# YOUR RISK ASSURANCE PARTNER

**nqa.**

**OUR PURPOSE**

IS TO HELP CUSTOMERS DELIVER PRODUCTS THE WORLD CAN **TRUST**

LONDON

BOSTON

SHANGHAI

BANGALORE

TRUSTED GLOBALLY
OVER **30** YEARS
SINCE 1988

**100%** TRANSPARENT FEES

**50,000** CERTIFICATES GLOBALLY

**1000+** EMPLOYEES WORLDWIDE

AVERAGE CUSTOMER PARTNERSHIP **10** YEARS

OVER **90** OPERATING COUNTRIES

# INFORMATION SECURITY ASSURANCE MANAGER

**Tim Pinnell**
BSc, MSc, PCIP, CIPP/E, CISMP

Tim has worked in telecommunications cyber and information security for over twenty years. From the early World Wide Web days to today's globally connected information services, Tim brings a wealth of experience in security, compliance and governance.

Throughout his career he has played a leading role in adopting, consulting and implementing information security compliance standards, including ISO 27001, PCIDSS and Cyber Essentials; helping organizations understand the risks facing their businesses and the controls needed to mitigate them.

With experience as an information security consultant previously, when helping organizations understand risk in business and in technical terms has been paramount, He has many years' experience in supply chain and internal security auditing.

In his last two years before joining NQA he was a data protection officer where he implemented GDPR and a compliance regime. Tim is also a Lead Auditor for Quality and Information Security, this allows him to get an understanding of client's needs and industry requirements, putting NQA in a unique position, to be at the forefront of standards and industry changes.

# RISK ASSURANCE ACCREDITATION

**NQA is a leading UKAS and ANAB Accredited Certification Body.**

We believe in the integrity of standards and rigor of the certification process. That's why it's our policy to achieve accreditation for our services wherever possible.

NQA holds Cyber Essentials certification which demonstrates our commitment to cyber security as well as ensuring we have the right processes in place to guard us against the most common cyber threats. Cyber Essentials is managed by the National Cyber Security Centre (NCSC) and is a required pre-requisite for any organization undertaking work for the UK government.

## SPECIALISTS IN SUPPORTING ORGANIZATIONS FOR RISK ASSURANCE

**Our auditors have extensive knowledge and experience in:**

- Information Resilience
- Risk Mitigation and Management
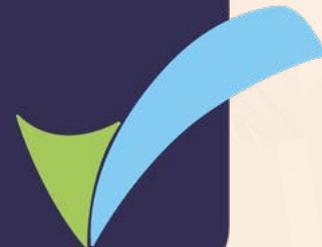- Supply Chain Security
- Corporate Governance

Our dedicated in-house team also possess excellent knowledge of risk assurance and are experienced in assisting clients through their certification journey.

UKAS MANAGEMENT SYSTEMS

015

ANAB ACCREDITED
ISO/IEC 17021
MANAGEMENT SYSTEMS CERTIFICATION BODY
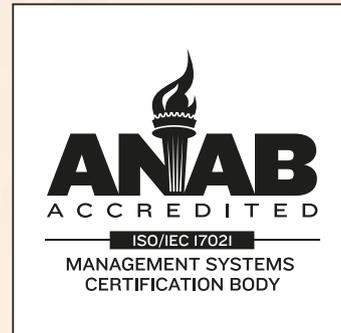
CYBER ESSENTIALS

**14%** INCREASE OF **ISO 27001**
VALID CERTIFICATES WORLDWIDE (2018-2019)

**12%** INCREASE OF **ISO 22301**
VALID CERTIFICATES WORLDWIDE (2018-2019)

*correct at time of print

# ABOUT US

We provide accredited certification, training and support services to help organizations improve their processes, performance, products and services.

## WE SPECIALIZE IN MANAGEMENT SYSTEM CERTIFICATION FOR:

- Information Security
- Business Continuity
- Quality
- Environment
- Energy
- Health and Safety
- Food Safety
- Medical Devices (Quality)
- Asset Management
- Aerospace (Quality)
- Automotive (Quality)

## OUR VALUES

Our values are focused on customer service and integrity. We are committed to supporting each of our clients on a day to day basis to ensure they get the best service possible to support them with implementing the management systems most suited to their organization/industry.

