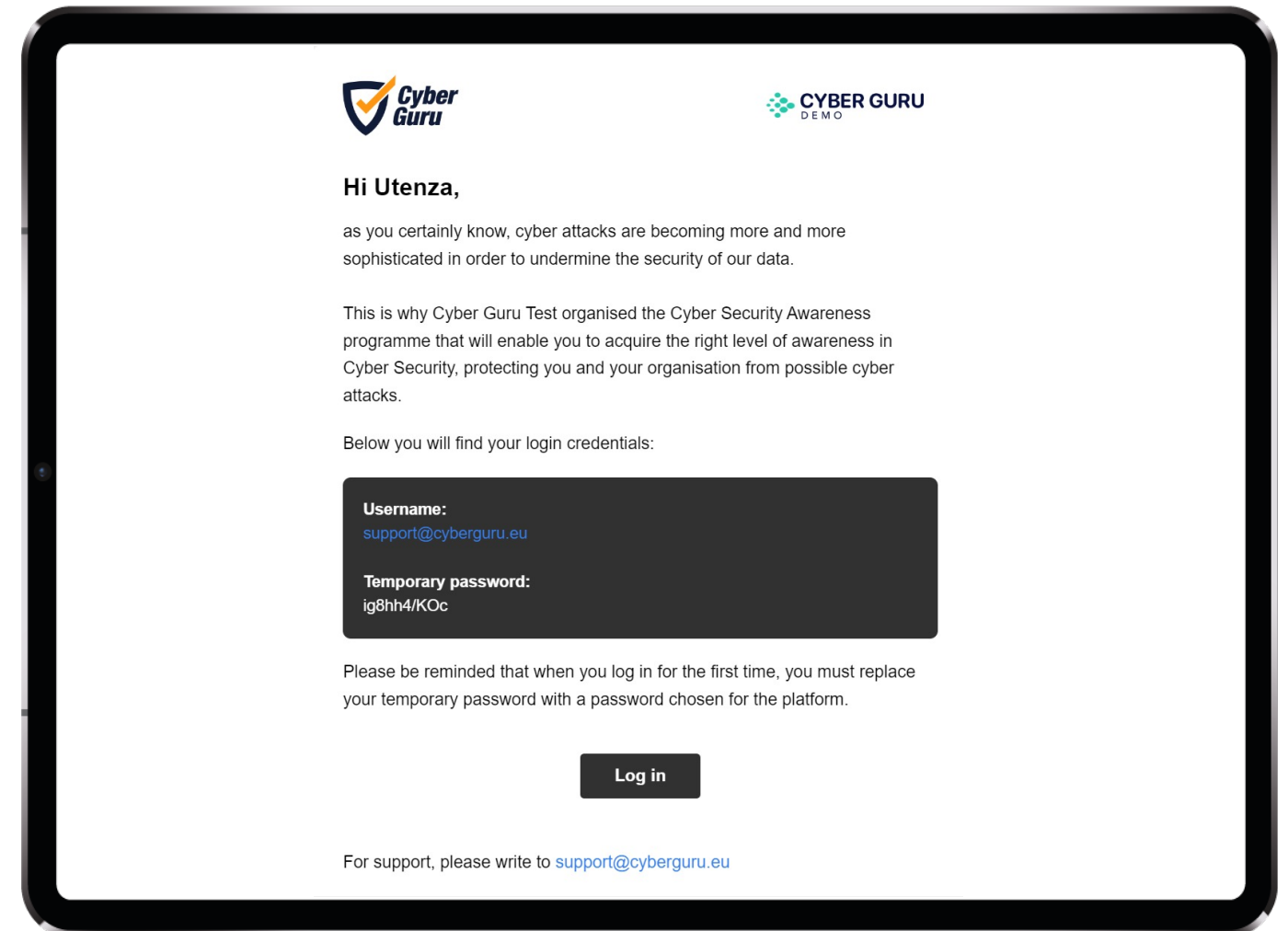
Notification of GO LIVE (after internal communication)



