PROFILE

ROBERT J TOOGOOD

MSc (Risk Management) SIRM M.ISRM MAPM

FRACTIONAL DIGITAL RISK AND RESILIENCE SPECIALIST

18 Homefield, Royal Wootton Bassett, SWINDON, Wiltshire, SN4 8DE, United Kingdom

Office: +44 (0)1983 617241
Email: robert_toogood@projectsystemssupport.com

LinkedIn: https://uk.linkedin.com/in/roberttoogood

OVERVIEW

As an independent digital risk and resilience specialist, I enjoy helping clients navigate and solve difficult compliance challenges in the digital space. With proven expertise in compliance remediation for enterprise, programme and technology risk management (including cyber, privacy, and AI governance), I deliver value by providing pragmatic advice and hands-on support.

When partnering with me, you benefit from over thirty years of real-world project turnaround and compliance remediation experience. This is based on a successful systems and project management background working on business transformation and M&A programmes with clients across Europe, Middle East and Africa (EMEA). Prior to that, my career started in the banking sector before spending time in other highly regulated sectors such as financial services and healthcare.

My broad digital risk and resilience experience begins in 2002, initially with Johnson & Johnson and their business continuity activities within the UK (and later involvement with Sarbanes-Oxley (SOX) compliance and pandemic planning preparations). Since then, I have continued working with many other clients and related areas including operational resilience, compliance transformation, data governance, third-party risk management (TPRM) and holistic GRC, as well as enterprise risk management itself.

This breadth and depth of experience allows me to seamlessly transition between roles within an assignment when needed, from strategic advising to hands-on execution. Finally, as part of my commitment to lifelong learning, I completed a Data Analytics Bootcamp last year and have just been accepted on an AI Leadership Skills Bootcamp at the University of Portsmouth to enhance and refine my skills in this important area.

Typical roles undertaken for clients, often on a fixed-price or part-time, fractional basis include compliance remediation, project turnaround, advisory and assurance services, as well as mentoring and critical friend support.

Previous clients and employers include: Grant Thornton, NHS England, Brown Rudnick, Greene King, Johnson & Johnson EMEA, JD Edwards (JDE)/Oracle, Alpharma, Amersham Biosciences, Arjo Wiggins, Christofle/LBDe, Pall Europe, WH Smith Business Supplies/Niceday, Sun Life Assurance of Canada, Dun & Bradstreet, Rank Xerox, TSB Trust Company, Hambro Life Assurance, SavaCentre, Bank of Ireland/British Credit Trust… to name but a few.

EXPERIENCE

In one of my latest assignments, I have been the interim Risk and Sustainability Lead (and Subject Matter Expert) for a major cyber resilience improvement programme; during this assignment, I reviewed the effectiveness of risk management processes within the programme, aligned with HMG Orange Book and ISO 31000 frameworks, as well as taking an operational role within the PMO and Programme Board. On other recent assignments, I have:

- Advised as member of Information Governance Committee on matters related to digital risk and resilience, and am currently providing hands-on guidance on an artificial intelligence (AI) governance implementation
- Reviewed enterprise risk management frameworks, business continuity and resilience plans (including ISO 31000, 27001, 22301, and 22316 aspects
- Developed and implemented business continuity, pandemic and resilience plans
- Reviewed cyber and information security as well as ICT governance based on NIST Cybersecurity Framework (CSF), ISO 27001, GDPR, and NHS Digital DSPT which also includes NCSC Cyber Essentials Plus, Cyber Assessment Framework (CAF) and EU Network and Information Systems (NIS) Directive requirements
- Reviewed digital strategy to ensure fit-for-purpose, and being implemented through effective governance
- Prepared for implementation of ISO 27001, as well as assisting with remediation reviews of existing implementations due to data breach and other non-conformance events
- Delivered initial cyber and information security related gap assessment actions including preparation of associated policies and procedures
- Reviewed third-party risk management (TPRM), through active participation in preparing records of processing activities (ROPA) and data protection impact assessments (DPIAs)
- Developed defensible position on GDPR compliance
- Reviewed data privacy compliance activities and prepared remediation plan to address areas for improvement
- Setup GDPR compliance programme, based on use of a Nymity (PMAF) approach
- Selected and implemented (pilot) privacy management software (OneTrust)

