# Annex 19: Standard Operating Procedures

## Prosperity Fund Evaluation & Learning Team

October 2017

**HM Government**

**Prosperity Fund**

Evaluation & Learning services delivered by:

wyg. LTS INTERNATIONAL INTEGRITY

# Contents

| Document Title | EL Prosperity Fund Standard Operating Procedures | | |
|---|---|---|---|
| **Document Title** | **WYGB9-INC-7-02** | **Revision** | **1** |
| | | | |
| **Revision** | **Written By** | **Checked By** | **Approved By** |
| Revision 0 | Lara Johnson | E. Snedden, W. Short, T. Pragasam, P. Abbott | PFMO |
| Revision 1 | W. Short | E. Snedden | PFMO |
| Revision 2 | | | |
| Revision 3 | | | |
| Revision 4 | | | |
| Revision 5 | | | |

This report was prepared during the inception phase of the Prosperity Fund Evaluation and Learning contract. It forms an annex to the main Inception Report.

It was produced and approved by the Prosperity Fund Management Office before the main Inception Report and Workplan were finalised and agreed.

If there is any inconsistency between this annex and the main Inception Report and Workplan, the main Inception Report and Workplan provides the agreed position.

# Purpose of SOPs

The purpose of the Standard Operating Procedures is to ensure a consistent level of performance, efficiency and quality in project delivery across key areas of PF E&L work. The SOPs are a set of step-by-step instructions that ensures implementation in accordance WYG policies and business practices (in line with WYG's Commercial Development & Operations Process, CDOP) and procedures specific to the Prosperity Fund EL team. This document is intended to be used as a reference point for all team members regarding operational matters.

# 1 Work packages for programme evaluations

## 1.1 Production of deliverables and QA process

The EL team operates a five-stage approach to the quality assurance (QA) of both internal team work and contractual deliverables for the PFMO. Internal team work can include data collection tools, meeting minutes, templates, matrices and papers intended for the internal use by the team. External deliverables include all those defined outputs (agreed between the PFMO and WYG) which are captured as contractual deliverables. It is the team's responsibility to produce these to the satisfaction of the PFMO. Table 1.1 below presents the QA process for different types of deliverables and the responsible team members involved.

*Table 1.1 – QA Process*

| QA Stage | Responsible Team Member | EL Deliverables | Description |
|---|---|---|---|
| 1 | Responsible Workstream Director | All deliverables | Each workstream director oversees and quality assures the work of respective team members to ensure that deliverables meets the technical requirements of the terms of reference. |
| 2 | Technical Reviewer | Evaluation reports | The technical reviewer subjects draft written evaluation reports to review using the EQUALS QA template for an entry level or exit level evaluation product. The reviewer scores the evaluation product in the same way as a EQUALS review would, making comments on the template and within the report document itself. |
| 3 | Team Leader | Deliverables for PFMO and external audiences (reports, presentations) | The Team Leader reviews the evaluation product independently of the Technical Reviewer at both draft and final stage.<br><br>Upon completion, the Team Leader and Technical Review compare scoring and notes to form one consolidated set of comments which they feed back to the responsible Workstream Director and Lead Expert. |
| 4 | Project Director | Deliverables for PFMO and external audiences | Once the Project Director is satisfied that all of the outstanding actions have been addressed, the evaluation product is then submitted to the PFMO for review, comment and QA. |
| 5 | PFMO/ EQUALS | All deliverables submitted to the PFMO | The PFMO reviews and comments on submitted deliverables. This may involve the feedback of a peer reviewer from EQUALS.<br><br>Upon receipt of the PFMO / EQUALS comments, Stages 1 to 4 are repeated as necessary. |

## 1.2 Change and variation control

Change is any alteration (additions or omissions) to the scope of work, the timescale in which work is completed, quality and cost. Variation means any contractual change with financial implications for the project. Change and variation control is therefore key to successful technical and financial delivery. At the centre of our approach to change-variation control is keeping an up-to-date log of all variations and their authorisation status and communicating agreed actions to the EL team.

The change and variation control process is:

1. A change is identified and then submitted to the Project Manager. In the event of a change within a single work package, the Team Leader should submit the change request to the WYG Project Manager. Should the change affect the scope of work previously agreed with the client, the WYG Project Manager should submit a change request to the PFMO Deputy Head of MREL.
2. The WYG Project Manager internally assesses the change, considering what would be the outcome if the change were not implemented and what would be the impact on time, quality and cost if it were implemented. He will escalate to the PFMO Deputy Head of MREL as required.

