

Third Surveillance

Report for:

CentralNic Ltd

LRQA reference:	LRQ4007101/0005
Assessment dates:	12th March 2014
Assessment location:	London, UK
Assessment criteria:	ISO 9001:2008 ISO/IEC 27001:2005
Assessment team:	Jonathan Akers
LRQA office:	Coventry

Contents

1.	Executive report	3
2.	Assessment summary	4
3.	Assessment findings log - ISO 9001:2008	10
4.	Closed Findings - ISO 9001:2008	11
5.	Assessment findings log - ISO/IEC 27001:2005	12
6.	Closed Findings - ISO/IEC 27001:2005	13
7.	Audit Programme/Plan	16
8.	Next visit details	18
9.	Report Explanation.....	19

Attachments

This report was presented to and accepted by:

Name:	Gavin Brown
Job title:	CTO

Lloyd's Register Quality Assurance Limited, its affiliates and subsidiaries and their respective officers, employees or agents are, individually and collectively, referred to in this clause as "LRQA". LRQA assumes no responsibility and shall not be liable to any person for any loss, damage or expense caused by reliance on the information or advice in this document or howsoever provided, unless that person has signed a contract with the relevant LRQA entity for the provision of this information or advice and in that case any responsibility or liability is exclusively on the terms and conditions set out in that contract.

1. Executive report

Assessment outcome:

The objective of this visit was to review the compliance of CentralNic, London, UK against the requirements of the international standards ISO 9001:2008 and ISO/IEC 27001:2005.

As a result of this one-day assessment, no major non-conformities were identified and therefore certification to the above Standards can continue.

No misuse of logo was observed.

The client is reminded that assessments are subject to time limitations, are restricted in scope and use sampling methodology. Consequently the absence of a comment on a particular area or system element does not necessarily imply conformance with relevant requirements of any specified standard or regulation. The client is reminded that assessments are subject to time limitations, are restricted in scope and use sampling methodology. Consequently the absence of a comment on a particular area or system element does not necessarily imply conformance with relevant requirements of any specified standard or regulation.

Continual improvement:

The management system is generally effective, and appears to be evolving well. As the business is expanding it is important to ensure that new staff, especially in those functions where information security may be less cultural, are suitably trained and have processes to follow (and that this is documented and evidenced where necessary).

Areas for senior management attention:

The degree of integration of the policy and objectives with the system effectiveness measures and relevant business metrics would benefit from more quantitative assessments than are presently being recorded.

2. Assessment summary

Introduction:

Purpose

The purpose of this report is to record the assessment activities carried out at CentralNic, London, UK against the requirements of the international standards ISO 9001:2008 and ISO/IEC 27001:2005.

Type of visit

Surveillance – to review, on an on-going basis, the continued compliance of the management system. Usually, a surveillance visit will contain one or more themes aimed at providing the organisation with business assurance. This is the third surveillance assessment in the cycle of five such visits in the life of the current certificate.

Theme of the visit

It was agreed that the theme of the visit would be process improvement.

Scope of certificate

This was confirmed as “The provision of innovative, reliable and flexible registry services for ccTLD, gTLD and private domain name registries. In accordance with the Statement of Applicability v1.2.1”

Business context

The assessment took place in a business context of the recent flotation of the parent holding company on the AIM. The company has grown over the last six months.

Changes to planned arrangements

None.

An opening meeting was held with Mel Blackmore (Blackmores) to discuss the programme for the visit.

The Closing meeting was held with Gavin Brown and Mel Blackmore to confirm the outcome of the visit, findings and the date of the next visit.