Notification for the release of a new module

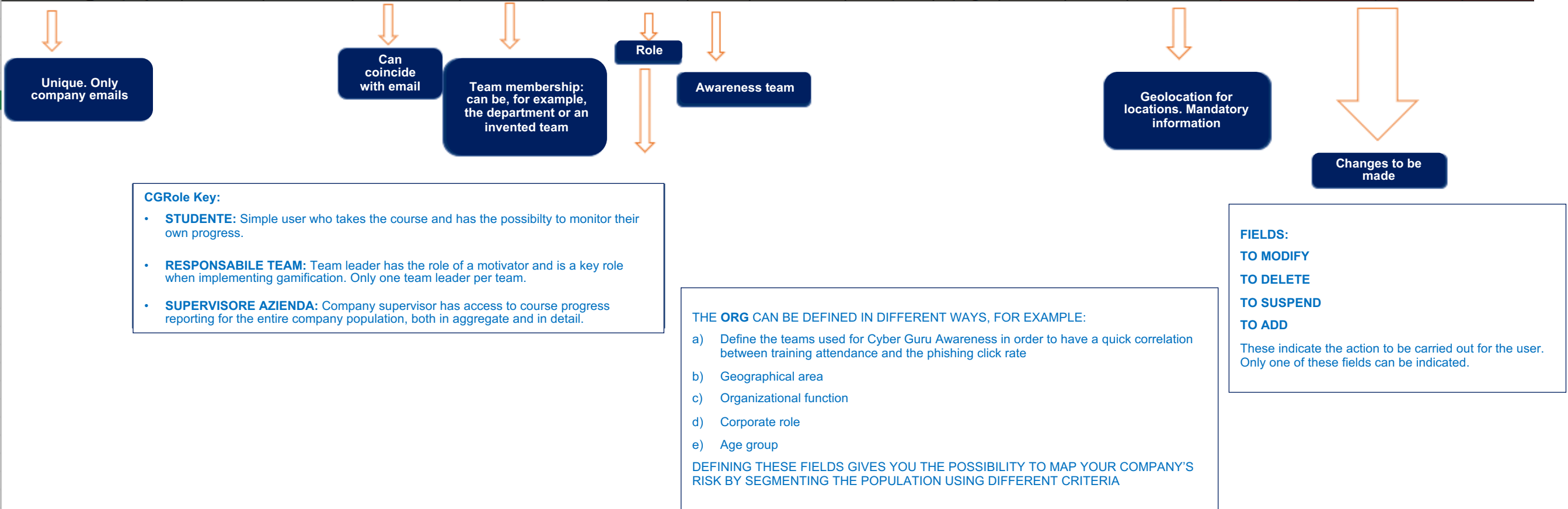


Sending massive emails from team leader and/or supervisor directly from the platform (e.g., reminders)



User List Template

COMMON				AWARENESS/CHANNEL			PHISHING						POST GO LIVE (USER LIST UPDATE)				
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	Country*	To modify	To delete	To suspend	To add
john.smith@company.com	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
mario.rossi@company.com	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
marco.lucini@company.com	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
bill.gates@company.com	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
elon.musk@company.com	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogna	Barcelons	ES		delete		
warren.buffer@company.com	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Developer	Impiegato	Lombardia	Milan	IT			suspend	



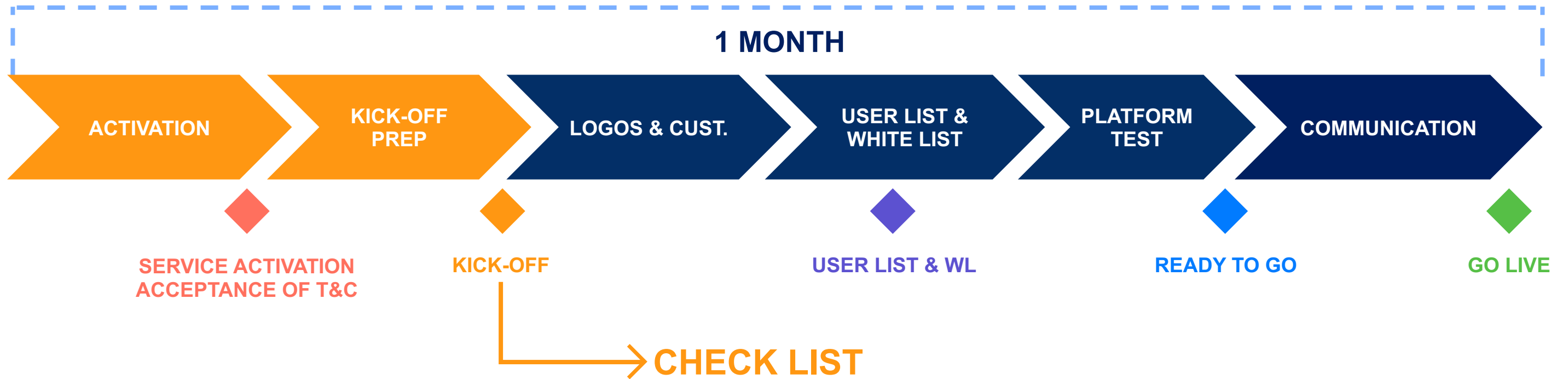
Master Plan



Service is active from the date of service activation notice (irrespective of Go Live).

Onboarding is recommended within a month of service activation in order to maintain an adequate cognitive load and effective learning. Delays in the Go Live require a planning of releases which may have an impact on the effectiveness of the training path.