3. The WYG Project Manager provides a recommendation to the WYG Project Director on whether to approve, reject or defer the change. All variations should be confirmed with the relevant authority in writing and copies of authorisation for the changes saved in the project folder. Internal project changes will be recorded on the project change register and external changes will be recorded on the project decisions log (both maintained by the project manager). Changes which affect the contractual cost will be handled through a signed and approved variation order with the client or a contract amendment letter to the relevant sub-contractor.
4. The WYG Project Manager then communicates the changes to those involved.

The WYG Project Manager will maintain an internal log in Excel listing the changes, date logged, description and effect on delivery, and if appropriate a unique variation number. In addition, a separate decision log shall be maintained detailing any project decisions made affecting the PFMO and will be reviewed at the monthly contract review meeting,

*Table 1.2 – Change Register*

| Change No. | Change Type | Requestor | Description | Date | Approver | Approval Status | Comments | Variation Number |
|---|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

# 1.3 Design of costed work packages

The EL team will define a robust and methodical process for designing packages of programme evaluation works. Where possible, as part of the inception phase the EL team will agree these work packages with the PFMO for evaluations to be performed as part of the implementation phase.

The key team members inputting to the work package design will be the Project Manager, the three Workstream Directors, the Ops Coordinator and Finance Project Coordinator. The workplans will primarily be prepared by the WYG Project Manager in collaboration with the other team members and then must be approved by the responsible workstream director and the WYG project Director. WYG Finance will also be consulted to ensure that the costed design is within the overall project budget.

WYG intends to use a bottom up estimating approach, guided by the overall EL resource envelope, whereby available information will be used to cost each component to develop an overall cost for each work package. This will be done by an analysis of the level of effort required to deliver each aspect of the work package. Each workstream will have an individual cost. Additionally, the cost of expenses will be estimated based on the number of people and the likely number of trips and location required. This approach will allow each programme to be costed using a summation of the total of the programmes individual workstreams.

Also of importance in the design of the work packages is the agreement of deliverables and timetables for the evaluation. This will be done through agreement with PFMO of the deliverables required under each work package and the schedule for these to be delivered by.

The costed workplan design will comprise an MS Excel based cost model and a MS Project based plan. The plan will show deliverable dates at the workstream level within the programme. This can be rolled up to show the overall EL PF implementation plan.

The EL team realises that the potential staggering of PF programmes means that a rolling evaluation approach will likely have to be adopted which means that the design of work packages will likely not be fully completed at the end of inception and as such further work will be undertaken throughout the life of the EL contract to design packages as and when they are needed.

# 2 Research Code of Conduct and Ethics Policy

This chapter sets out requirements, advice and guidance in relation to good research conduct and practice. This includes the research ethics policy and procedure and receiving and documenting informed consent.

In the context of our EL activity, our Professional Code of Conduct, which is aligned to the UKES Guidelines for Good Practice[1], ensures that we always:

- Meet our obligations to society in terms of adherence to the highest standards of integrity and transparency in the collection analysis and synthesis of data and the impartial assessment and dissemination of findings.
- Meet our obligations to subjects by protecting them from undue harm arising as a result of their participation in research. This requires that subjects' participation is voluntary and fully informed.
- We strive to ensure equality in all our research and that no group is disadvantaged by being excluded from consideration.
- Communicate findings openly and that findings are not misleading or misrepresented by omission.
- Respect and uphold human rights.

WYG's commitment to ethical business is enshrined in our published Ethics Policy. This is provided to all staff and associates and adherence is required by all WYG contracts. The policy is overseen by the Ethics Committee which consists of senior WYG executives and reports directly to the company board. It is responsible for all ethical aspects of company policy including due diligence, training, external assurance, monitoring and investigating and disciplinary actions. The Committee reports annually to the Chief Executive and the Company Report.

All our research and evaluation activity upholds the principles of research ethics set out in the DFID Ethics Principles for Research and Evaluation[2]. Our approach to operationalising these principles is as follows:

- All our work is in accordance with international human rights conventions and covenants regardless of the operating country.
- We accept responsibility to gain ethical approval where necessary/ appropriate.
- While seeking participation by implementers, stakeholders and beneficiaries/ end-users in the evaluation process, this is not at the expense of our independence. Objectivity is paramount in our work and we will clearly document the roles of all actors to ensure transparency and integrity in our evaluations.