Assessor:	Jonathan Akers
------------------	----------------

Assessment of:	Management Elements, Policy and Objectives.	Auditee(s):	Mel Blackmore
Audit trails and sources of evidence:			
<ul style="list-style-type: none"> • Quality and Info Security Management Review Report 12/12/13 • CentralNic Management System Manual v1.2.1 10 Sep 13 • Electronic commerce, PCI • Overview of changes to the Integrated Management System since the last visit • IST – Ben Crawford and Gavin Brown but will include CFO and exec assistant to CEO • Plan to extend the scope beyond the current team. • ICANN feedback from registrars • Internal Audits • Quality Policy • Information Security Policy • “the Wiki” - Access control policy • Document Classification Policy rev 1.7296 19 June 2012 • Biannual IST meeting Minutes 23/12/2013 • Internal Audit Schedule 2014 v2.0 10/3/14 • Internal Audit Report 001/014 11th March 14 v1.0 06/13 • The CTO provided an update on the recent business and management system changes. • The sixth floor is now earmarked for use by the sales team in lieu of the previously planned office move and the acquisition of the first floor.. 			
Evaluation and conclusions:			
The area was adequate. Policy and Objectives have been reviewed, but have not been fully revised to be SMART.Actions. The internal audit process was satisfactory.			
Areas for attention:			
<p>The system effectiveness is described as ‘good’ by the management review.</p> <p>Opportunity for Improvement The management review should be based on clear evidence rather than anecdotal. This may be assisted by the provision of KPI performance summaries. Measurements of effectiveness (i.e. achievement of Objectives).</p>			

Assessment of:	Overview/Introduction	Auditee(s):	Gavin Brown
Audit trails and sources of evidence:			
<ul style="list-style-type: none"> • Rack servers – primary site is Angel Qube managed services – building is Level 3 • Secondary is being built (Maidstone). Custodian data centre • Both Qube and Custodian certified to 27001 QUBE IS 587514 • Custodian IS 567248 exp 30/06/14 			
Evaluation and conclusions:			
<p>The area was adequate. Historically the market has been focused on the UK, Europe and USA, currently significant expansion is expected in Asian (Japan, China, India) and Middle Eastern Markets.</p> <p>New staff are part of TLD registry solutions.</p> <p>Registrar provides domains to end users,</p> <p>Technical staff are part of CentralNic, registry.</p>			
Areas for attention:			
Opportunity for Improvement The hosting is collocated with Level 3, clarification on the certification.			

Assessment of:	Risk Assessment	Auditee(s):	Mel Blackmore
Audit trails and sources of evidence:			
<ul style="list-style-type: none"> • Risk Assessment v1.2.0 • Methodology • Competency Matrix covering – training, access and competency • Denial of service attack via botnets by nation states 			
Evaluation and conclusions:			
<p>The area was adequate. Some mitigating actions. Source code is held in the GRDC data centre with a backup copy at Moorgate, tertiary copy held in Portsmouth Daily backups.</p>			
Areas for attention:			
None at this time.			

Assessment of:	Asset Management	Auditee(s):	Gavin Brown
Audit trails and sources of evidence:			
General DNS servers are located in Tier 1 locations around the world and are monitored remotely. Asset Register spreadsheet General IT security Policy (iPads, encrypted if required),			
Evaluation and conclusions:			
The area was satisfactory. Ports are locked down.			
Areas for attention:			
Opportunity for Improvement The asset register is not actively managed, however this could be done with the IT request form. Opportunity for Improvement The company enforces backup, password and antivirus on company devices and has some guidelines, these could be extended to personal devices..			

Assessment of:	Physical Security	Auditee(s):	Gavin Brown
Audit trails and sources of evidence:			
Cleaners – issues, Rentokil			
Evaluation and conclusions:			
The area was satisfactory.			
Areas for attention:			
Opportunity for Improvement Consider whether cleaning could be done within office hours without unduly disrupting staff (e.g. early morning or early evening).			