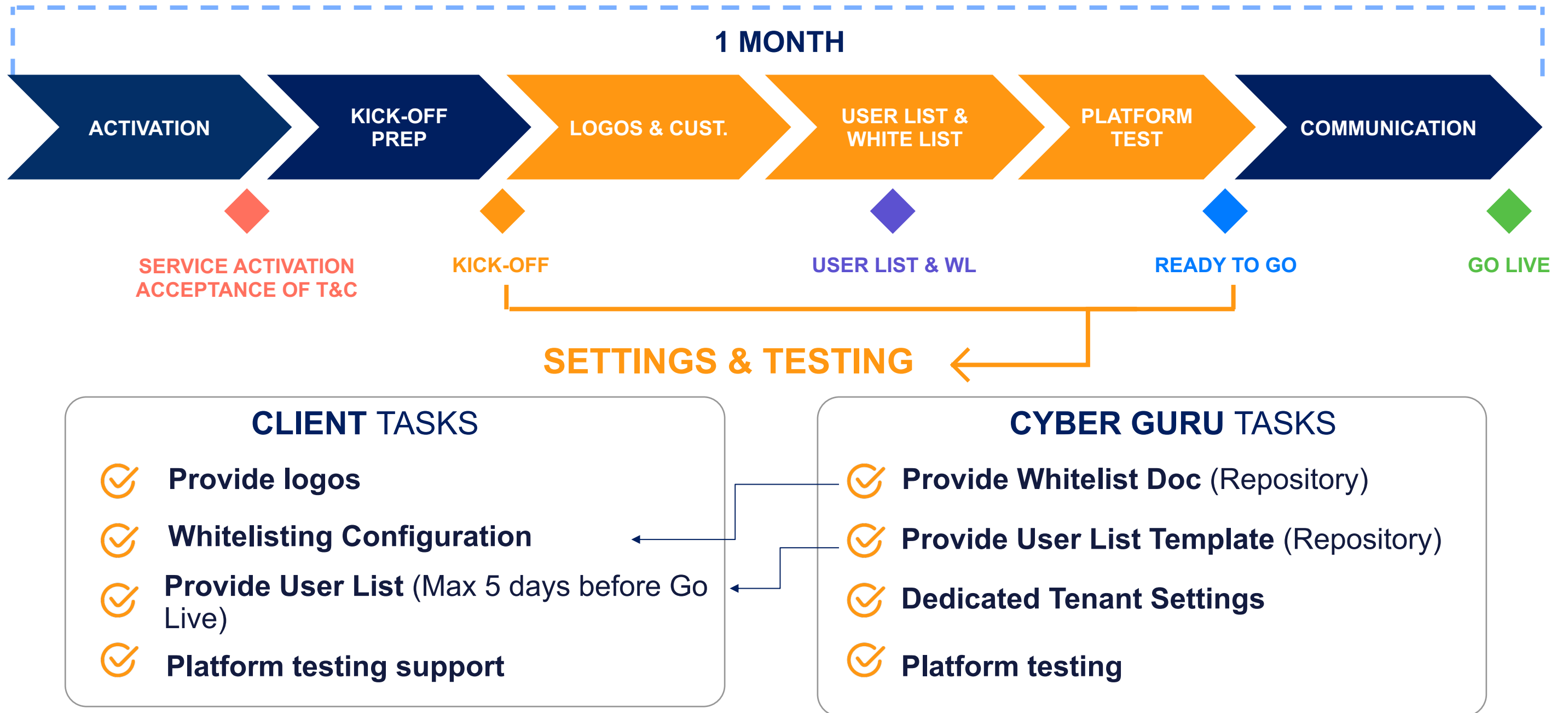
OnBoarding: checklist



- ✓ **Contact person during onboarding**, access to the document repository and follow up
- ✓ **Names** for supervisor access to the platform
- ✓ **Detailed statistics** with names
- ✓ **Client subdomain** for creation of dedicated tenant
- ✓ **Required languages**

- ✓ **Gamification (strongly recommended)**
- ✓ Monitored video with blocked progress bar
- ✓ Ranking closure (by level/year or at the end of all years)
- ✓ Go Live date
- ✓ Schedule releases within the license expiration date

OnBoarding: checklist



OnBoarding: GO LIVE



CLIENT TASKS

- ✓ Internal communication for program launch

CYBER GURU TASKS

- ✓ Upload User List to platform
- ✓ Go Live

Training Access



HELP DESK FOR USERS

support@cyberguru.eu



USER LIST UPDATES

To be provided in standard format within **5 working days** before Go Live



GO LIVE

Go Live dates and subsequent releases must be scheduled at least 5 business days in advance of date



REPORTING

Reporting is standard pursuant to platform



FOLLOW UP

Follow up meeting



Cyber Guru Phishing

Onboarding Procedure

How to turn employees and contractors into your organization's first line of defense

www.cyberguru.io

CG Phishing Overview

Breakdown of year

12 CAMPAIGNS

Each campaign consists of **10 templates**; with the first 3 campaigns, the A.I. engine studies the behavior of the individual recipient to calibrate the level of subsequent mailings.