Generating learning with clear developmental and practical value is at the heart of all WYG's evaluations. To the extent possible, we strive to achieve external validity in all our evaluation work. WYG is committed to wide dissemination of our evaluation outputs in line with PFMO expectations.

Regarding our responsibilities to evaluation contributors:

- We ensure that all contributors are fully informed of the evaluation purpose, measures to ensure anonymity, and of their right to withdraw.
- In cases where it is necessary to include children or young people, informed consent from the child and a responsible adult will always be sought.
- Our approach preserves the confidentiality of evaluation contributors. We do not name individuals in our outputs and all data is anonymised and presented in aggregate form.

Regarding inclusion, cultural and conflict sensitivity:

- An intrinsic 'do no harm' approach underpins all of our evaluation assignments.
- We are committed to achieving representation and an inclusive approach in all our evaluation work, striving to ensure the voice of the full spectrum of stakeholders, beneficiaries/ end-users (including marginalised groups) is heard. Incorporating beneficiary feedback is a key in our evaluations, and a cross-cutting facet of all our evaluation work.

---

1 https://www.evaluation.org.uk/index.php/news-resources/ukes-publications/46-ukes-guidelines-for-good-practice-in-evaluation

2 https://www.gov.uk/government/publications/dfid-ethics-principles-for-research-and-evaluation

- Our approach respects cultural sensitivities.

# 3    Data Management Protocol

## 3.1    Data protection and use of personal information

### Responsibilities for storage, management and transmission of data

This Data & Information Security Protocol defines the roles and security requirements for users of information services (including IT) for the EL team and how it complies with the Digital Service Standard, Security Policy Framework and Data Protection Act. It outlines our approach to the appropriate storage, management and transmission of Prosperity Fund evaluation-related information.

HMG is responsible for ensuring that all information shared with the EL team is done in accordance with internal HMG policies and standards. WYG as the EL prime contractor is responsible for ensuring that all information gathered by the EL team is stored and accessed in compliance with HMG standards. Users accessing PF information will be required to demonstrate compliance with this policy, and can be held personally liable for its breach.

> **Box 1: Government Security Classifications, 2014**
>
> *"Everyone who works with government has a duty to respect the confidentiality and integrity of any HMG information and data that they access, and is personally accountable for safeguarding assets in line with this policy"*

Table 3.1 sets out the responsibilities for organisations and individuals to adhere to the agreed protocols.

*Table 3.1 – Responsibilities for data management*

| Role | Responsibilities |
|---|---|
| HMG sources | • Follow HMG and specific departmental policies and standards<br>• Help define appropriate level of access / privileges |
| WYG | • Accountable for EL programme data and information security |
| Organisations responsible for contracting EL team members (WYG and its sub-contractors) | • IT infrastructure security<br>• Security Policy deployment (including mobile devices)<br>• User training, guidance, information security best practice<br>• Respond to emergency IT security incidents |
| Individual users | • Attend user inductions, refresher training<br>• Comply with all policies and guidance<br>• Report known or suspected information security breaches / risks |

### HMG classification policy and security clearance

HMG operates a Classification Policy to identify and value information according to its sensitivity and to drive the right protections. It comprises three levels: OFFICIAL (most day-to-day business of government), SECRET and TOP SECRET (typically requires bespoke sovereign protection). Information with an OFFICIAL classification can be managed by commercial solutions that mitigates the data and information risks faced.[3]

These levels of classification are outlined in Table 3.2, overleaf.

---

3 HMG Security Policy Framework, 2014 - link

*Table 3.2 - HMG Security Classifications*

| OFFICIAL | SECRET | TOP SECRET |
|---|---|---|
| Most information created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stolen or published in the media, but are not subject to a heightened threat profile. Does not require sovereign protection. | Sensitive information that justifies heightened protective measures to defend against determined and highly capable threat actors. For example, where compromise could seriously damage military capabilities, international relations or the investigation of serious organised crime. Requires sovereign protection. | HMG's most sensitive information requiring the highest levels of protection from the most serious threats. For example, where compromise could cause widespread loss of life or else threaten the security or economic wellbeing of the country or friendly nations. Requires sovereign protection. |

There are four levels of UK Government security clearance: Baseline Personnel Security Standard (BPSS), the Counter-Terrorism Check (CTC), Security Check (SC) and Developed Vetting (DV). The PFMO should confirm if the EL team need a level of clearance to be able to receive / access relevant documents.