Assessment of:	HR starters, leavers, Awareness, training	Auditee(s):	Stella Flattery(CEO Exec Asst/HR)
Audit trails and sources of evidence:			
<p>Screening – 2 references, proof of ID (passport/driving licence) and RTW, qualifications or technical test ICANN requirements</p> <p>Introduction for new employees – awareness course</p> <p>IMS presentation – 9001, 27001</p> <p>Controls</p> <p>Password 30 days, 8, alpha & numeric</p> <p>Macs, windows, linux</p> <p>Leaver E.Marriott, exit form, Letter of resignation, letter re dates and receipts.</p> <p>Starters</p> <ul style="list-style-type: none"> - Matt McLeary job description Domain Administrator v1.0 CV passport GBR 515817476 employee info, induction checklist 13/2/14 contract, offer of employment, confidentiality agreement, reference from Sky BroadBand, confirmation of employee safety handbook. - Alvaro Retortillo IT request form employee information form, confidentiality, started 10/2/14, confirmation of safety handbook, passport exp 21/04/2015 ESP AAB46323, terms and conditions, linux system admin technical test, Reference – Amber Innovaciones 			
Evaluation and conclusions:			
The area was satisfactory. Induction training is undertaken periodically – usually a target within a month via interactive, however a written version could be used.			
Areas for attention:			
<p>Social engineering maybe a consideration.</p> <p>Observation Employee has not signed the form because they email it, in this case then the user field is unnecessary.</p>			

Assessment of:	Tech Operations, Design & Development	Auditee(s):	Gavin Brown
Audit trails and sources of evidence:			
<ul style="list-style-type: none"> • In-house developed Bug Tracker system is used for everything • Development Process 1.8587 11/3/2014 • Operational Testing and Evaluation – UAT in controlled environment • Change Control Process 1.7309 25/6/2012 • 4412 Design and Development Changes 			
Evaluation and conclusions:			
The area was satisfactory. Parent-child dependencies may be stipulated for bugs.			
Areas for attention:			
None at this time.			

Assessment of:	Legal & Technical Compliance	Auditee(s):	Mel Blackmore, Gavin Brown
Audit trails and sources of evidence:			
<ul style="list-style-type: none"> • Changes to Firewalls are monitored using an in-house tool and will alert if there is a change in the firewall configuration. • Version control system must be attached to bug report. • Servers use puppet configuration mgt system, centralised server which is connected to hourly and variations. • Puppet server is in the version control. • CentralNic IS Legal Register v2 • ICANN(Internet Corporation for Assigned names and Numbers) 			
Evaluation and conclusions:			
The area was satisfactory.			
Areas for attention:			
Opportunity for Improvement Note that the EU data protection Regulation will come into force at some time and may have implications for data retention.			



3. Assessment findings log - ISO 9001:2008

Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Minor NC	Open	<p>Review of the IPV6 & IPV4 design & development aspects of the ISP Project in the Bug Tracker Tool revealed that there was traceability of the various network technical changes up to and including go-live scheduled for 03 Feb 2013.</p> <p>There was also evidence of various test activities with the GRDC and a Go-live Maintenance Schedule had been produced and signed-off by the CTO.</p> <p>However, there was no over-arching project plan as such and without searching through several related Bugs within the Bug Tracking Tool; it was difficult to ascertain the specific requirements to each aspect of the project and their dependencies within the context of the overall development engineering task.</p> <p>There was no formal requirements specification or a functional design specification, no formal test plan or procedures (Verification, Validation and Integration etc), acceptance criteria or configuration management/change controls to be applied etc.</p> <p>All aspects expected of a critical customer impacting project of this nature and lacking in the formality prescribed in the client's own SDLC requirements for application and web based development projects.</p>	<p>17/10/13 JLP</p> <p>It is evident that improvements to the development process have been made, particularly with respect to change management and segregation of responsibilities. However, the client is still considering how best to meet the specific requirements of Section 7.3 of ISO 9001:2008 in a manner that best suits the business and development needs of the company.</p> <p>The NC remains Open and the client is reminded of the need to demonstrate the implementation of required corrective action at the next surveillance visit.</p> <p>12 Mar 14 JPA The new development process has been defined, but to date has not been applied as the process has only just been issued.</p> <p>Review at next visit to confirm effectiveness.</p>	Design & Development Planning	31 Jan 13	1301JLP001	7.3.1

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYYY<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



