Convergent Risks

AUDIO BUSINESS
CONTINUITY ALLIANCE

Developing Security Best Practices for Localization Talent

Security Best Practice Assurance Concept

25th February 2021

AUDIO BUSINESS
CONTINUITY ALLIANCE

Convergent Risks

Localization | Security assurance and awareness for Talent and Organizations

Brief

- Provide improved security awareness for talent operating within the global localization services industry using a set of recognized easy to follow security best practices and guidance.
- Provide access to an online register for participating talent using a self attestation and validated assessment process.

Target audience

- Freelance / Contractor personnel working in a remote environment.
- Organizations managing third-party personnel working in a remote environment.

Roadmap 2021

- Q1 2021 Create Best Practice statements, Awareness and Implementation Guidance, Questionnaire and Validation
  - Draft Best Practices complete awaiting board approval
  - Create supporting information and implementation guidance
- Q1 Industry standards and control mapping e.g., TPN, MPA Best Practices, ISO 27001/2-2013, NIST SP 800-53 (Rev. 5), DPP Committed to Security.
- Q3 Beta Launch of the ABCA registry platform.

Localization | Security assurance and awareness program – Talent

Types of Remote Working – Third-Parties

- Non-local (e.g., Cloud-based applications and environments, VPNs and Virtual Desktop Infrastructure).
  - Remote Worker.
- Local (content is hosted in a physical environment, e.g., stored on external encrypted hard drive, local HDD).
  - Remote environment.
  - Remote Worker

Localization use cases – Remote Environments

- Translation (Transcript, Proofreading, QC, Dubbing Script/Bible).
- Subtitling (i.e. Closed Captioning, SDH and HOH, Text and Metadata).
- Dubbing (i.e. ADR).
- Graphics (i.e. titles, end cards).

Areas of focus

- Talent Management.
- Security Awareness.
- Policy and Process.
- Environment Management.
- Media Asset Management.
- Information Technology Asset Management.
- Account Management and Authorization.
- Device Security.
- Application and Software Security.
- Digital Asset Management.

AUDIO BUSINESS
CONTINUITY ALLIANCE

Localization | Security assurance best practice topics – Talent

Convergent Risks

Management Systems

No.	Topic	Best Practice
LOCT-MS-1	Talent Management	Users should provide appropriate pre-employment screening and/or background check information (*where permitted and applicable by local law*), and be required to sign a non-disclosure agreement (NDA) or confidentiality agreement prior to accessing client assets.
LOCT-MS-2	Security Awareness	Users should undertake basic security awareness including how to respond in the event of incident and reporting before being granted access to client assets. Training and awareness undertaken should be recorded.
LOCT-MS-3	Policy and Process	Users will be responsible to adhere with organization’s policies and processes. Acknowledgement should be formally recorded.

Physical Security

No.	Topic	Best Practice
LOCT-PS-1	Environment Management	Users must implement and maintain procedures to ensure that physical perimeter access remains secure at all times. Ensure all content handling is in an appropriate area / environment.
LOCT-PS-2	Media Asset Management	Users must ensure assets housed on physical media (including hard copy) are physically and digitally secured by appropriate means, and a documented process for checking out/tracking assets from the premises is implemented.
LOCT-PS-3	Information Technology Asset Management	All systems authorized to receive, distribute, manipulate and store content must be provided by the client (i.e. zero client).

Digital Security

No.	Topic	Best Practice
LOCT-DS-1	Account Management and Authorization	Users must ensure decisions around the creation, secure handling and authentication of user accounts are aligned to client policy. Appropriate conditional access controls must be enforced for access to client environments.
LOCT-DS-2	Device Security	Systems must adhere to client baseline hardening, Bring-Your-Own-Device policies (as relevant), and Cyber Security hardening guidelines, not limited to: authentication, authorization, encryption, logging, and security testing.
LOCT-DS-3	Application and Software Security	All local / online applications and remote access protocols should ensure protection of client assets through appropriate authentication, authorization, encryption and logging mechanisms.
LOCT-DS-4	Digital Asset Management	Users must ensure the receipt, distribution and storage of client content is appropriately managed through client approved technical tools and techniques.

Localization | Talent

Talent Registry Two| Level concept

Validated

Target participant:

- working on Tier 1/ sensitive pre-release content.
- Access to high-sensitive A/V material.
- Questionnaire to complete. 20-30 questions
- Applicable to local and non-local remote working types.

- Response validation (evidence requirement).
- Background checks for employment and experience of proprietary tools.
- Inclusion of validation through security test (multiple choice).
- Validation through remediation management to ensure grade compliance.
- Membership awarded upon compliance validation.

Self Attested

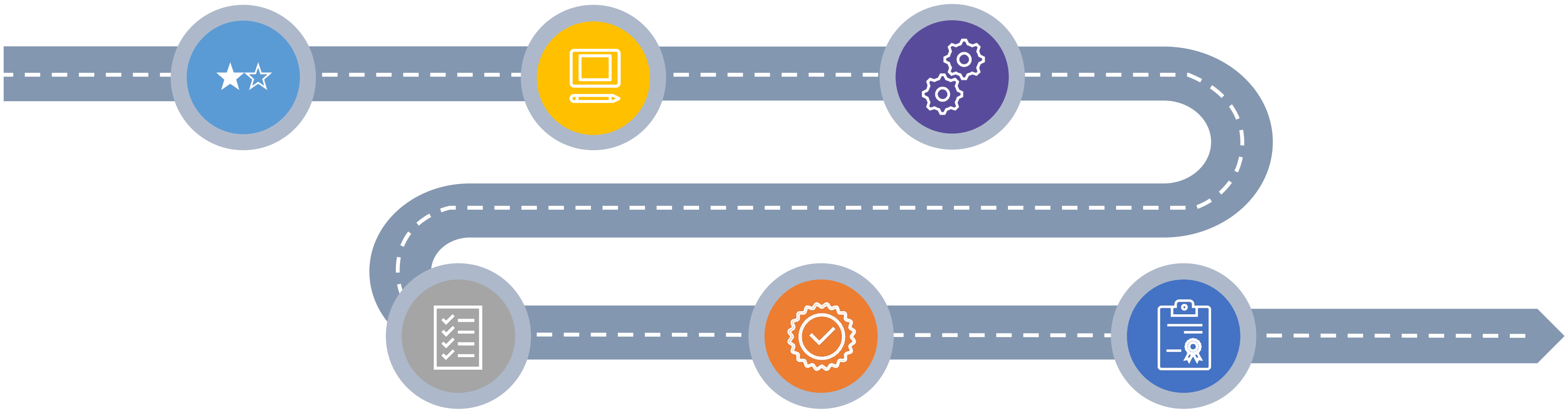
- Elementary questionnaire to complete.
- Questionnaire to complete. 20-30 questions
- Target both local and non-local remote working types.

- Anytime upgrade to Enhanced level option.
- Self-attestation response only.
- Automated security posture score.
- Membership awarded upon response submission.

AUDIO BUSINESS
CONTINUITY ALLIANCE

Localization | Talent Registry

Convergent Risks



Talent subscribes to program.

Access to online questionnaire and support materials.
Self-attestation responses.

Validation.

Result published to Talent account.

Talent Membership awarded.

Studios / Organizations access and review Talent database.

Thank You