### *Information storage and security*

The EL team accesses HMG documents and files in five ways:

- from public domain repositories (e.g., DevTracker, Results for Development (R4D), HMG department websites);
- when HMG departments share them directly with us;
- when PFMO or PF Project Managers shares them with us;
- when shared by and between EL team members;
- when we access information held by the M&R service provider.

To maximise availability of information to approved users, assured, commercially available products will be used to store electronic programme information that are compliant with a) The Data Protection Act and b) the ISO/IEC 27000 family.[4] Security policies and ISO compliance can be accessed for the products we are using for project management (Podio[5]) and for file storage (Dropbox for Business[6]).

Whilst these controls cannot absolutely assure against the most sophisticated threats, they provide robust and effective protections that make it very difficult and expensive to illegally access OFFICIAL/sensitive information.[7]

In addition to using compliant systems, and providing training and support to team members, we also add a layer of security to computers with access to large volumes of programme documents using encryption, conditional access,[8] configuration policies, remote administrator access, and mobile device security policies. Devices that meet these criteria can access approved systems. WYG has included confidentiality clauses in all contracts with sub-contractors and associates.

Physical data and information security measures adopted by the EL team are fourfold:

- physical destruction of copies of personal information – paper documents should be shredded and memory devices (e.g. USB sticks) must be rendered permanently unreadable;
- a 'clear desk policy' to avoid accidental information leakage;
- controlled access to any premise(s) used to carry out EL work; and
- system-level password requirement when devices are left unattended.

---

4 ISO 27001: Information security management systems - link
5 Podio security information, and Security White Paper can be accessed here - link
6 Dropbox security and compliance information - link
7 p.14 Government Security Classification, Apr 2014 - link
8 minimum system-level requirements for documents or email to be accessible.

*Information sharing between EL and MR teams*

The EL team collaborates with the Prosperity Fund Monitoring and Reporting (M&R) service provider to deliver the PFMO contract. The MR team manages a web-based solution (the 'Observatory') to store HMG data and information relating to the Prosperity Fund. The Observatory is being designed to be compliant with PFMO, HMG, Communications-Electronics Security Group (CESG) policies, standards and principles.[9]

The EL team has role-based access[10] to the Observatory, and is responsible for safeguarding access within the EL team, who transfer them to EL systems. EL hold accountability for all information and documents in its systems. To minimise risk, access is provided in a limited way to ensure users only have access to the information necessary for carrying out their duties.

Information shared with the EL team will be treated in accordance with its classification, and stored using the programme's approved systems (Dropbox for Business, Podio). Approval from EL is required on a case-by-case basis to store PF materials outside these storage and communication systems. Using alternative storage or communication systems without approval is considered a breach of contract and EL policy.

## 3.2    Stakeholder management architecture

## 3.3    File-sharing architecture

WYG has provided the EL team a facility via Drop Box for Business for the storage and archiving of evaluation content. The general architecture of the team Drop Box is split into three distinct categories which are further sub divided:

1.  Programme Documents – This includes all business case related information for the Prosperity Fund programmes and includes PFMO generated content as well as consortium analysis. It is the repository for team members to access information relating to the programmes they are evaluating.

2.  Work in Progress – This is split between the Inception and Implementation phase and then sub divided by workstream to ensure that all deliverables to PFMO are filed in an easy to access place for the appropriate team members.

3.  Reference – Contains all non-programme or WIP information for the EL team including administration (timesheets, templates, plans), PF general information (on countries, sectors, themes etc.), EL general information.

The architecture of the team Drop Box is designed by the Project Manager to ensure that all members of the consortium team have timely and accurate access to the information required to carry out effective evaluations and the management team have confidence that information is being managed in a way conducive to ongoing rolling evaluations and is capable of withstanding changes in team organisation.

## 3.4    File-naming conventions

The purpose of file-naming conventions is to ensure that all documentation produced or gathered is named in a coherent and consistent manner and strict revision control is adhered to. This applies to three categories of files:

1.  Deliverables produced by the EL team for the PFMO in the delivery of the Prosperity Fund evaluations;
2.  Internal working documents generated within the EL team; and
3.  (External) documentation gathered by the EL team.