**Our values are at the core of everything we do, we believe in:**

- ✔ Quality customer service
- ✔ Respect for the individual
- ✔ Organizational integrity
- ✔ Stewardship to stakeholders
- ✔ Embracing and driving change
- ✔ One enterprise approach
- ✔ The best people make the best teams
- ✔ Personal and organizational growth

# OUR TEAM

**With the development of technology and advancing threats every day, more and more organizations are turning to management systems to manage and mitigate the risk. At NQA we have a dedicated team of experts that focus solely on our risk assurance client base.**

We recognise that the risk assurance standards are tough on our clients and sometimes you need that little extra support and help with the management and requirements of the scheme. The Information Assurance Business Unit within NQA was set up to provide this additional support and has a team of technical experts.

# ASSESSMENT TEAM

For more than two decades, NQA has been a valued partner to IT and information security businesses adopting ISO or other standards. Our team of internationally recognized auditors can assist you at all stages of the certification process, providing a dedicated team associated to your location to simplify matters from start to finish.

Information security management certification is often viewed as a stressful process, but it doesn't have to be. At NQA, our goal is to help you adopt the system that is best for your business — our approach to certification is results-driven and performance-based rather than bureaucratic. With a global team of auditors, we have a truly international reach. Our affordable rates also mean we are positioned to serve clients of any size.

# OUR CLIENTS

**We provide certification, training and support services to help organizations improve their processes, performance, products and services.**

We work with many large and small organizations to ensure that information is managed through a risk based approach. Management systems can ensure that information resilience and risk mitigation is a focal point of corporate strategy as well as becoming a part of everyday business practice.

NQA is able to understand, service and support each individual client and we are proud to be working with innovative and ground-breaking organizations.

# RISK ASSURANCE STANDARDS

We are passionate about helping our clients to improve their products, processes and people so they can manage and mitigate the risks associated with data and information. Our approach is pragmatic and supportive whilst meeting the rigorous technical demands and integrity of accredited certification.

## Certification to these standards helps you with:

- Asset protection
- Threat mitigation
- Proving business credentials
- Data breaches
- Customer satisfaction
- GDPR
- Supply chain security
- Emergency preparedness

## ISO 27001:2013

The standard for organizations that provide continued confidentiality, integrity and availability of information as well as legal compliance.

ISO 27001 implementation is an ideal response to customer and legal requirements such as the GDPR and potential security threats including: cyber crime, personal data breaches, vandalism / terrorism, fire / damage, misuse, theft and viral attacks.

## ISO/IEC 27701:2019

The standard, ISO/IEC 27701:2019 is a data privacy extension to ISO 27001.

This newly published information security standard provides guidance for organizations looking to put in place systems to support compliance with GDPR and other data privacy requirements. ISO 27701, also abbreviated as PIMS (Privacy Information Management System) outlines a framework for Personally Identifiable Information (PII) Controllers and PII Processors to manage data privacy.

This reduces risk to the privacy rights of individuals and to the organization by enhancing an existing Information Security Management System.

## ISO/IEC 27017:2015

The standard for security control for cloud services and is an extension to ISO/IEC 27001 and ISO/IEC 27002.

The standard advises on both the cloud service customers and cloud service providers. ISO 27017 is designed to help you and your organizations when selecting security controls for cloud services when implementing a cloud computing information security management system.

## ISO 22301:2019

The standard is designed to help organizations prevent, prepare for, respond to and recover from a wide range of potential threats and disruptions including: technology failure, sudden loss of critical resources, natural disasters, terrorist attacks and other emergency situations.

This standard may be right for your organization if you need to demonstrate to stakeholders that your organization can rapidly overcome operational disruption to provide continued and effective service.

## ISO 20000-1

This standard is designed to help organizations deliver effective managed IT services to customers and maintain those standards over time.

ITSMS implementation is designed to be a bedrock upon which to build continually improving service management systems. It is fully scalable to organizations large and small or to customers internal and external.

## CMMC

The standard for implementing appropriate level of cybersecurity across the supply chain of the defence industrial base.

The Cybersecurity Maturity Model Certification is the latest verification method put in place by the Department of Defense. This certification is the Department's first attempt to set clear requirements for contractors when it comes to cybersecurity.