- Completed detailed review of existing information security (including cyber) policies and procedures to identify changes needed, including new Privacy by Design (PbD) requirements
- Completed all outstanding information security compliance (including data privacy/PIA) activities relating to Business Intelligence projects within EMEA
- Implemented new System Development Lifecycle (SDLC) into EMEA Business Intelligence team
- Prepared for internal Corporate Audit visit with focus on Sarbanes-Oxley (SOX) EMEA compliance activities
- Implemented requirements of Sarbanes-Oxley (SOX) across both UK Finance and IT functions
- Implemented Records and Information Management (RIM) into multiple sites

STRENGTHS

- Enjoy troubleshooting difficult challenges and problems
- Relish dealing with complexity, uncertainty and ambiguity
- Comfortable within large-scale, global initiatives as well as country/location specific activities
- Effective in decentralised, centralised, matrix as well as virtual organisations
- Benefit from strong systems background with extensive hands-on business experience
- Critical and holistic thinker, delivers pragmatic, value-driven innovative solutions
- Communicate effectively at all levels, including boards and executive teams
- Believe in collaborative power of working through people to make things happen

PROFESSIONAL ENGAGEMENT AND RECOGNITION

MSc Risk Management (Distinction), 2013
Technical Specialist Member, Institute of Risk Management (SIRM)
Member, Institute of Strategic Risk Management (M.ISRM)
Member, Association for Project Management (MAPM)
Member, Chartered Institute of Internal Auditors (IIA)
Affiliate Member, Global Association of Risk Professionals (GARP)
Member, Information Systems Audit and Control Association (ISACA)

EXPERTISE AND INTERESTS

GOVERNANCE incl Programme & Project Governance; Project Turnaround & Remediation; Project Assurance; Project Management; Portfolio Management; Programme Management; Programme & Project Management Office (PMO); Business Transformation; Change Management; Methodologies (ITIL, PRINCE2, COBIT, MSP, P3M3, P30, DevOps, Agile/Extreme etc); PMI PMBOK; APM BOK; Cyber Security Governance; ICT Governance; Digital Governance; Artificial Intelligence (AI) Governance; Information Governance; Data Governance; Sustainable Project Management (GPM); Green PMO; ESG/Sustainability Governance

RISK incl Enterprise Risk Management (ERM); Operational Risk Management (ORM); Holistic GRC; Technology & Digital Risk Management; Cyber Risk Quantification; ISO 31000; HMG Orange Book; Control Frameworks (COSO, COBIT, NIST CSF, CIS, NCSC); Information Security; ISO 27001; ISMS; Cyber Security; Supply Chain Risk Management (SCRM)/Third-Party Risk Management (TPRM)/Business Resilience (IT Resilience/Technology & Digital Resilience/Cyber Resilience/Data Resilience/Operational Resilience/Organisational Resilience/Strategic Resilience/Adaptive Resilience & Culture); ISO 22336, ISO 22316; FCA PS21/3 - Building Operational Resilience Policy; Digital Operational Resilience Act (DORA); Network and Information Systems (NIS/NIS2) Directive; Emergency Preparedness, Resilience & Response (EPRR); Business Continuity Planning (BCP); ISO 22301; Crisis Management; Incident Management; Disaster Recovery; Pandemic Planning; Risk Intelligence; ESG, Climate & Nature Risk

COMPLIANCE incl Compliance Transformation, Compliance Analysis; Systems Development Lifecycle (SDLC); Sarbanes-Oxley (SOX); UK Corporate Governance Code - Provision 29; Records & Information Management (RIM); Data Protection; Privacy; General Data Protection Regulation (GDPR); UK Data Protection Act 2018; Privacy by Design (PbD); NHS Data Security & Protection Toolkit (DSPT); NCSC Cyber Assessment Framework (CAF); Secure by Design; ESG and Sustainability Standards and Frameworks (incl Net Zero; Global Reporting Initiative (GRI); Corporate Sustainability Reporting Directive (CSRD); TCFD/TNFD; ISSB/IFRS S1/S2); Sustainable IT; Net Zero Transition Planning