4. Closed Findings - ISO 9001:2008

Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Minor NC	Closed	<p>The current procedures for the control of documents and the control of records as detailed in the Management System Manual - Section 6.5 are not sufficiently detailed to meet all of the requirements of ISO 9001:2008 (4.2.3 & 4.2.4) and ISO 27001:2005 (4.3.2 & 4.3.3). Particularly in relation to defining the controls relating to document review and approval and versioning methods to be used.</p> <p>It is also noted that for availability purpose a significant amount of High Level Policy and Process documentation is stored on the Wiki and that this documentation may be changed without approval by a wide audience.</p>	<p>10/07/12: JLP: Document and record control procedure has been updated</p> <p>Access and version controls applied to Wiki documentation.</p>	Control of Documents and Records	15 May 12	1205JLP01	4.2.3, 4.2.4

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYMM<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



5. Assessment findings log - ISO/IEC 27001:2005

Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYMM<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



6. Closed Findings - ISO/IEC 27001:2005

Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Minor NC	Closed	<p>Whilst there is some level of oversight applied to changes to the Network (CTO active involvement), the concept of segregation of duties is not being applied e.g. the system engineer can initiate, make and self authorise changes to the firewall and other parts of the network.</p> <p>Whilst the size of the business and small pool of technical resources may not allow for total segregation, any risks associated with allowing open access and authorisation should be considered as part of Risk Assessment. A review of the clients Risk Treatment Plan for Network Security identifies 'Segregation of Duties' as a primary Control Measure.</p>	<p>10/07/12:JLP: Proposed Corrective Action Review of technical controls that could be put into place. Revisit the Risk Treatment Plan to reflect the change in control value from any lack of segregation and SOA to ensure consistency. Review change management policy and access control policy for segregation of duties where resources permit. Target Date: 31/10/12</p> <p>31/01/13 JLP: Segregation of duty controls have been better defined and applied and although the CTO still has wide access to many systems this is based on a Risk based business need. Additionally an innovative automated approach to enforcing segregation of duties for network changes has been implemented.</p> <p>NC Closed</p>	Segregation of Duties (Network Management)		1207JLP02	A10.1.3 A10.6.1

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYYY<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Minor NC	Closed	<p>Whilst change control is reasonably well defined for software development type activity in the Development Procedure the change control disciplines to be applied to Web based development and changes to the network infrastructure are less clear.</p> <p>Sampling also found:</p> <ul style="list-style-type: none"> • Firewall changes have not gone through formal Change control since 2010. • Personal e-mails provide the main means of initiating, reviewing and authorising changes to Web based developments. • There is no traceability in the Bug Tracking Tool of the requirements relating to any Web based changes or indeed traceability of any testing/proofing, review and authority to go live and customer acceptance. 	<p>10/07/12:JLP: Proposed Corrective Action Carry out a review of the procedures and full root cause analysis to ensure the procedures are sufficient and appropriate. Internal training on the use of the change control system and the review board. The process is to be re-audited to ensure the process is being followed. Target Date: 31/10/12</p> <p>31/01/13 JLP: Change control has been reviewed, process improvements made and the procedures and SOA updated accordingly. Additionally an innovative automated approach to enforcing segregation of duties for network changes has been implemented.</p> <p>NC Closed</p>	Change Control		1207JLP03	A10.1.2 A12.5.1

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYMM<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



Grade 1	Status 2	Finding (including location if applicable) 3	Correction, root cause & corrective action review 4	Process / aspect 5	Date 6	Reference 7	Clause 8
Minor NC	Closed	<p>Whilst there are some procedures in place for the management of 3rd party suppliers (Policy document and preferred supplier list in Drop Box shown), the measures in place fall short in terms of setting out supplier selection evaluation criteria and the maintenance of records relating to any service reviews/performance evaluation activity</p> <p>Sampling also revealed that there was missing and/or incomplete 3rd party contractual/service level documentation for one or two key suppliers for example: Xelerance Corporation (DNS SEC Signers) and Message Labs (Semantic Cloud Mail Services), Mr Don Baladsan (Financial Services). (See also requirements for ISO 9001:2008 7.4.).</p>	<p>10/07/12:JLP: Proposed Corrective Action Introduce a new supplier evaluation form and expand the supplier list to include all service providers outside of IT. Carry out a document audit on contracts, SLA's and confidentiality agreements. Add onto the quarterly checklist a review of all contracts due to expire in the following quarter. Target Date: 31/08/12</p> <p>31/01/13 JLP: Whilst there was good evidence of process improvements being made the NC is to remain open pending further evidence of the implementation of effective implantation of corrective action covering all aspects of supplier management and control. NC Remains Open</p> <p>17/10/13 JLP: There was sufficient evidence presented to demonstrate effective implementation of the policies and requirements relating to supplier and Third Party Service Delivery management. NC Closed</p>	3rd Party Service Delivery Management	10 Jul 12	1207JLP01	A10.2 ISO 9001 7.4