# INDUSTRY INVOLVEMENT

## WEST MIDLANDS CYBER RESILIENCE CENTRE (WMCRC)

The Cyber Resilience Centre for the West Midlands is part of the national roll out of Cyber Resilience Centres in the UK which began in 2019. The WMCRC began its journey in June 2020. Lead by West Midlands Police, and facilitated by Business Resilience International Management (BRIM), they have followed a structured modular programme based on a highly successful model that had previously been established for over 9 years in Scotland.

The Advisory Group fulfils a very important function in the establishment and development of the Cyber Resilience Centre. The Advisory Group is key to assisting with the reach of the CRC to the many varying types and sectors of business across the West Midlands region.

Being an advisory member of the WMCRC gives us an opportunity to engage and develop the cyber resilience of businesses in the region. Connecting with organizations, sharing cyber experience and knowledge, is paramount to building a secure and resilient UK PLC. NQA is a member of the advisory group.



## ISO 22301

NQA is highly involved in a wide variety of industry committees and standards writing teams, helping us to maintain a keen awareness of changes within this standard. NQA is an active participant and recognized leader in the DHS PS-Prep and IAF BCMS working groups (convened by ANAB).

With a wealth of experience providing accredited management systems certifications, NQA is ideally placed to partner with you to meet customer requirements and exceed industry expectations.

NQA issued the first-ever PS-Prep certification in 2012. NQA is the only Certification Body to offer the full suite of ISO and PS-Prep BCMS certifications including: ASIS SPC.1, ISO 22301 and NFPA 1600.

## CMMC

The Cybersecurity Maturity Model Certification (CMMC) lays a framework to implement cybersecurity policies and practices for organizations throughout the US Defense Industrial Base (DIB).

NQA has been an active participant in the development of the CMMC Program and stands well-positioned to provide CMMC audits. As the DoD's CMMC (Cybersecurity Maturity Model Certification) Program continues to roll along and reach closer to the first DoD RFP's calling out CMMC requirements, NQA continues to be heavily involved in this new program and has recently achieved preliminary approval as a CMMC C3PAO (Certified 3rd Party Assessor Organization).

# MEMBERSHIPS

The Armed Forces Covenant is not a charitable organization. It is a promise from the nation to those who serve or who have served, and their families, which says we will do all we can to ensure they are treated fairly and are not disadvantaged in their day-to-day lives. The Covenant Scheme enables employers to publicly declare their support for Defence personnel. The pledge is voluntary and Employers are able to tailor their pledge to the needs of their business.

NQA has pledged to support the Armed Forces community, including existing or prospective employees who are members of the community. This recruitment and maintenance programme is not considered a short term goal for NQA, it's something we are incorporating into every-day business and we will continue to strive to offer further support to our ex-service men and women following their time in the military.

**ARMED FORCES COVENANT**

Employer Recognition Scheme

SILVER AWARD 2018
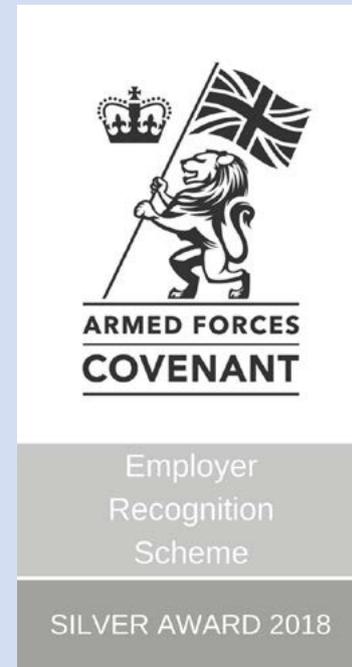
# BEYOND CERTIFICATION

Certification is one element of what the Risk Assurance Business Unit is there for but some organizations require either more management or additional support.

NQA run regular training events for the scheme which include Lead and Internal Auditor courses. The courses are held throughout the year and can be found on the NQA website. Regular training is also held through webinars and seminars, all of which are free to attend and will be hosted by one of our technical experts.

For our larger clients who have a number of sites within their certification we project manage their program for them.

Key account managers are assigned and regular meetings set up tailored to the client's individual needs.

