• **Studio** – checks quality/accuracy of artwork. Also retains all previous versions of artwork (numbered/dated), in the event we need to re-visit previous proofs

• **Production department** – checking prior to sending to print, including a final circulation to all key departments within Story, ensuring a zero-defect policy. Handles internal approval of live lasers, attends press pass, etc.

2. Externally

At the outset of any new project/relationship, we'd produce a Service Level Agreement (SLA), detailing how we'll deliver for the FPB, and commitment required from them at key approval stages, namely formal written:

- Confirmation of marketing objectives
- Approval of Creative Brief, subsequent Update Briefs (which will detail client feedback and agreed next steps), Digital and Data briefs
- Confirmation of approved media plan
- Approval of proposed production suppliers
- Approval and supply of purchase orders for agency fees and production costs
- Feedback and ultimately final approval of artwork
- Approval of contact reports

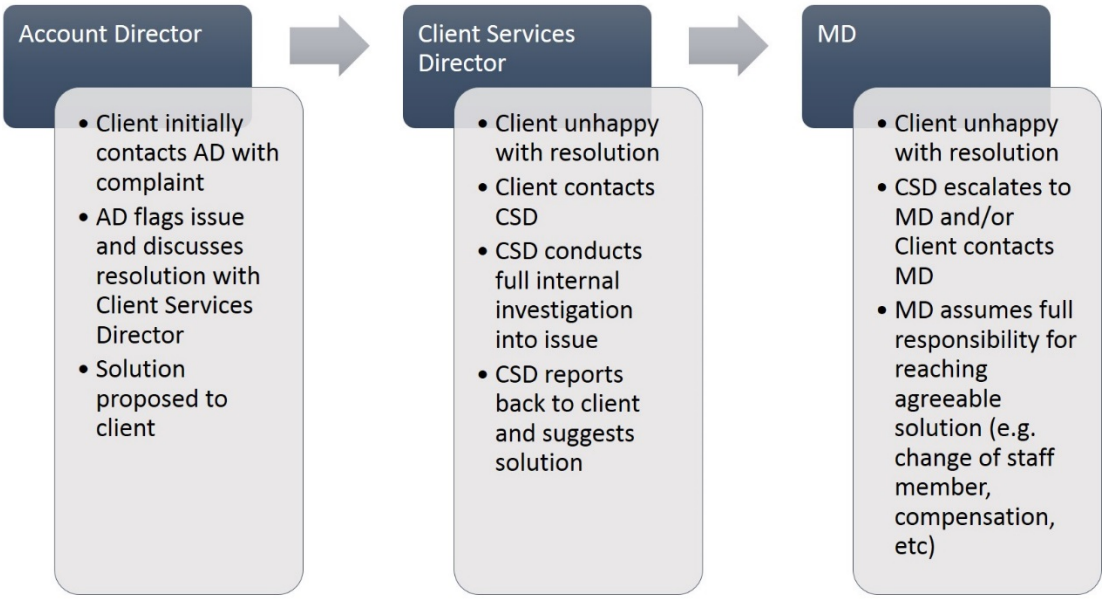
Detailed timing plans highlight each project stage/deadlines and client review/approval stages – a traffic light system provides an 'at a glance' view of whether the project is on track, at risk or running over.

We send diary invites for key approval deadlines and events, e.g. film shoots, field marketing team briefings, digital testing pre-go-live.

We also use weekly status reports to monitor progress and flag approval deadlines to clients.

Our complaints procedure/escalation process

Our SLA would include our formal escalation procedure which accounts for various stages of escalation to ensure speedy, satisfactory resolution:



Training/development and monitoring of performance of Account manager(s)

As outlined in 2.2.4 we instigate a programme of continuous professional development involving:

- On-the-job learning bespoke to FPB requirements, e.g. monitoring/collating/interpreting relevant coverage/market developments
- Formal CPD programme which includes self-learning, tutorials and attendance at events/courses
- In-house training programmes, including Lunch and Learn sessions where we invite industry experts to brief us on latest industry developments.

