Questions	Answers
Is Geneva Call subject to Information Security requirements expressed by auditors, partners, or authorities in the countries it operates?	We do not have any specific requirements and any alignement with existing framework is not mandatory.
How is the IT department structured ?	The IT department is composed of only two people internally (Head of IT and IT Assistant). The technical management, support and monitoring of the tenant is done by a third party IT service provider.
The IT infrastructure	We have only one hosted server for online backups. (except for this, no Saas, No cloud based hosting). We have only one firewall in our main office. There are approximatively 200 laptops and 300 users. Mobile devices are currently not managed.
Microsoft 365 tenant	100% of our services run in one single MS 365 tenant. There are 2 or 3 applications online that we are using outside of the tenant with SSO.
Please clarify the expectation behind the following objective stated in the RFP: "Evaluate existing security controls, policies, and practices aligned with NGO's requirements".	We expect the IT security Audit to be aligned with the NGO standards (not with private companies standards) and to take in conideration the specificities and challenges specific to our type of business.
Do you have expectations on the format of the audit report between a maturity assessment or a gap assessment?	more a gap assessment
Who will be the responsible for the delivery of the audit at Geneva Call, and our direct contact? What will be the resources provider to the selected bidder to support Geneva Call's efforts for the delivery of the audit (*e.g.,* identification of contacts and documentation, schedule of interviews)?	the IT team (head of IT and IT assistant) and the external IT provider will be available to answer all questions and provide with the needed documents (if available). Interviews with other people could be organised (e.g. Head of Security, Directors, etc..), which will be defined at a later stage
What is the expected range period for the IT Security Audit to take place? Is there a deadline or an opportunity to consider for the report's conclusions sharing and optional presentation?	we would like to start the IT security audit as soon as possible after the signature of the contract.
Is it possible to get an overview of the M365 services currently subcribed	Most of the users have Microsoft Business Premium Licenses, enrolled with intune. We are not using Purview
Do you have an idea of the budget allocated for this IT security audit ?	this information is not provided
Will we have to perform our assessment during business hours in Switzerland, or should we consider other time zones, such as the regions of the world your organization operates in, as part of the service?	The assessment can be performed at your convenience, during the business hours in Switzerland.
In the section "Objectives of the Audit", point 4, you mention a "practical, prioritized roadmap of security improvements". Should this roadmap be focused on technical elements, on general governance or a mix of both?	a mix of both. Anything that would allow us to improve in our overall IT security
Are the references to be delivered on demand (III, point I) or with the proposal (section E)?	Reference should be delivered with the proposal
Could the service be performed remotely or does it have to be done on-premises in Geneva?	The service could be performed remotely but we expect at least one in persor meeting
In which language should we deliver the offer ?	English only
Is there an existing tool for risk and compliance management?	no, you can provide your own if needed.
In the first point of the section "Objectives of the Audit", you mention that you would like us to identify key security risks and current vulnerabilities of your IT environment. Would you prefer us to do a full scan of your perimeter or us to provide you with a declarative report?	We would prefer to have a declarative report, solutions based.
12.In the "Technical Controls (High-Level Reviews)" section, you mention the production of "high-level reviews". Could you please elaborate a list of your requirements for a review to be considered as "high-level"? Would a vulnerability scan be enough or should we install agents and investigate further?	A vulnerability scan would be enough
Could you tell us whether we ought to focus only on the Azure tenant level or if we ought to review the Entra ID policies in their entirety?	The focus should be on the Azure tenant level.
Under Technical Controls: is the list of topics per domain - e.g. firewalls, segmentation, remote access for Network Security - to be understood as scope or should the assessor include additional relevant topics?, e.g. Internet Access Controls, Network DLP Controls, etc. for Network Security	The provided Technical Controls can be viewed as a scope, we are of course welcoming your expertise to propose additional relevant topics if aligned with current infrastructure. The scopes and additional propositions would be reviewed and defined prior to the start of the audit task
Is the "Incident Readiness" scope limited to Security Incident Management or IT Incident Management in general?	IT Incident Management in general