### 3.4.1    Client deliverables

*Storing client deliverables*

All files relating to the deliverables are to be stored on the EL team dropbox in the *2. Work In Progress* folder.

---

9 As advised by PA Consulting, the M&R service provider.

10 Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the information needs of individual users (eg access is to perform a specific task, such as view, create, or modify a file).

There are separate sub folders for Inception and Implementation and within these there are folders for each unique workstream to ensure that all deliverables are stored in a logical way for ease of location.

Within the workstream folder the final version should be saved as both a MS Word document and a PDF in a sub folder named *Final As Submitted* – this ensures there is no confusion as to what will be submitted to the client.

Upon completion and QA of a deliverable when it is ready for submission, the WYG Project Manager will submit the document to the client. No other team members should submit deliverables to the client unless express prior permission is given by the Project Manager or Project Director.

### *File-naming of client deliverables*

Dropbox has a limitation in that the number of characters should be below 260 to sync with the system. Therefore, a concise alpha-numeric file naming system will be implemented. This enables both the EL consortium and the PFMO to file documents in a consistent manner.

This system will have 5 components and take the following form: WYGB09-IMP-7-01 REV 02. Table 3.3 below sets out the logic of these components.

*Table 3.3 – Client deliverable file-naming components*

| Component | Explanation |
|---|---|
| WYGBO9 | This identifies the file for the PFMO filing system and relates to the PFMO No. |
| IMP/INC | Indicates if the document refers to Inception or Implementation. |
| 7 | The workstream to which the deliverable belongs. |
| 01 | A numerical odometer of the number of documents in the workstream |
| REV 02 | This records the revision the document is at. |

Table 3.4 provides examples of what file names represent.

*Table 3.4 – Examples of client deliverable file names*

| File Name | Represents |
|---|---|
| WYGB09-INC-16-02 Rev 01 | WYG PFMO deliverable B09, inception phase, workstream 16, second deliverable at its first revision |
| WYGB15-IMP-02-01 Rev 02 | WYG PFMO deliverable B15, Implementation phase, workstream 2, first deliverable, original revision |
| WYGEL4-INC-11-01 Rev 01 | WYG PFMO deliverable EL4, Inception phase, workstream 11, first deliverable, first revision |

## 3.4.2   Internal working documents

All internal working documents are to be stored on the EL team Drop Box in the *2. Work In Progress* or *3. Reference* folders. The former is for work related to specific workstreams and the latter for other items related to team meetings, work planning and scheduling. Old drafts should be stored in a 'Drafts' sub-folder so that old versions can be saved for reference but do not clutter up the folders.

The naming of internal working documents should have the components shown in Table 3.5, using underscores between the components.

*Table 3.5 – Internal working documents file naming components*

| Component | Example | Explanation |
|---|---|---|
| Date (YYMMDD) | 171026 is 26 October 2017 | Indicates the date of the version |
| Title | PF BC Assessment | Designates what the document covers |
| Author Initials | WS is 'William Short' | Indicates the lead author |

| Initials of editor / commenter | ES edits is 'Ewan Snedden edits' | Indicates who has commented |
|---|---|---|

By way of illustration, a file named '171026_PF BC Assessment_WS_ES edits' would refer to a BC assessment undertaken by William Short on 26 October 2017 and edited by Ewan Snedden.

### 3.4.3   Documentation

All documentation gathered by the EL team are to be stored on the EL team Drop Box in the *1. Programme Documents* folder. Table 3.6 shows the four main categories of documentation and how files should be named.

*Table 3.6 – External documentation file naming components*

| Category | | File Naming |
|---|---|---|
| Fund-level documentation | | Date(YYMMDD)_Document Title_Version |
| Programme-specific documentation | Concept Notes | 1.Concept Note_Programme Name_Version |
| | Business Cases | 2.Business Note_Programme Name_Version |
| | Terms of Reference | 3.ToR_Programme Name_Version |
| | Reports | Date(YYMMDD)_Report Type_Programme Name_Version |
| Contextual information / secondary data | | Source_Data Title_Date(Year or YYMM)_Geography |
| Methods / best practice | | Source_Title_Date(Year) |

## 3.5   Process for obtaining documents

There is no central point of contact or repository within the PFMO for all Prosperity Fund-related documents at both Fund and programme level. The MEL Specialist for Data Management, Analysis and Synthesis will identify gaps in the available documentation and flag to the Engagement Support to contact the relevant stakeholders for copies of the requested files. Team members can also source documents through the Engagement Support where they identify a specific documentary gap. Team members that directly receive documentation should store in the relevant folder in Drop Box and update the documentation catalogue.