CLIENT FEEDBACK (DELIVERED VALUE)

"… able to introduce order into a situation that is full of complexity and ambiguity"

"… attention to detail and tenacity in chasing through issues to find people who can make an impact on delivering"

"… expert in making complex processes clear"

"… good at uncovering complexity and trying to make sense of it, to help colleagues understand what's going on"

"… individual of broad vision who recognises the importance of people to achieving quality results"

"… good at both high-level strategic thinking and more detailed "this is what needs to be done urgently" type actions"

"… the ideal right-hand man, bit like Jiminy Cricket sitting on your shoulder reminding you of stuff that needs sorting"

CLIENT ASSIGNMENT SUMMARY

Senior Director
Project Systems Support Limited: February 1992 - Present, UK/EMEA
Management Consultancy (Owner)

Date: 2002 to present
Fractional Digital Risk and Resilience Specialist
Consultant, Subject Matter Expert and Practitioner

NB Specific client names not given below due to NDA restrictions

Date: January 2017 to present
Sector/Client: Various including
Assignments: **Public Sector - Major Cyber Resilience Improvement Programme**
Conducted comprehensive risk management review, aligned with HMG Orange Book and ISO 31000 frameworks, and produced required remediation plan, which was subsequently approved by the Programme Board; also undertook operational Risk and Sustainability Lead (and Subject Matter Expert) role within the PMO and Programme Board.

Public Sector - NHS, Hospice (Pro Bono), Local Government and Central Government
Conducted enterprise risk management framework, business continuity and resilience reviews (including ISO 31000, 27001, 22301, and 22316 aspects); lately, this has included providing advice on artificial intelligence (AI) governance as well as climate and sustainability related matters. In addition, has undertaken information security and ICT governance audits for NHS Trusts based on their compliance with NHS Digital's Data Security and Protection Toolkit (DSPT), which includes elements of NCSC Cyber Essentials Plus and Cyber Assessment Framework (CAF), GDPR, ISO 27001 and EU Network and Information Systems (NIS) Directive. Also reviewed digital strategies to ensure they are fit-for-purpose and being implemented efficiently through effective governance.

Venture Capital Firm
Conducted cyber security audit based on the firm's implementation of the NIST Cybersecurity Framework (CSF) in both their pre-investment cyber due diligence checks and more widely within their global organisation.

International Distribution Group
Provided programme management and GDPR SME support to client on first stage of GDPR remediation work (including delivery of initial information security and cyber security related actions), following earlier gap assessment and other activities.

International Law Firm
Provided high-level programme management support on organisation and delivery of remediation activities to ensure client had a defensible position on GDPR compliance by May 2018. These activities leveraged gap assessment recommendations and stakeholder views on previous approach used. Key members of the client team included US based CIO and other senior members of the Firm, as well as London based SME members of the consultancy team.

UK Pub Retailer and Brewer
Provided SME support to help client setup their GDPR compliance programme, based on the use of a Nymity Privacy Management Accountability Framework (PMAF) approach, working directly for the client's Company Secretary and IT Director. Also, helped client select and then implement (pilot) privacy management software (OneTrust) and assisted with selection of data discovery tools. Finally, completed detailed review of client's information security (including cyber) policies and procedures to identify changes needed, including Privacy by Design (PbD) requirements.

Date: January 2021 to present (part-time)
Sector/Client: Internal (Project Systems Support)
Assignment: **Real-World Research - Operational Resilience and Holistic GRC**
Investigating how operational resilience is influenced when adopting a more coordinated and holistic approach to governance, risk and compliance (GRC/IRM) related activities.