1. Grading of the finding *

2. New, Open, Closed

3. Description of the LRQA finding

4. Review by LRQA

5. Process, aspect, department or theme

6. Date of the finding

7. YYMM<Initials>seq.#

8. Clause of the applicable standard

* Major NC = Major nonconformity

Minor NC = Minor nonconformity



7. Audit Programme/Plan

Visit Type	SV1	SV2	SV3	SV4	SV5/Focus Visit			Certificate Renewal
Due Date	Jan 13	Jul 13	Jan 14	Jul 14	Jan 15			Jul 15
Start Date	25 Jan 13	17 Oct 13	12 Mar 14	4 Aug 14				
End Date	25 Jan 13	17 Oct 13	12 Mar 14					
Audit Days	1	1	1	1				
Any change in workforce numbers That may impact visit duration (if yes add new number)	N	Y (circa 20 in total)	N	Y/N	Y/N	Y/N	Y/N	Y/N
Process / aspect / location								
Final selection will be determined after review of management elements and actual performance								
ISO 9001:2008 Management System Elements	x	X	x	X	x			x
ISO 27001:2005 Management System Elements (4.1 to 8.3 inc) A.5, A.6)	x	X	x	X	x			x
Senior Management Interview	x		x		x			x
Risk Assessment & Treatment	x	X	x	X	x			x
SOA	x	X	x	X	x			x
Marketing					x			x
Business Development				X				x
Finance/Purchasing		X						x
Customer Services/Account Management/Complaint Management		X						x
Asset Management (A.7)			x		x			
HR - Information Security Awareness, Training, Starters & Leavers (A.8)			x					x
Physical Security (A.9)	x			x				x
3 rd Party Service Delivery Management (A.10.2)	x	X (NC only)						x
Technical Operations and Support (A.10, A.11)			X					x
Change Management (A.10.1.2)	x				x			x
Projects/Design & Development (A.10, A.11, A.12)	x	X (NC only)	X (NC only)					x
Incident Management (A.13)	x	X		x				x
Business Continuity Management (A.14)		X						x
Compliance (A.15)	x		x		x			x
Off-site Data Centre (Qube) (A.10.2, A.10)								x
27001:2013 transition				x				
Use of LRQA Logo	x	X	x	x	x			x

Scope	The provision of innovative, reliable and flexible registry services for ccTLD, gTLD and private domain name registries. In accordance with the Statement of Applicability v1.2.1
-------	---



Lloyd's Register
LRQA

Exclusion

ISO9001:2008 7.5.2 & 7.6
SoA: A11.5.6 and 12.5.5

8. Next visit details

Visit type	SV4				
Theme(s) for Next Visit	Compliance(Transiiton)				
Audit days	1	Due date	Jul 14	Visit start / end dates	4 Aug 14
Locations	Moorgate, London EC2R 6AR				
Activity codes	007802, 007850, 108301				
Team	J.Akers				
Standard(s) / Scheme(s)	ISO 9001:2008, ISO/IEC 27001:2013				
Remarks and instructions					
Transition to 2013 is planned for this visit.					



LRQA Findings Log definitions and information

Definitions of Grade Findings

Major Nonconformity

The absence of, or the failure to implement and maintain, one or more management system elements, or a situation which would, on the basis of the available objective evidence, raise significant doubt of the management to achieve:

- *the policy, objectives or public commitments of the organisation*
- *compliance with the applicable regulatory requirements*
- *conformance to applicable customer requirements*
- *conformance with the audit criteria deliverables.*

Minor Nonconformity

A finding indicative of a weakness in the implemented and maintained system, which has not significantly impacted on the capability of the management system or put at risk the system deliverables, but needs to be addressed to assure the future capability of the system.