Account Managers' performance is monitored by:

- Formalised annual appraisals, conducted by line managers and incorporating feedback from colleagues and clients. These appraisals identify specific short and long-term development points
- Regular one-to-ones with their line manager which calibrate progression against personal development goals
- Quarterly/annual client reviews – we actively encourage client feedback on team performance at any time.

Key senior/account management CVs:

[20 pages redacted exempt.]

2.3.3

Business Management *- In order to meet the contract management requirements outlined in Schedule 1 and Schedule 1A of the Entire Agreement, the Contractor must have well established formal tracking tools and processes to deliver the service, ensuring business continuity at all times. These must be used as a formal monitoring mechanism within your organisation. Please provide a detailed breakdown of your processes for tracking and delivery, paying particular consideration to the following:*

• details of all tools and processes to track and report on progress of tasks and how you keep abreast of the latest tools and technologies in the sector;

• details of the management reporting arrangements employed to monitor tasks;

• details of how these outputs will contribute to the management of risk and inform future activities; and

• details of formal methods/process for identifying and addressing errors or under delivery including how and at what stage the client is informed.

• provide examples of the management information and details of any additional management information that will be available, including frequency. Outline how all of this will be used to identify and manage activity across the framework.

• details of any business continuity management standards applicable e.g. ISO 22301, and the processes and procedures in place to ensure the service is delivered in the event of an emergency situation occurring.

The tools and processes we use to track and report on progress of tasks and how we keep abreast of the latest tools and technologies in the sector

We deploy a bespoke blend of tools and processes to ensure seamless project progression, developed to meet our own exacting standards, as well as client requirements.

This involves both off-the-shelf tools (where these are appropriate) but also proprietorial tools that have been developed by The Mission Marketing Group (TMMG), specifically for marketing agency requirements, namely:

1. **Float**

Float is our day-to-day workflow scheduling system. A secure online browser-based tool, Float allows us to upload, track and monitor every single client job, both in the office and remotely/out-with normal working hours.

It's designed to ensure that job creation and progression is visible by, and flagged to, all relevant parties – account management, creative, traffic and production. When a new job is entered into Float by the account manager – along with the relevant schedule – this job is then flagged to creative and traffic and needs their approval for the job to go 'live.' In this way, there are immediate checks and balances in place to ensure that the job is deliverable with all required resource allocated to ensure delivery on time and on budget.

Because each job is allocated its own Story job number, it can then be tracked through with monitoring of all major milestones. At the agency's weekly scheduling meetings, Float is able to flag all jobs e.g. as 'on track' or 'slipping'.

Float also sets up automated email alerts, including individuals' weekly workload plus specific project milestones with diary invites for internal reviews and, if required, external presentations.

As a real-time system, Float also provides pinpoint accuracy around agency workload, dissectible in a number of ways:

- By client
- By client project
- By agency department
- By individual agency employee
- By hour, day and week

In this way, there is a helicopter view that allows for any urgent client briefs to be allocated and progressed with minimised delay. Because our pool of trusted freelance resource is also plugged into Float, we get an even broader view on resource availability.

[25 lines redacted exempt.]

Management reporting arrangements employed to monitor tasks

We deploy a full suite of reporting across all aspects of client projects:

Report	Role	Frequency
Contact Reports	Meeting outcomes and immediate actions/responsibilities	Inside 24-36 hours
Client Status Reports	Overview of all live and imminent projects	Weekly
Job reporting	On-going actions	As required
Detailed schedule	Ensuring on-time project delivery	At project outset – updated in real time
Reverse Creative Brief	Our interpretation of the client brief with agency insights	At project outset
Creative Updates	To capture key development requirements	As required
Quotations	Transparent financial management	Provided at outset of job and revised as required (e.g. as deliverables confirmed)
Studio and Production Briefs	Internal scheduling of artwork and production requirements	On-going
Financial reports	Overview of FPB expenditure on individual/all jobs	Monthly & Quarterly
Wash-ups	To provide integrated project evaluation	Upon availability of results v KPIs
Client reviews	To evaluate overall agency performance	Quarterly & Annually
Intelligence reporting	Sharing relevant intel with client teams, e.g. relevant global case studies	On-going

How these outputs will contribute to the management of risk and inform future activities

The above reporting ensures full transparency for all internal and client stakeholders to provide the earliest warning possible of developing risk. We also adopt continuous monitoring of all projects to ensure:

- We're on brief - Story strategic/briefing documents
- We're on time - Schedules
- We deliver on our zero-defect policy - Internal approval processes
- We're on budget - Financial management and reporting.