Quarterly strategic reviews will review trends and audit findings to allow clients to focus on key areas of concern/ opportunities. Change management is another common problem with larger organizations as structures and facilities change rapidly, NQA help to manage these changes relating to your certification during the quarterly strategic reviews.

We also utilise these meetings to share knowledge in current and future needs and highlight certification changes which will impact the organizations management system.

# KNOWLEDGE TRANSFER

Involvement with industry stakeholders is vital to the success of NQA and it's what sets us apart from our competitors. Our involvement with the committees and forums allows us to transfer knowledge both internally and externally to the business. The first phase of the process is to transfer the knowledge gained internally to our employees and auditors, raising their awareness and subsequent support for our client base. The second phase is to transfer the knowledge to our clients and their supply chain as well as industry stakeholders themselves, it's a two way knowledge transfer process not just us listening to them. By transferring knowledge to the various different groups we are addressing the following needs:

## INTERNALLY

- Customized focussed customer interactions
- Communication to understand needs & customer 'care-abouts'
- Adaptive to business & isms needs
- Operational interface and oversight
- Cost focus for budget management

## EXTERNALLY

- Knowledge and awareness due to industry involvement
- Application of industry/ technical structure to:
  - Address more complicated isms
- Solution needs
  - Stay abreast of emerging industry risks
  - Provide knowledge transfer interactions

INDUSTRY KNOWLEDGE

Manufacturers

Operations

Downstream Customers

SOLUTIONS

Sales

Suppliers and Service Providers

Auditors

Industry Groups and Committees

INDUSTRY KNOWLEDGE

# DEDICATED ACCOUNT MANAGEMENT

We understand the challenges facing Risk Assurance on a daily basis. That's why, when you apply for certification with NQA, you will receive the details of your dedicated account executive. This individual will be your sole point of contact and will be able to answer any questions you may have as well as giving direct support to your auditing team.

Our Client Executives are members of the Certification Body Management Committee and get first-hand knowledge on future changes which will impact our clients.

# DIGITAL REALTY

**ISO 9001, ISO 14001, ISO 27001, ISO 45001 and ISO 50001**

**Digital Realty powers the world's increasingly digital economy. The company supports the data center, colocation and interconnection of more than 2,000 organizations across five continents, 14 countries and more than 210 data centers. Its customers include companies of all sizes across many sectors, including communications, information technology, financial services, energy, healthcare, manufacturing, consumer products and more.**

**Digital Realty provides its customers with global strength, local expertise and exceptional reliability. The firm boasts 12 consecutive years and counting of 99.999% uptime, the best in the industry.**

In everything it does, Digital Realty is dedicated to quality, information security, sustainability and health and safety. The company has robust physical security and cybersecurity systems in place that include surveillance systems, access control systems, multi-factor authentication protocols and continuous monitoring. These systems protect against cyberattacks, theft, natural disasters, accidental damage and other threats. Digital Realty is also committed to developing efficient, environmentally responsible data centers that help its customers reach their sustainability goals. Since 2007, it has achieved more than 60 sustainable building certifications, and more than half of its certified projects have earned Gold or Platinum equivalent ratings.

# FINDING CERTIFICATION SUCCESS

To find success on the road to certification, Digital Realty knew it needed a commitment from senior management to secure appropriate resources to the program, gain stakeholder support and encourage active engagement in corrective actions to drive continuous improvement. NQA ensured it had this commitment, which helped Digital Realty to find success in the initial certification process and over the long term.

Through this process, Digital Realty successfully achieved certification to all five ISO standards — ISO 9001, ISO 14001, ISO 27001, ISO 45001 and ISO 50001 — since initial certification in Q4 2011. The company was also able to improve its operations and continues to do so today through its commitment to continual improvement. Certification to these standards provides Digital Realty with an auditing platform that helps to identify operational non-conformances, provides effective root cause analysis and drives corrective action across the organization. They also provide senior management with a monitoring tool that gives them insight into how actions align with corporate goals and procedures. Crucially, the certifications boost consumer confidence in Digital Realty's operations and help ensure that the company is meeting all local legislative requirements.

As Digital Realty continues to expand into new global markets, it maintains compliance with the standards of its ISO certification. NQA remains a partner for Digital Realty in the certification process, helping Digital Realty to improve its operations and increase customers' confidence in the company.