3-4 WEEKS

The **standard duration** of a single campaign is 3-4 weeks.

SENDING CAMPAIGN

Template sending is random by time of sending, type of template sent and users affected.

DASHBOARD & ANALYTICS

The **Dashboard** available on the platform highlights the progress of campaigns, the distribution of weak/strong users for each campaign and numerous other metrics.

REMEDIATION

Based on what statistics reveal, one can decide to launch a campaign aimed at a cluster of users in order to reinforce the level of resistance to attacks. We recommend a few **remediations** after **7/8 campaigns**.

Types of users:



Weak user:

These are users that tend to regularly open emails and click on links.



Strong user:

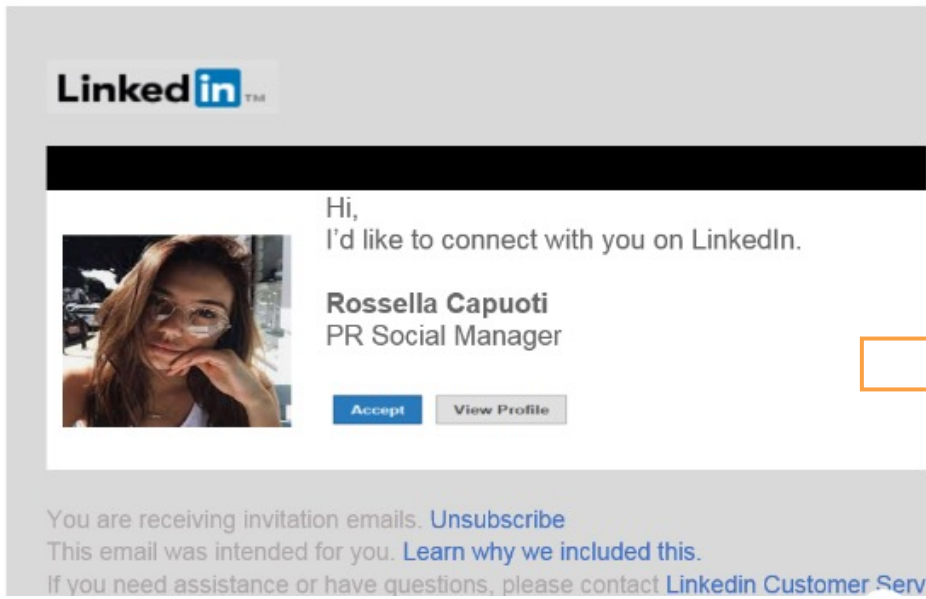
These are the users that tend to open emails but not click on links.



Defender:

These are users that, not only do not fall for the phishing attacks, but also report them following the set procedure.

CG Phishing Overview



The landing page has a dark red background with a repeating pattern of icons: a magnifying glass, a laptop with a padlock, a bell, and a document with a checkmark. It features three main white boxes:

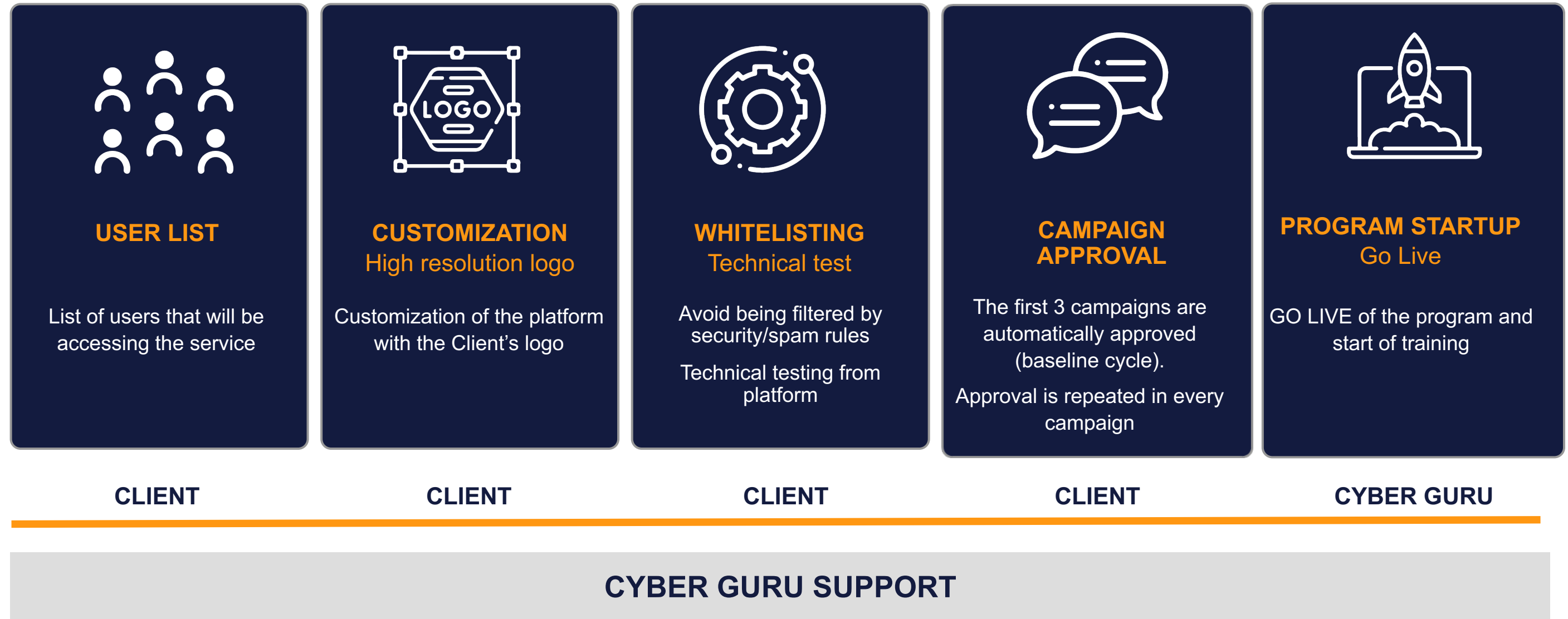
- ACME CORPORATION**
Warning: simulation of a real attack!
An illustration of a hacker with a laptop and binary code (0s and 1s) around them.
Text: "You clicked on a link in a message that simulates a phishing attack. This is a tutorial to raise your awareness and help you recognise real threats"
- Make a note of these suspicious signs**
 -  The sender is posing as an organisation official (from the HR Team), but the email address (HR@human-resource.tech) is not an internal one
 -  The email refers to a general business event, without giving any details about it
- You can learn more about the topic by watching this video**
A video player showing a video titled "WHAT IS PHISHING AND HOW TO AVOID IT". The video player has a play button, a progress bar at 01:30, and various control icons. The video content shows a computer monitor with a fishhook icon and a person icon.

Powered by 

Clicking on the link in the phishing email will take the user to a landing page with information on phishing hints that the user should have noticed and an educational video.