Date: October to December 2016, EMEA/Global
Sector/Client: Medical Devices
Assignment: **Quality Records Inventory Systems User Requirements**
Provided business analysis support to document user requirements for new GxP validated Quality Records Inventory System (QRIS) for use globally across all manufacturing sites, and developed an initial proof-of-concept (POC) based on the Collibra Data Governance solution (including data resilience requirements)

Date: November 2015 - April 2016
Sector/Client: Internal (Project Systems Support)
Assignment: **Workshop Development Project**
Overview: Completed initial research and preparations for new workshop on “Using Risk Management to Innovate within Projects”

Date: August 2015 - April 2016
Sector/Client: Internal (Project Systems Support)
Assignment: **Book Writing Project**
Overview: Wrote chapter on Governance, Risk and Compliance (GRC) for new book on Multi-Dimensional Risk Management that was published by Kogan Page in June 2016

Date/Scope: July 2014 - July 2015, EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **Business Intelligence - Programme/Senior IT Project Management**
Overview: Provided specialist programme/senior project management support to help client develop way of using JDE/SAP transactional and master data from EMEA with IBM Cognos BI/TM1 to feed new global Financial Planning and Analysis (FP&A) application

Date/Scope: 2013-2014, UK
Sector/Client: University of Portsmouth
Assignment: **Doctorate Research - Projects, Systems and Risk**
Overview: Completed first phase of real-world research investigations into how success and costs of complex project activities can be influenced by adopting a more coordinated approach to the management of governance, risk and compliance (GRC) activities. NB Second phase on hold, pending commercial sponsorship. Currently refocused original research objectives to address challenges associated with operational resilience and sustainability related change.

Date/Scope: 2013, UK
Sector/Client: Specialist Consultancy
Assignment: **Risk Assessment Review**
Overview: Conducted risk assessment in response to recent security breach and prepared action plan to help client address weaknesses in ISO 27001 based operating environment

Date/Scope: 2011-2013, EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **Business Intelligence - Programme Compliance Review and Implementation**
Overview: Provided specialist programme management support (risk/compliance) to help client complete as quickly as possible all outstanding compliance (including data privacy/PIA) activities relating to previous/current IBM Cognos based Business Intelligence projects within EMEA and implementation of new System Development Life-Cycle (SDLC)

Date/Scope: 2010-2011, UK/EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **Portfolio Management Implementation**
Overview: Provided specialist project management support (portfolio/risk) to help client implement portfolio management approach to oversee and manage project activity within Finance

Date/Scope: 2009-2010, UK
Sector/Client: Medical Devices & Diagnostics
Assignment: **HR Reorganisation Financial Consolidation**
Overview: Provided specialist project management support (risk) to help client facilitate timely consolidation of all HR budget data associated with recent UK reorganisation

Date/Scope: 2010-2011, EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **M&A Acquisition Integration**
Overview: Provided specialist programme management support (risk/compliance) to help client manage integration of a recently acquired business in all areas outside of US

Date/Scope: 2009, UK
Sector/Client: Medical Devices & Diagnostics
Assignment: **Data Privacy Research**
Overview: Provided specialist support (risk) to help client understand Data Privacy implications of corporate and local country legal requirements

Date/Scope: 2009, UK
Sector/Client: Medical Devices & Diagnostics
Assignment: **Business Continuity and Pandemic Plan Implementation**
Overview: Provided specialist project management support (risk/compliance) to help client develop and implement business continuity, pandemic and data resilience plans for new UK campus facility

Date/Scope: 2008-2009, UK
Sector/Client: Medical Devices & Diagnostics
Assignment: **SOX Audit Preparation**
Overview: Provided specialist project management support (risk/compliance) to help client prepare for forthcoming internal Corporate Audit visit with focus on Sarbanes-Oxley (SOX) compliance activities across Finance functions of UK operation

Date/Scope: 2008-2009, EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **ERP - SOX Interfaces Review**
Overview: Provided specialist project management support (risk/compliance) to help client prepare for forthcoming internal Corporate Audit visit with focus on Sarbanes-Oxley (SOX) system ERP interfaces on shared-service EMEA-wide JDE World ERP solution

Date/Scope: 2008, UK/EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **Records and Information Management (RIM) Implementation Preparation**
Overview: Provided specialist project management support (risk/compliance) to help client understand, develop and implement records information management into two sites (including data resilience)

Date/Scope: 2007-2008, EMEA/Global
Sector/Client: OTC/FMCG
Assignment: **M&A Merger Integration**
Overview: Provided specialist programme management support (risk/compliance) to help client manage integration of a recently acquired business in Europe, Middle East and Africa