# COMPLEMENTARY STANDARDS

**NQA clients often integrate their Management Systems across more than one standard to reduce duplication, achieve efficiency and maximize performance.**

The following standards may be used to complement existing management systems for organizations.

## QUALITY MANAGEMENT
### Key benefits of ISO 9001

- Customer satisfaction
- Operational efficiency

## ENVIRONMENTAL MANAGEMENT
### Key benefits of ISO 14001

- Environmental policy
- Corporate responsibility

## HEALTH & SAFETY MANAGEMENT
### Key benefits of ISO 45001

- Improve productivity
- Enhanced occupational health measures

## ASSET MANAGEMENT
### Key benefits of ISO 55001

- Effective management of value, risk and reliability
- Personal and process safety

## COLLABORATIVE RELATIONSHIP
### Key benefits of ISO 44001

- Supports mutual understanding between organizations
- Reduced operating costs

## MEDICAL DEVICES MANAGEMENT
### Key benefits of ISO 13485

- Traceability and recall
- Legal Compliance

# JOURNEY TO CERTIFICATION

| Client submits quote request form | → | NQA reviews and submits quote (client is contacted within 24 hours) | → | Quote is accepted and contracts are signed | → | Scheduling team book Stage 1 Audit |

## STAGE 1 AUDIT COMPLETED

| Requirements met | Requirements not met |
|---|---|
| Report issued | Report issued |
| Stage 2 Audit planned | Time given to rectify issue |

## STAGE 2 AUDIT COMPLETED

| Requirements met | Requirements not met |
|---|---|
| Report issued | Report issued |
| Certification recommended | Non-conformances corrected and corrective action verified |

# CERTIFICATION AWARDED

3 year validity and surveillance audits to maintain certification

# CERTIFICATION TRANSFER

**Not all certification bodies are the same. At NQA we focus on providing you (our clients) with what you deserve - value for money and great service! That means certification that helps to improve your organization as well as meeting the requirements of your chosen standard.**

If you hold certification with an accredited certification body, you can transfer this to NQA. It doesn't matter if your management system and certification is for one standard or multiple standards, for a single or multiple sites – the process is really simple.

1. You send us your current certificate and latest audit reports, alongside your evidence of closure of any non-conformances.

2. We conduct a transfer audit for each certificate. Our Assessors will make this process as seamless and painless as possible.

3. Upon successful completion, we will issue you with an NQA certificate of registration with the same validity as your previous certificate.

4. You will be assigned an Assessor and will enter your ongoing audit program with NQA.

**To request a transfer quote visit nqa.com/certification/transfers**

# CERTIFICATION TRAINING

In addition to supporting your organization in gaining certification, we offer a range of training options from self-paced learning through to lead auditor training, for Information Security Management standards and more.

## Risk related training include:

| COURSE DETAILS | LEVEL | DURATION | PRICE |
|---|---|---|---|
| NQA ISO 27001 ISMS (Information Security) E-Learning Introduction Training | 1 | 0.5 Days | £150.00 |
| CQI and IRCA Foundation Introduction To Risk Management Training | 1 | 2 Days | £699.00 |
| NQA ISO 27701 ISMS (Information Security) Introduction and Implementation Training | 1 | 2 Days | £699.00 |
| NQA ISO 27001 ISMS (Information Security) Introduction and Implementation Training | 1 | 2 Days | £699.00 |
| CQI and IRCA ISO 27001 ISMS (Information Security) Internal Auditor Training | 2 | 2 Days | £699.00 |
| CQI and IRCA ISO 27001 ISMS (Information Security) Lead Auditor Conversion Training | 3 | 3 Days | £950.00 |
| CQI and IRCA ISO 27001 ISMS (Information Security) Lead Auditor Training | 3 | 5 Days | £1350.00 |
| NQA Advanced Training - Managing Information Security whilst Working Remotely | 3 | 0.5 Days | £150.00 |
| NQA Advanced Training - Operational Resilience Planning | 3 | 0.5 Days | £150.00 |

**To learn more about training options, visit nqa.com/training**

# ADDITIONAL MATERIALS

## Gap Analysis
https://www.nqa.com/en-gb/certification/gap-analysis

## Implementation Guides
https://www.nqa.com/resources/news/implementation-guides

## Webinars
https://www.nqa.com/en-gb/resources/events