At the outset of every client project, the lead account manager adopts a risk assessment in conjunction with the lead client and traffic/production. In this way, any required contingencies are built into reporting, e.g. Float, and notified to all relevant agency personnel.

Our campaign wash-up report is a key tool to inform future activity – it reviews a campaign holistically and formally records key learnings and recommendations – vital in ensuring continuous improvement.

Also, any lessons learned from a risk mitigation is reflected in an update to our Story FPB Manual.

Details of formal methods/process for identifying and addressing errors or under delivery including how and at what stage the client is informed.

Our initial risk assessment, undertaken on being commissioned by a new FPB/for a new project, identifies potential risks and proposed mitigation to minimise the chance of errors occurring.

As jobs progress, we use the reporting detailed above to identify errors or under-delivery timeously, alongside our internal processes, e.g:

- Weekly internal team meetings highlight jobs at risk of slippage, allowing us to quickly allocate further resource
- Weekly WIP meetings with the Story Finance team monitor any cost discrepancies (e.g. supplier bill not matching client quote)
- Real-time monitoring of our Float/Easl systems

Addressing errors

As an experienced, flexible and nimble agency, we'd initially look to resolve an error ourselves, e.g: if the error results from a resource shortfall, then we are able to action:

- The best additional resource, identified quickly via Float
- This might include drawing upon our pool of trusted freelancers, or from the 900-strong workforce of TMMG, covering all the specialisms required of the FPB from 13 UK locations.

Whilst Story's project management processes (including formal approvals at all key project stages to minimise miscommunication or deliverables being 'off brief') and account manager training mean it's rare that projects are late/incorrect, we have formalised methods of recovery:

[redacted exempt.]

Keeping clients informed

If an error has been identified, and remedial action is required:

- The client will be informed by the Account Director and kept up to date at all times
- The error is discussed at the project wash-up stage
- The learnings are incorporated into Story's FPB Manual

If resolution proves to be unachievable, then we have comprehensive insurance policies:

- Employers Liability - [redacted]
- Public/Products Liability - [redacted]
- Professional Indemnity [redacted]

Examples of the management information/ details of any additional management information that will be available, including frequency, and how all of this will be used to identify and manage activity across the framework.

We have detailed our standard management reporting and its frequency above. Should additional management information be required, we would discuss this as part of a) being appointed to the Framework, i.e. with SG Procurement; and b) our induction to a new FPB. We are well-versed in delivering the current quarterly management reporting for SG, detailing all invoicing and added value provided across the existing Framework. Our Finance team will also provide monthly invoicing statements as standard.

We also commit to sharing FPB client performance reviews and campaign wash-ups with both SG and other FPBs if permitted to demonstrate our credentials.

Details of any business continuity management standards applicable e.g. ISO 22301, and the processes and procedures in place to ensure the service is delivered in the event of an emergency situation occurring.

Key principles of ISO 22301 are embedded in our business continuity plan (BCP), including:

- Using impact analysis and risk assessment to develop our business continuity strategy
- Ensuring we have the necessary resources to implement our BCP
- That we have competent staff who are aware of their responsibilities for implementation of the BCP
- Established communication procedures

Our Business Continuity Plan incorporates alternative Edinburgh-based premises (with 20 fully-operational workstations), meaning that within two hours of any catastrophic systems failure – or other force majeure – we can be fully operational.

Staff can access emails via Microsoft 365 and project files via a Virtual Protected Network to ensure that an issue at Story HQ doesn't jeopardise service delivery.

In the event of a catastrophic staff shortage, as part of TMMG we can make use of all sister agency resource (c. 950 experienced staff across UK, Asia and America).