Date/Scope: 2007, EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **ERP - Solution Partner RFP Selection**
Overview: Provided specialist project management support (risk) to help client select an IT Solution Partner to support implementation of new EMEA-wide JDE/SAP solution

Date/Scope: 2006-2007, EMEA/Global
Sector/Client: OTC/FMCG
Assignment: **ERP - Implementation**
Overview: Provided programme management support to help client manage the setup of a new programme to facilitate the implementation of a new EMEA-wide SAP solution

Date/Scope: 2005-2006, EMEA
Sector/Client: OTC/FMCG
Assignment: **Portfolio Management Implementation**
Overview: Provided specialist project management support (risk/portfolio) to help client oversee and manage project life-cycle activity across Europe, Middle East and Africa (EMEA) in more controlled and orderly way using portfolio management

Date/Scope: 2005, UK/EMEA
Sector/Client: OTC/FMCG
Assignment: **Reorganisation Facilitation/Support**
Overview: Provided specialist programme management support to help client reorganise EMEA IT organisation

Date/Scope: 2004-2005, UK/EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **SOX Implementation**
Overview: Provided specialist project management support (risk/compliance) to help client implement requirements of Sarbanes-Oxley (SOX) across both UK IT and Finance

Date/Scope: 2002-2003, UK/EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **Business Continuity Plan Implementation**
Overview: Provided specialist project management support (risk/compliance) to help client understand, develop and then implement Business Continuity Plan for two separate sites including data resilience requirements

Date/Scope: 1999 to 2002, EMEA/Global
Sector/Client: Various, Whitehouse Consultants (JDE)
Pharmaceuticals, Medical Devices & Diagnostics; Paper Manufacturer; Luxury Goods Manufacturer; Supplier of Flavour, Fragrance & Cosmetic Ingredients
Assignment: **ERP - Implementation Project Management Consultancy**

Date/Scope: 2001, EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **ERP - European Distribution Centre Integration Support**

Date/Scope: 1999-2000, UK/EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **Y2K Preparation**

Date/Scope: 1997-1999, EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **ERP - Implementation**

Date/Scope: 1997, EMEA/Global
Sector/Client: Medical Devices & Diagnostics
Assignment: **Manufacturing Plant Relocation**

Date/Scope: 1996-1997, EMEA
Sector/Client: Medical Devices & Diagnostics
Assignment: **ERP - Implementation**

Date/Scope: 1995-1996, UK
Sector/Client: Filtration, Separations and Purification (Pall Europe)
Assignment: **Project Management Review**

Date/Scope: 1994-1995, UK, Retail - Office Supplies and Stationery (Niceday)
Assignment: **ERP - Implementation and Business Consolidation**

Date/Scope: 1992-1993, UK, Financial Services (Sun Life Assurance of Canada)
Assignment: **Custom Systems Development and Implementation**

EMPLOYMENT SUMMARY

Date/Scope: 1988 to 1992, UK, Financial Services (TSB Trust Company)
Roles: **Project Manager to Business Systems Manager** (Financial Systems)

Date/Scope: 1985 to 1988, UK/EMEA, Financial Services (Dun & Bradstreet EBIC BV)
Roles: **Project Leader to Project Manager** (Financial Systems)

Date/Scope: 1984 to 1985, UK, Financial Services (British Credit Trust)
Roles: **Senior Systems Analyst to Project Leader** (Financial Systems)

Date/Scope: 1983 to 1984, UK, Hypermarket Retailing (SavaCentre)
Roles: **Senior Systems Analyst** (Financial Systems)

Date/Scope: 1979 to 1983, UK/EMEA, Office Communications (Rank Xerox)
Roles: **Trainee Systems Analyst to Senior Systems Analyst**

Date/Scope: 1976 to 1978, UK, Unit Linked Life Assurance and Pensions (Hambro Life Assurance)
Roles: **Projects Administrator to Systems Developer**

Date/Scope: 1974 to 1975, UK, Banking (NatWest Bank/SG Warburg)
Roles: **Branch Trainee to Eurobond Administrator**