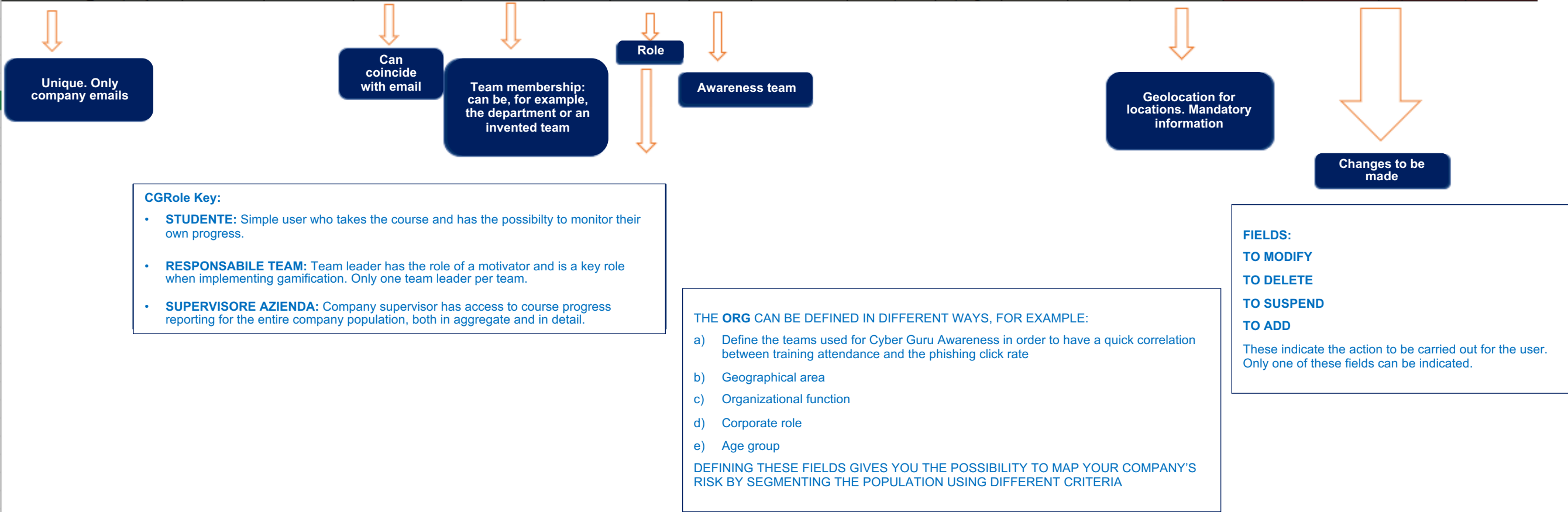
Onboarding Process

Operational Aspects



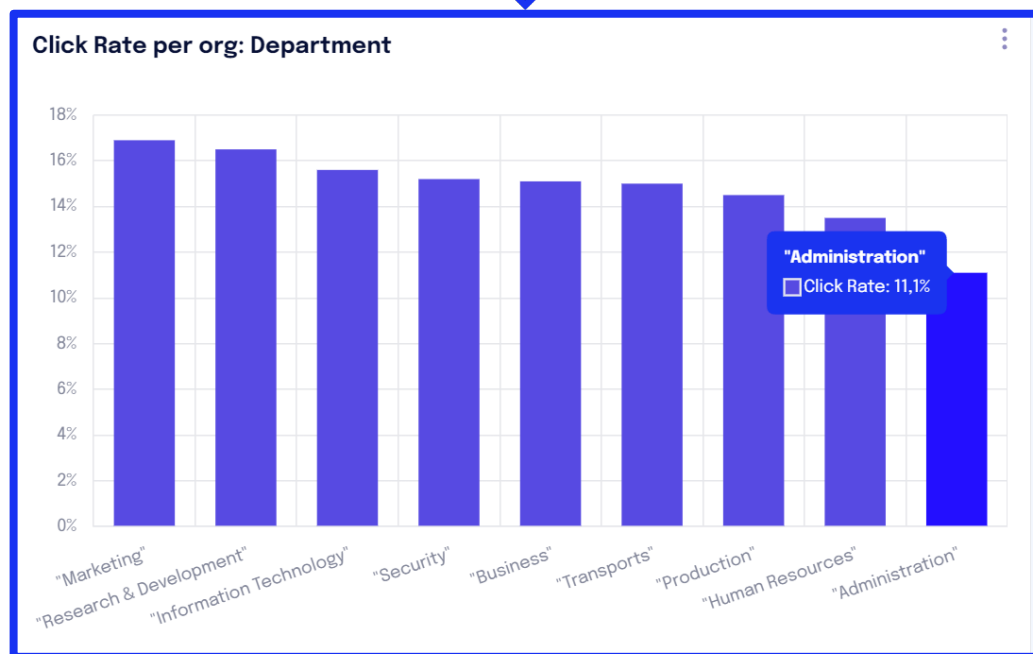
User List Template

COMMON				AWARENESS/CHANNEL			PHISHING						POST GO LIVE (USER LIST UPDATE)				
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	Country*	To modify	To delete	To suspend	To add
john.smith@company.com	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
mario.rossi@company.com	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
marco.lucini@company.com	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
bill.gates@company.com	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
elon.musk@company.com	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogna	Barcelons	ES		delete		
warren.buffer@company.com	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Developer	Impiegato	Lombardia	Milan	IT			suspend	



Mapping business risks by Org

COMMON				AWARENESS/CHANNEL			PHISHING							POST GO LIVE (USER LIST UPDATE)			
Email	firstname	lastname	username	Team	lang	cgrole	Org_1	Org_2	Org_3	Org_4	Org_5	Org_6	COUNTRY*	To modify	To delete	To suspend	To add
John.Smith@company.com	John	Smith	John.Smith	Red Team	it	Studente	Red Team	Marketing	CFO	Dirigente	Lazio	Rome	IT	modify			
Mario.rossi@company.com	Mario	Rossi	Mario.Rossi	Blue Team	it	Studente	Blue Team	Sales	CEO	Dirigente	Lazio	Rome	IT				add
Marco.lucini@company.com	Marco	Lucini	Marco.Lucini	Red Team	en	Supervisore Azienda	Red Team	Production	Inbound	Impiegato	England	London	UK				
Bill.Gates@company.com	Bill	Gates	Bill.Gates	Red Team	de	Team Leader	Red Team	Research & Development	Developer	Quadro	Illinois	Chicago	US	modify			
Elon.Musk@company.com	Elon	Musk	Elon.Musk	Yellow Team	fr	Studente	Yellow Team	Research & Development	Developer	Quadro	Catalogna	Barcelon	ES		delete		
Warren.buffer@company.com	Warren	Buffer	Warren.Buffer	Yellow Team	es	Studente	Yellow Team	Administration	Junior Developer	Impiegato	Lombardi	Milan	IT			suspend	