2.3.4

Business Continuity and Cyber Resilience *- A key element of the service will be the Contractor's Business Continuity in respect of Cyber Resilience services. Tenderers should provide details of any standards applicable in this area (e.g. ISO 27001, ISO 22301, ISO/IEC 20000, Cyber Essentials/Cyber Essentials Plus or their equivalents), advise whether any certifications are held and provide details of any plans to achieve any certification. Tenderers must also describe their procedures to ensure continuity of service and protection against cyber-attacks, paying particular attention to the following:-*

• details of processes followed including those for assessing future risks;

• testing of Disaster Recovery policies and procedures, including the dates, duration and frequency;

• methods for the back-up of delivering services should an incident occur including manpower and access to equipment;

• methods in place to mitigate against cyber-attack and crime using online technologies including processes relating to Boundary Firewalls and Internet Gateways, Secure Configuration, Access Control, Malware Protection and Patch Management;

Tenderers should refer to the UK Governments Cyber Essentials Scheme and consider the information included within the scheme when providing their response to this section. (https://www.gov.uk/government/publications/cyber-essentials-schemeoverview)

Where applicable, Tenderers must ensure that any sub-contractors appointed to deliver any of the services have Business Continuity and Cyber Resilience measures in place.

Story UK have adopted a robust and industry standard based information security policy, covering items such as firewall and gateway protection, secure configuration, access control, malware and patch management.

Story are currently progressing along the Government's Assurance Framework as defined within the Cyber Essentials Scheme, and are actively engaged to achieve a Cyber Essentials Plus accreditation during the first quarter of 2017.

Longer term, Story are working to achieve the industry recognised ISO27001 accreditation for a demonstratively effective Information Security Management System (ISMS). The ICT roadmap has this marked as a Q4 2017 project.

On-going Risk Assessment

Story have an ICT Security Committee that meets quarterly and assesses current and possible future risks to the ICT and business infrastructure, and updates the Business Recovery plan accordingly, as well as issuing any new or revised guidance in terms of agreed ICT security policies. The ICT Security Committee adopt a general framework, based on the ISO27001 recommendations, of:-

- Defining a Security Policy
- Defining the Scope of the ISMS
- Conducting a Risk Assessment
- Managing Risks Identified
- Implementing Controls
- Preparing Statements of Accountability and Incident Reporting and Monitoring

The ICT Security Committee reports to the firm's Digital Director, who ultimately is responsible for ICT security and Business Continuity. A "risk register" is maintained by the ICT Security Committee and reviewed in depth annually. Risks are measured in terms of likelihood and impact, and what mitigating actions can be taken to prevent occurrence, and what remedial actions would be needed should occurrence happen.

Business Continuity and Disaster Testing

The Business Continuity plan centres on two inter-related pillars:

- Off-site replication of critical business information; and
- Workplace recovery space to allow staff to relocate.

Each evening, all of the Story servers backup up locally to a Network Attached Storage device, which holds up to 28 days' worth of backups for each server. Overnight, the latest backups are transmitted securely over an encrypted link to a local data centre, where the backup is added to the data centre set.

The data centre holds up to 7 days' worth of backups, but more importantly, converts the latest backup into a virtual "hot standby" for each server, ready to be moved into production within 30 minutes.

Story have contracted to ensure that up to 20 key staff can relocate to a dedicated recovery centre close to Edinburgh city centre, where they are provided with desks, desktop computers, Internet access and telephony. These desktops connect back to the replicated hot-standby servers at the data centre, providing an end-to-end recovery process.

The target recovery point is 8pm the evening before an incident, and the recovery time is targeted to be within 2 hours on invocation of an incident.

The Business Continuity plan is tested annually, with a select group of Story staff attending at the recovery centre and verifying that they can access emails, files, accounts and other essential services on the replicated servers, as of the end-of-play the previous evening. The Recovery Centre then supplies a certificate of compliance. Any actions or learning experiences resulting from the test are then discussed at the next ICT Security Committee meeting and appropriate adjustments to the risk register and Business Continuity plan are enacted.