## 3.6   Stakeholder Relationship Management

WYG have implemented a customer relationship system on an online platform Podio. This system is accessible by all team members and used to manage client and stakeholder interactions. The system will store records, agendas and minutes of meetings in order to ensure that interactions with client and stakeholders are efficient and team members are not duplicating effort in their engagement with external parties.

# 4 WYG Policies

## 4.1 Anti-Bribery & Corruption Procedure

WYG have in place a formal Anti-Bribery and Corruption Policy which all our staff, associates and sub-contractors are expected to operate within. This policy ensures that WYG PLC complies with the Bribery Act 2010 both internally in the UK and wherever WYG operates worldwide.

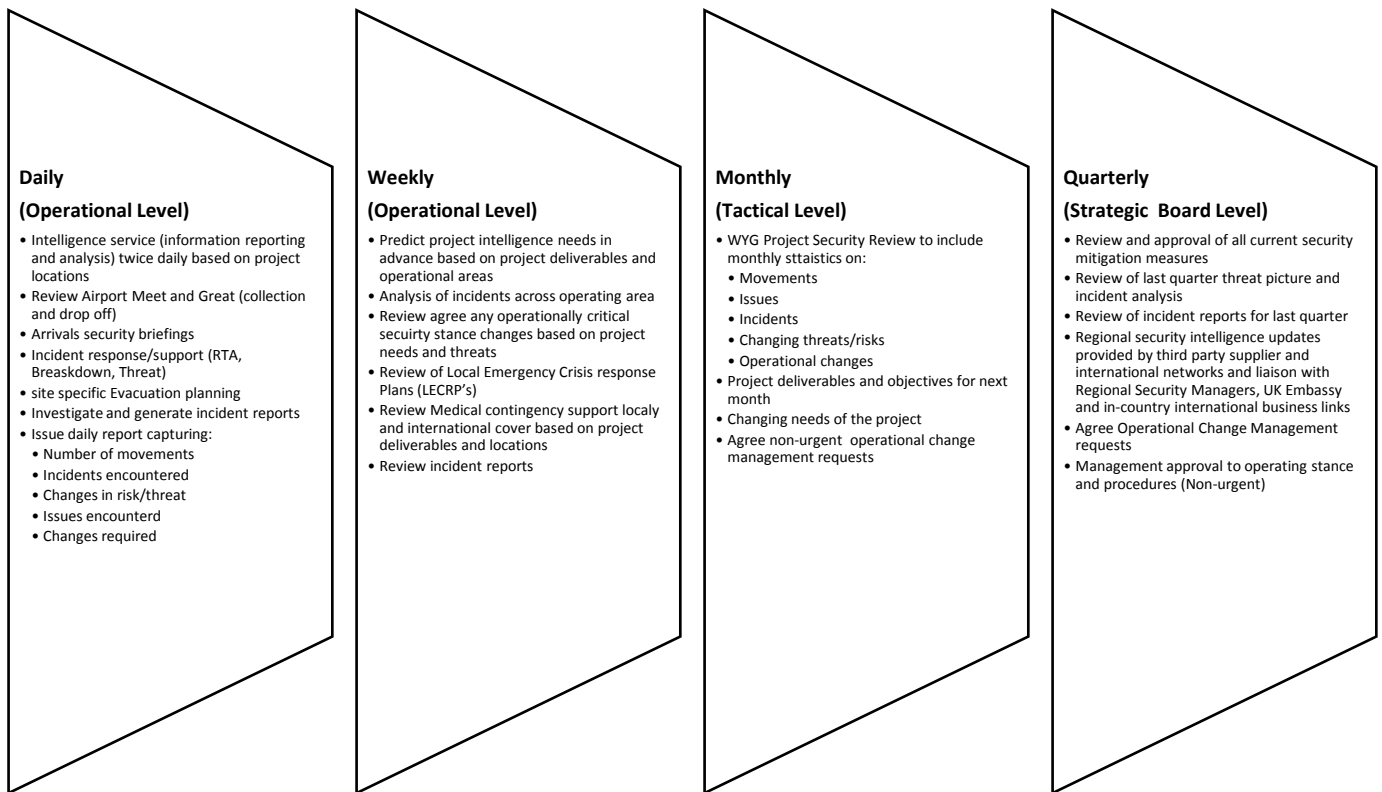The key tenets of this policy are as follows:

- We are **open**, **honest** and **truthful** with everyone but we are not confrontational, unhelpful or devious.
- We **comply with the spirit and letter of all laws**, regulations and relevant institutional and corporate standards relating to our professional conduct.
- We **do not conceal or ignore** ethical issues but deal with them robustly.
- We **willingly consult** with appropriate authorities and co-workers to resolve ethical issues.
- Whilst competing with vigour, we will **never have recourse to unethical or illegal practices**.
- We **do not offer nor will we accept individual illicit inducement** to secure work for ourselves or offer work to others.
- We **keep proper records** of our appointments and business operations and never destroy or alter such records for any improper reason.
- As professional service providers, we jealously maintain our **independence and objectivity** in all dealings with clients.
- We manage such personal and professional conflicts of interest as may arise from time to time in an **open and consultative manner**.
- We do not accept **gifts or hospitality** which could be reasonably viewed as likely to influence our advice or judgments.

## 4.2 WYG Duty of Care

The EL prime contractor, WYG, is a global consultancy with considerable experience of working around the world in contexts with varying levels of security. Discharging effective duty of care (DoC) to our project teams is our number one priority, and as such, WYG has developed a robust set of internal procedures.  We have an in-house Group Security Manager (Michael Allen MBE) to oversee our internal security and risk management training, policies and procedures and project level requirements; provision of pre-deployment briefing, ongoing risk assessment, transportation, secure accommodation and security management.  We also have an International Operational Security Manager (Shane Moore) who accompanies project teams on country deployments as required. We have a contract with International SOS (ISOS) for country intelligence and travel/medical advice.

WYG fully understands the moral obligation and legal responsibility to provide all employees and associates involved with its work, both nationally and internationally, with the protection and safe guard of life, which extends to assets, property and information regardless of operational location.

Our strict operating protocols dictate that we have in place procedures to ensure that all our people are safe at all times and any required changes needed to ensure this, are addressed in a timely manner.  The matrix overleaf provides an overview of how this is achieved:

**Daily**

**(Operational Level)**

- Intelligence service (information reporting and analysis) twice daily based on project locations
- Review Airport Meet and Great (collection and drop off)
- Arrivals security briefings
- Incident response/support (RTA, Breakdown, Threat)
- site specific Evacuation planning
- Investigate and generate incident reports
- Issue daily report capturing:
  - Number of movements
  - Incidents encountered
  - Changes in risk/threat
  - Issues encounterd
  - Changes required

**Weekly**

**(Operational Level)**

- Predict project intelligence needs in advance based on project deliverables and operational areas
- Analysis of incidents across operating area
- Review agree any operationally critical secuirty stance changes based on project needs and threats
- Review of Local Emergency Crisis response Plans (LECRP's)
- Review Medical contingency support localy and international cover based on project deliverables and locations
- Review incident reports

**Monthly**

**(Tactical Level)**

- WYG Project Security Review to include monthly sttaistics on:
  - Movements
  - Issues
  - Incidents
  - Changing threats/risks
  - Operational changes
- Project deliverables and objectives for next month
- Changing needs of the project
- Agree non-urgent operational change management requests

**Quarterly**

**(Strategic Board Level)**

- Review and approval of all current security mitigation measures
- Review of last quarter threat picture and incident analysis
- Review of incident reports for last quarter
- Regional security intelligence updates provided by third party supplier and international networks and liaison with Regional Security Managers, UK Embassy and in-country international business links
- Agree Operational Change Management requests
- Management approval to operating stance and procedures (Non-urgent)

All our operational policies and procedures are considered *"live"*, allowing constant review at any time with any changes required to be made using the formal change management and review process. The oversight of the project at Strategic, Tactical and Operational levels ensures that accountability is realised and that all levels within the project team participate in the review process, therefore ensuring that all aspects of project risk are mitigated, fit for purpose and can be escalated when need arises.

All bespoke designed procedures and protocols are fundamentally required to address real time security issues and as such define security stance (static and mobile), medical contingency procedures (local and international evacuation), security infrastructure (residence, offices, remote sites), reporting and oversight. All plans are maintained in the main by individual departments and project teams, supported by WYG Group Security Team when needed.