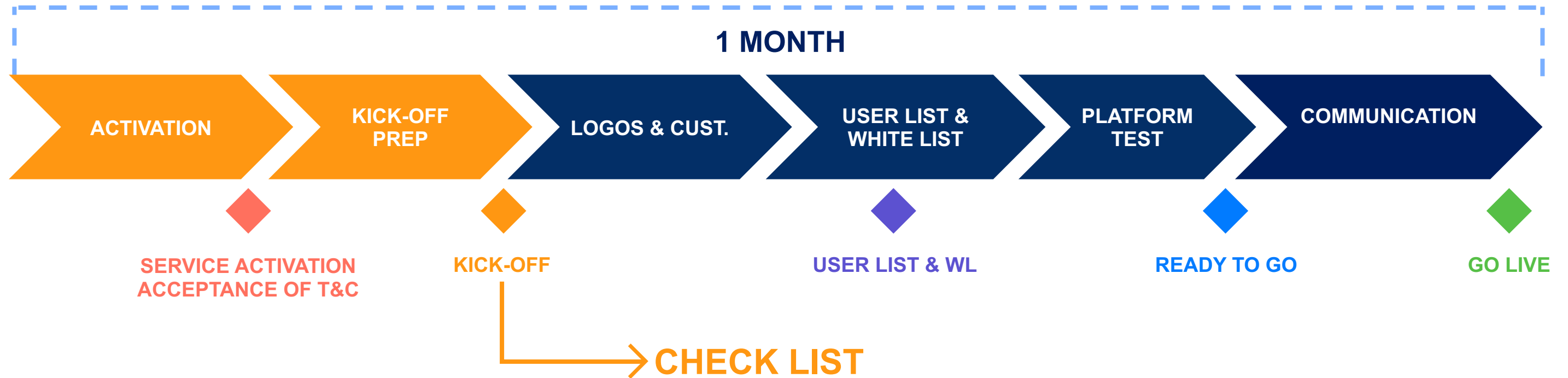
Master Plan



Service is active from the date of service activation notice (irrespective of Go Live).

Onboarding is recommended within a month of service activation in order to maintain an adequate cognitive load and effective learning.