Methods and processes to mitigate against cyber-attacks

In regards the prevention and protection from cyber-attack, Story comply with what used to be the Government's "10 step approach" which has now evolved into the Cyber Essentials Scheme.

Based on the work of the ICT Security Committee, common Internet based risks have been identified and mitigated against at the firewall and gateway level. The perimeter defences are checked annually by an external third party (ProCheck) via penetration testing. Furthermore, and more than the Cyber Essential recommendations, Story also operate a "defence-in-depth" approach, and operate two firewalls and gateways from different manufacturers with differing rule bases, to ensure that a single perimeter breach will not provide access to the core systems.

Story also operate a fully managed Intrusion Detection System (IDS) within the network infrastructure in order to proactively monitor any unusual, or out of band, network activity.

Story have adopted industry standard hardening procedures for all perimeter devices and all servers, especially those running the Microsoft Windows Server operating systems. This is in line with published hardening recommendations by vendors.

System access to data, web sites, applications and USB devices is based on a “denied by default” basis, with the ICT Security Committee approving any changes to security profiles.

Information areas on the servers have been classified by client and by access needs, and appropriate security groups created to allow only the staff needing access to have access. The same applies to accessing any external USB hard disks or other mass media devices.

Access to web sites and social media sites and applications is also restricted by default, and line managers need to approve any staff members needing access and these requests are logged and audited.

An annual audit is carried out by the external IT support company to ensure that the levels of access granted matched the audited requests and to ensure that any completed projects have had their related security permissions revoked. This also applies to any staff who have left employment.

Malware is addressed by cloud based anti-spam services to “clean” emails in transit, and the company has a policy in place to prevent encrypted or compressed files reaching the end user directly, but requiring the Compliance Director to authorise their release. Any form of executable code is prohibited from being transmitted.

Anti-virus software is implemented on each end user device and centrally managed and controlled. A separate anti-virus product is installed on the perimeter gateways to provide a further defence-in-depth approach.

The final malware protection is link protection within emails, with links being sent to a cloud based sandbox service that verifies each link on access to ensure that the destination is valid and no malicious code is present at the destination page.

Patch management is looked after by Story’s external IT Support company who apply desktop and laptop patches on a weekly basis and check for compliance. Servers are patched monthly, with the exception of any vendor mandated critical patches, which are then applied as soon as operationally possible. The patch compliance is monitored weekly and any exceptions are followed up by the IT support company to ensure that any machines that have been switched off (laptops away, holidays, etc.) have been caught up and that all machines are no more than 14 days out of compliance.

The above aspects of boundary controls, secure configurations, access control, malware protection and patch management all cover and exceed the Cyber Essentials requirements, and as Story have an active ICT Security Committee assessing future risks and policies, this places them squarely in line for achieving their Cyber Essentials Plus certification in the coming months, as they already have a mature culture of ongoing assessment and management of Cyber Security risks.

Finally, and as a matter of course, we liaise with sub-contractors to assess their own processes for Business Continuity and Cyber Resilience.

2.3.4

Business Continuity and Cyber Resilience *- A key element of the service will be the Contractor's Business Continuity in respect of Cyber Resilience services. Tenderers should provide details of any standards applicable in this area (e.g. ISO 27001, ISO 22301, ISO/IEC 20000, Cyber Essentials/Cyber Essentials Plus or their equivalents), advise whether any certifications are held and provide details of any plans to achieve any certification. Tenderers must also describe their procedures to ensure continuity of service and protection against cyber-attacks, paying particular attention to the following:-*

• details of processes followed including those for assessing future risks;

• testing of Disaster Recovery policies and procedures, including the dates, duration and frequency;

• methods for the back-up of delivering services should an incident occur including manpower and access to equipment;

• methods in place to mitigate against cyber-attack and crime using online technologies including processes relating to Boundary Firewalls and Internet Gateways, Secure Configuration, Access Control, Malware Protection and Patch Management;

Tenderers should refer to the UK Governments Cyber Essentials Scheme and consider the information included within the scheme when providing their response to this section. (https://www.gov.uk/government/publications/cyber-essentials-schemeoverview)

Where applicable, Tenderers must ensure that any sub-contractors appointed to deliver any of the services have Business Continuity and Cyber Resilience measures in place.