Objectives of the visit

For all visits:

- *using the LRQA Business Assurance methodology to help clients manage their systems and risks to improve and protect the current and future performance of their organisation*
- *with the exception of Stage 1 visits, to address all issues outstanding from previous visits and any changes to the client's organisation or system that impacts on the approval (or potential approval) which will be recorded as visit specific objectives within the report.*

Stage 1:

- *the assessment of the design and definition of the system to confirm conformity with certification requirements such as the assessment criteria and certification scope*
- *the assessment of the client's self governance, the essential indicators, including the process for the assessment of risk (EMS and OHS), internal audits and management review*
- *the confirmation of the contractual arrangements. This includes any changes required as a result of the outcome of the Stage 1 visit (including changes to the scope of assessment, duration of the Stage 2 visit, and duration of subsequent surveillance visits)*
- *the determination of the planning, logistics, sampling, etc. that will be used during the Stage 2 visit.*

Stage 2: *The assessment of the implementation of the management system. This is to confirm conformity with certification requirements such as the assessment criteria and certification scope.*

Surveillance: *To determine that the client's system continues to meet the assessment criteria and certification scope.*

Certificate Renewal Planning / Focus: *To review the system and the performance of the company during the previous certification cycle, to see how the client plans to move forward in the future and to plan the Certificate renewal visit while confirming continued compliance with the assessment criteria and certification scope.*

Certificate Renewal: *The re-assessment of the implementation of the management system based on the results of the certificate renewal planning visit. This is to re-confirm conformity with certification requirements such as the assessment criteria and certification scope.*

Special Surveillance: *To review the effectiveness of the correction and corrective action taken after the raising of a Major Nonconformity at a surveillance visit.*

Follow-up: *To review the effectiveness of the correction and corrective action taken after the raising of a Major Nonconformity at a Stage 2 or Certificate Renewal.*

Change to Approval: *The assessment of the implementation of the management system for an additional site or activity, which expands the existing scope of approval.*

Additional information

Isolated issues and opportunities for improvement

Any isolated issues identified during the assessment, which have not resulted in a nonconformity being raised, we will record in the appropriate process table in the report.

If we identify opportunities to improve your already compliant system, we will either record them in the process table applicable to the area being assessed, or in the Executive summary of the report if they can deliver improvement at a strategic level.

Confidentiality

We will treat the contents of this report, together with any notes made during the visit, in the strictest confidence and will not disclose them to any third party without written client consent, except as required by the accreditation authorities.

Sampling

The assessment process relies on taking a sample of the activities of the business. This is not statistically based but uses representative examples. Not all of the detailed nature of a business may be sampled so, if no issues are raised in a particular process, it does not necessarily mean that there are no issues, and if issues are raised, it does not necessarily mean that these are the only issues.

Terms and conditions

Please note that, as detailed in the Terms and Conditions clause of the contract (1.7), clients have an obligation to advise LRQA of any breach of legal, regulatory, or statutory requirements and any pending prosecution. Although proportionality and scale of the situation should be considered, you are required to advise LRQA of any serious potential risks to our certification but not, for example, isolated cases of a minor nature.

"The Client is required to inform LRQA as soon as it becomes aware of any breach or pending prosecutions for the breach of any regulatory requirements relevant to the Certified Management System. LRQA will review the details of any breaches brought to its attention and may elect to perform additional verification activities chargeable to the client to ensure compliance with specified requirements. LRQA reserves the right to suspend or withdraw certificates of approval / verification statements and opinions for both failure to inform LRQA and the appropriate regulator of such breaches".

LRQA information

The client is also reminded of the information and guidance available to them from our website (www.lrqa.co.uk). This includes information on our QMS, EMS, OHSAS, Verification and Validation products, our Training Services, and our CE Directives products.

Information is also available from www.lrqa.com.