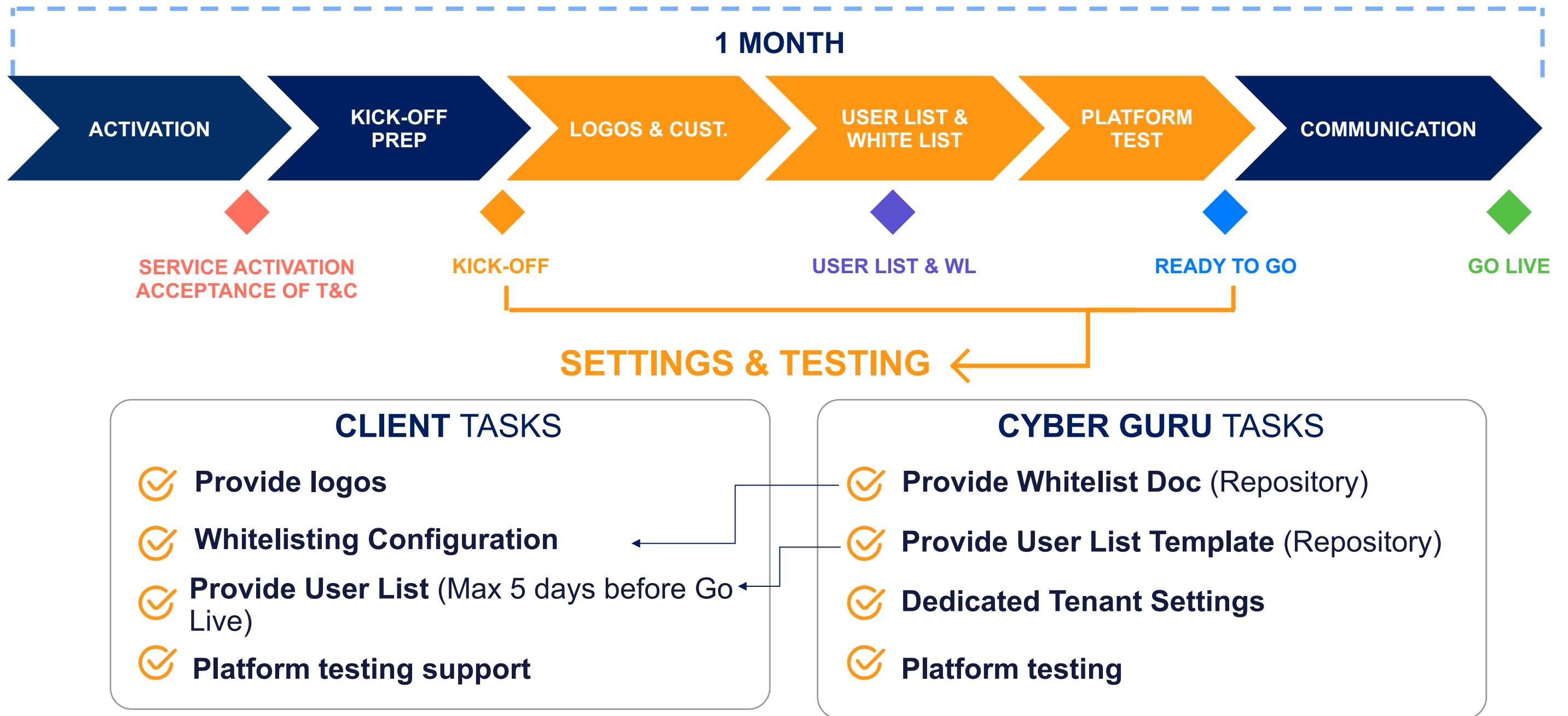
OnBoarding: checklist



- ✔ **Contact person during onboarding**, access to the document repository and follow up
- ✔ **Names** for supervisor access to the platform
- ✔ **Detailed statistics** with names
- ✔ **Client subdomain** for creation of dedicated tenant

- ✔ **Languages and countries requested**
- ✔ **Go Live date**
- ✔ **Schedule releases** within the license expiration date

OnBoarding: settings and testing



OnBoarding: GO LIVE

1 MONTH



CLIENT TASKS

- ✔ Approval of Baseline campaigns

CYBER GURU TASKS

- ✔ Upload User List to platform
- ✔ Go Live

Delivery of phishing campaign





**Cyber
Guru**

PhishPro



USB ATTACK

Carry out **simulated phishing attacks** through the use of **USB flash drives**.



QR CODE ATTACK

Carry out **simulated phishing attacks** through the use of **QR Codes**.



ADAPTIVE LEARNING REMEDiation

Carry out **Adaptive Remediation actions**: offering users **dedicated educational content**.

USB Attack



Objective:

Carry out **simulated phishing attacks** through the use of **USB flash drives**

Features:

- Supervisors will be able to enhance anti-phishing training by creating a USB flash drive containing a "malicious" file
- Each time the file is opened, a report will be supplied in the Remediation Dashboard where the number of times the document has been opened will appear.
- The execution of the Word macro will trigger the name capture of the Host (it will be recorded that the user not only inserted the USB flash drive into the device, but also agreed to run the macro, thus an additional exposure to cyber risk with a particularly dangerous security action).



Qrcode Attack



Objective:

Carry out **simulated phishing attacks** through the use of **QR Codes**

Features:

- Supervisors will be able to expand anti-phishing training by creating "malicious" QR codes.
- The QR Codes will be printed and distributed within the organization.
- People who scan and agree to open the link in the QR Code will be redirected to a dedicated landing page where they will be asked to provide sensitive information such as their name and email.
- Each time a QR Code is scanned, a report will be supplied in the Remediation Dashboard. This report will indicate scans and those who have submitted the additional information requested.



Adaptive Learning Remediation



Objective:

Carry out adaptive Remediation actions: providing users in need with dedicated educational content aimed at threat recognition.

Features:

Supervisors will be able to assign content dedicated to the users defined as "weak" or those who meet similar criteria, from the Remediation Dashboard to provide specific training aimed at recognizing phishing threats.






Phishpro OnBoarding



Same onboarding as Phishing

PhishPro features come in the form of 3 new “Remediations”

<p>QR Code Attack Start...</p>  <p>Generate a QR code to simulate Qishing attacks. You will receive the QR code via email</p>	<p>USB Attack Start...</p>  <p>Generate a file to copy onto a USB drive to simulate USB attacks. You will receive the file via email</p>
<p>Adaptive Remediation Start...</p>  <p>Assign dedicated and additional training content to “at-risk” students by email based on their results on phishing campaigns</p>	

Customer Success Team

What we offer



CST PACKAGE

- Kick off meeting *
- Support to check & upload first user list **
- Support for whitelisting settings
- Support for internal launch communication
- Training analysis and recommendation - Mid Term SAL*



KNOWLEDGE BASE (DOCUMENTATION)

- Onboarding
- Product
- Technical



DEDICATED CST MANAGER

During all service life cycle



HELPDESK

During service life cycle
support@cyberguru.eu

* *Mandatory activity*

** *Strongly suggested activity*

Customer Success Team

CST Package per purchased licenses

SIZE	XS	S	M	L	XL
CST PACK (H)	8	16	24	48	56

- License package
- Documentation
- Helpdesk
- Customer Management Service
- Regular reporting on hours balance

LEGENDA

XS Users \leq 250

S 251 < Users \leq 1000

M 1001 < Users \leq 3000

L 3001 < Users \leq 10000

XL Users > 10000



SECURITY AWARENESS TRAINING THAT WORKS!

Thank you

www.cyberguru.io