Story UK have adopted a robust and industry standard based information security policy, covering items such as firewall and gateway protection, secure configuration, access control, malware and patch management.

Story are currently progressing along the Government's Assurance Framework as defined within the Cyber Essentials Scheme, and are actively engaged to achieve a Cyber Essentials Plus accreditation during the first quarter of 2017.

Longer term, Story are working to achieve the industry recognised ISO27001 accreditation for a demonstratively effective Information Security Management System (ISMS). The ICT roadmap has this marked as a Q4 2017 project.

On-going Risk Assessment

Story have an ICT Security Committee that meets quarterly and assesses current and possible future risks to the ICT and business infrastructure, and updates the Business Recovery plan accordingly, as well as issuing any new or revised guidance in terms of agreed ICT security policies. The ICT Security Committee adopt a general framework, based on the ISO27001 recommendations, of:-

- Defining a Security Policy
- Defining the Scope of the ISMS
- Conducting a Risk Assessment
- Managing Risks Identified
- Implementing Controls
- Preparing Statements of Accountability and Incident Reporting and Monitoring

The ICT Security Committee reports to the firm's Digital Director, who ultimately is responsible for ICT security and Business Continuity. A "risk register" is maintained by the ICT Security Committee and reviewed in depth annually. Risks are measured in terms of likelihood and impact, and what mitigating actions can be taken to prevent occurrence, and what remedial actions would be needed should occurrence happen.

Business Continuity and Disaster Testing

The Business Continuity plan centres on two inter-related pillars:

- Off-site replication of critical business information; and
- Workplace recovery space to allow staff to relocate.

Each evening, all of the Story servers backup up locally to a Network Attached Storage device, which holds up to 28 days' worth of backups for each server. Overnight, the latest backups are transmitted securely over an encrypted link to a local data centre, where the backup is added to the data centre set.

The data centre holds up to 7 days' worth of backups, but more importantly, converts the latest backup into a virtual "hot standby" for each server, ready to be moved into production within 30 minutes.

Story have contracted to ensure that up to 20 key staff can relocate to a dedicated recovery centre close to Edinburgh city centre, where they are provided with desks, desktop computers, Internet access and telephony. These desktops connect back to the replicated hot-standby servers at the data centre, providing an end-to-end recovery process.

The target recovery point is 8pm the evening before an incident, and the recovery time is targeted to be within 2 hours on invocation of an incident.

The Business Continuity plan is tested annually, with a select group of Story staff attending at the recovery centre and verifying that they can access emails, files, accounts and other essential services on the replicated servers, as of the end-of-play the previous evening. The Recovery Centre then supplies a certificate of compliance. Any actions or learning experiences resulting from the test are then discussed at the next ICT Security Committee meeting and appropriate adjustments to the risk register and Business Continuity plan are enacted.

Methods and processes to mitigate against cyber-attacks

In regards the prevention and protection from cyber-attack, Story comply with what used to be the Government's "10 step approach" which has now evolved into the Cyber Essentials Scheme.

Based on the work of the ICT Security Committee, common Internet based risks have been identified and mitigated against at the firewall and gateway level. The perimeter defences are checked annually by an external third party (ProCheck) via penetration testing. Furthermore, and more than the Cyber Essential recommendations, Story also operate a "defence-in-depth" approach, and operate two firewalls and gateways from different manufacturers with differing rule bases, to ensure that a single perimeter breach will not provide access to the core systems.

Story also operate a fully managed Intrusion Detection System (IDS) within the network infrastructure in order to proactively monitor any unusual, or out of band, network activity.

Story have adopted industry standard hardening procedures for all perimeter devices and all servers, especially those running the Microsoft Windows Server operating systems. This is in line with published hardening recommendations by vendors.

System access to data, web sites, applications and USB devices is based on a “denied by default” basis, with the ICT Security Committee approving any changes to security profiles.

Information areas on the servers have been classified by client and by access needs, and appropriate security groups created to allow only the staff needing access to have access. The same applies to accessing any external USB hard disks or other mass media devices.

Access to web sites and social media sites and applications is also restricted by default, and line managers need to approve any staff members needing access and these requests are logged and audited.

An annual audit is carried out by the external IT support company to ensure that the levels of access granted matched the audited requests and to ensure that any completed projects have had their related security permissions revoked. This also applies to any staff who have left employment.

Malware is addressed by cloud based anti-spam services to “clean” emails in transit, and the company has a policy in place to prevent encrypted or compressed files reaching the end user directly, but requiring the Compliance Director to authorise their release. Any form of executable code is prohibited from being transmitted.

Anti-virus software is implemented on each end user device and centrally managed and controlled. A separate anti-virus product is installed on the perimeter gateways to provide a further defence-in-depth approach.

The final malware protection is link protection within emails, with links being sent to a cloud based sandbox service that verifies each link on access to ensure that the destination is valid and no malicious code is present at the destination page.

Patch management is looked after by Story’s external IT Support company who apply desktop and laptop patches on a weekly basis and check for compliance. Servers are patched monthly, with the exception of any vendor mandated critical patches, which are then applied as soon as operationally possible. The patch compliance is monitored weekly and any exceptions are followed up by the IT support company to ensure that any machines that have been switched off (laptops away, holidays, etc.) have been caught up and that all machines are no more than 14 days out of compliance.

The above aspects of boundary controls, secure configurations, access control, malware protection and patch management all cover and exceed the Cyber Essentials requirements, and as Story have an active ICT Security Committee assessing future risks and policies, this places them squarely in line for achieving their Cyber Essentials Plus certification in the coming months, as they already have a mature culture of ongoing assessment and management of Cyber Security risks.

Finally, and as a matter of course, we liaise with sub-contractors to assess their own processes for Business Continuity and Cyber Resilience.

2.4.2

Tenderers must confirm that, where appropriate, they will support the Scottish Ministers policies on Sustainability and Corporate Social Responsibility in delivering the service required.

Story can confirm its support for the Scottish Ministers' policies on Sustainability and CSR.

Some demonstrable examples of how we have supported these policies:

- Our independently-evaluated Health/Greener Scotland campaigns have contributed to positive behaviour change, meaningful improvements in public service and quality of life

- We are recognised for our highly collaborative approach to working with our partners and delivering Value-For-Money (e.g. identifying cost-efficiencies)

- Through our Greener Scotland work, we have an intimate understanding of the importance and vision for a low-carbon economy – Story's Sustainability policy ensures we maximise our efforts to reduce our environmental impact.

2.5.2

Please describe how your organisation proposes to commit to being a best practice employer in order to support these Scottish Ministers workforce policies in the delivery of this Framework. Answers need not be constrained to or be reflective of any examples given alongside this question.

The tenderer should take the engagement and empowerment of staff seriously; take a positive approach to rewarding staff at a level that helps tackle poverty (e.g. through a commitment to paying at least the living wage), provide skills and training which help staff fulfil their potential, that you do not unfairly exploit staff (e.g. in relation to matters such as the inappropriate use of zero hours contracts): that your company will demonstrate organisational integrity with regards to the delivery of those policies. This reassurance should be achieved by providing tangible and measurable examples that can be monitored and reported as part of on-going contract management.

Story is committed to being a best-practice employer, offering staff key opportunities and benefits, including:

1. **Continuing Professional Development (CPD) to help staff fulfil their potential**

A key requirement of our membership of the Institute of Practitioners in Advertising (IPA), all staff benefit from:

- 24 hours min development activity p/a, including 5% of the agency completing both the IPA's LegRegs and Commercial Certificates.
- Creation of a Strategic Development Plan, with staff training a core component - setting out Story's business objectives, identifying how CPD will help achieve them and how we'll measure its impact.
- An induction process for new staff, ensuring swift uptake of our agency processes.
- Annual appraisal system, capturing key areas for development and identifying training needs. Staff then work with their line manager to create a personalised development plan that will make developmental goals achievable and constructive.
- Two dedicated CPD managers highlight training opportunities and monitor CPD progress across Story.

In addition to the IPA's own resources, we also subscribe to other leading-edge sources of information and inspiration on the marketing industry to keep staff motivated and inspired through CPD – for example, WARC: the World Advertising Research Centre which houses the world's biggest online resource of award-winning marketing case studies, micro/macro consumer trends, global and market data and futurology.

2. **The Story Management Group – empowering and rewarding staff**

This is a small team drawn from all levels/disciplines of Story, who are recognised as rising stars in the business. Complementing the IPA CPD programme, the Group takes responsibility for making induction/appraisal processes effective and engaging, and also identifying opportunities for Lunch & Learn sessions with interesting speakers.

The latter can be in relation to industry skills and crafts

[3 lines redacted exempt.]

[1 page redacted exempt.]

3. **Focus on Welfare at Work**

Every new start at Story gets a full induction and we provide a welcome directory which covers everything from making the tea to the company's benefits' programmes, which include a subsidised healthcare scheme, contributory company pension scheme and a share scheme in our parent company TMMG.

The Management Group also includes workplace wellbeing in its remit, e.g. they've formed a reciprocal relationship with a local osteopath who visits us to undertake group and one-to-one consultations on posture. (In return we provide marketing consultancy to this micro business.)

We also offer staff free fruit, herbal tea and caffeine-free drinks.

We moved premises 18 months ago and have purposefully developed a bright, airy workplace environment to enhance staff wellbeing. We worked with specialist workplace designers to create the most ergonomic and productive of office environments.

We have a large communal kitchen and run lunch clubs to encourage staff interaction and downtime away from their desks during the working day.

[9 lines redacted exempt.]

5. **Free and incremental benefits reward staff and tackle poverty**

In addition to our contributory pension scheme and subsidised healthcare, we offer:

- Cinema voucher scheme
- Subsidised gym memberships
- Interest-free season ticket loans
- Bike2Work interest-free loans

6. **Equal Opportunities and Living Wage**

We place significant focus on gender equality (our Story board comprises four females to three males), and have a diverse workforce. Flexible working patterns, e.g. for parents, help staff manage their work/life balance.

All staff – full, part-time and contractors working regularly on the premises – are paid above the current living wage of £8.45 per hour. No staff are, or ever will be, on zero-hour contracts. We adopt the Ethical Trading Initiative's international Living Wage guidance in relation to overseas' suppliers.

2.5.3

The Scottish Business Pledge is a Government initiative which aims for a fairer Scotland through more equality, opportunity and innovation in business. Information on this can be found at the following link:

https://scottishbusinesspledge¬.scot/

Tenderers are asked to confirm if they have signed up to the Scottish Business Pledge.

As an agency we are in a position to make pledges against all of the Scottish Business Pledge's nine components.

For example, as well as paying the living wage, we:

- Never use zero hours contracts
- Have a very diverse workforce with strong female representation in senior positions
- Have a significant proportion of internationally sourced business.

We are also an active participant in our local communities via several education outreach programmes with schools and colleges.

On this basis, we have made our submission to the Scottish Business Pledge administrators.

2.5.4

The Scottish Living Wage Accreditation Initiative and the Living Wage Foundation recognise and celebrate the responsible leadership shown by Living Wage Employers and support employers to incorporate the Living Wage into organisational structures long term. More information can be found at the links below:

http://scottishlivingwage.org/¬

http://www.livingwage.org.uk/

Tenderers are asked to confirm if they are accredited as a Living Wage Employer.

We have a fundamental belief in treating our employees fairly and with respect – this ethos is good not just for our employees but for the future health of the business as well.

We can confirm that all of our directly employed staff, and all contracted employees, are paid at rates above the new living wage rate of £8.45 per hour in Scotland. In line with Living Wage guidance, this does not include non-guaranteed bonuses such as sales or production.

On this basis, we are in the process of seeking our Living Wage Employer accreditation.