CHURCHILL & HARRIMAN

CHURCHILL & HARRIMAN (C&H) PRE-CERTIFICATION WORK, ASSESSMENT CRITERIA DEVELOPMENT AND CRITICAL SECURITY ARTIFACT PRODUCTION — SUMMARY OF RESULTS

Churchill & Harriman (C&H) provides 20+ years of institutional expertise in architecting remote-based methodologies through which critical security due diligence artifacts are produced against an agreed to standard of care (including ISO, NIST, FSSCC, CMMC), and delivers those artifacts and related work product with efficiency.

We are privileged to serve federal government agencies, institutions whose infrastructure is Designated as "Critical", industry regulators and governing bodies, global public/private consortiums, industry trade groups and global Fortune 100 multi-nationals and additional clients.

CHRONOLOGY — 1997 TO PRESENT

1997	Selected by highly regulated Fortune 100 organizations to develop assessment criteria for the assessment of their critical vendors; execute onsite and remote assessments in alignment with that criteria and report.
1998	Selected to develop Business Continuity and Disaster Recovery Plans for Fortune 100 organizations, today in formal alignment with ISO 22301.
2000	Selected by global Fortune 100 organizations to build out original global information security policies based on BS 7799, today in formal alignment with ISO 27001.
2005	Selected by the Federal Reserve Bank of New York (FRBNY) to perform all pre-certification services and help the bank ultimately earn certification to ISO 27001. THE FRBNY was the very first entity of any kind in North America to earn certification to ISO 27001.
2007	Selected by Global Systemically Important Banks (G-SIB's) to implement ISO 27001.
2007	Selected by Tier One Financial Institutions to implement and execute their third-party risk management program employing the Shared Assessments Program artifacts.
2007–Present	Member of Shared Assessment Program Leadership. Matured AUP/SCA assessment test criteria and SIG Questionnaire criteria year over year.
2008	Developed original third party risk assessment criteria (security, privacy, and compliance) based on ISO 27001 for a Business Process Outsourcer (BPO). Conducted global onsite third party risk assessments, enabling our client to formally satisfy security and privacy requirements contained in a U.S. $1.2B contract awarded by an FDA-regulated customer.

2009	Scope development and execution of a combination NIST 800-53 / AUP Assessment on the internal operations of a Big 4 Advisory Firm.
2010	Selected by a G-SIB to build and execute their global onsite critical supplier vendor assessment program.
2011	Harmonized ISO 27001, ISO 9001, and the ITIL framework requirement for a Fortune 500 market data services provider. Provided extensive pre-certification consulting services ultimately resulting in our client achieving multiple ISO 27001 certifications.
2012	Selected by G-SIBs to settle third-party vendor-specific regulatory findings and to develop and implement vendor risk management programs.
2013	Selected by a U.S. nationwide mobile commerce enterprise and successfully developed and implemented an information security management system (ISMS) under ISO 27001 including enterprise information security controls, policies, and standard operating procedures; performed all pre-certification consulting ultimately leading to ISO 27001 certification; development and delivery of an information security training and awareness program; conducted an enterprise ISO 22307 privacy impact assessment (PIA); development and implementation and testing of enterprise business continuity management/disaster recovery plans under ISO 22301; implemented an enterprise vendor-management system, performed vendor/service provider contract reviews and risk ranking; and assessed high-risk vendors. Earned a formal endorsement from the CEO.
2015	Executed combination NIST 800-53/NIST Cybersecurity Framework (CSF) Assessments for Fortune 100 organizations. Provided outward facing attestations to satisfy regulatory and audit requirements and customer inquiries.
2016	Selected by an Information Sharing and Analysis Center (ISAC) to develop their first global third-party vendor security artifact including assessment criteria grounded in ISO 27001. Helped stand up this ground breaking Utility service and executed third-party vendor risk assessments on behalf of the ISAC's Members. Assessment outputs formally recognized by the Department of Homeland Security (DHS) and Health & Human Services (HHS).
2019	Recipient of the Lifetime Achievement Award from the Shared Assessments Program.
2019	Executed and reported on the new Financial Services Sector Coordinating Council (FSSCC) Cybersecurity Profile (The Profile) Assessments for global financial institutions whose infrastructure is designated by DHS as "Critical." Successfully developed 277 tests to satisfy the 277 diagnostic statements that comprise this new assessment.
2020	Selected to ensure U.S. Department of Defense contractors are compliant to NIST 800-171 and prepared for certification to CMMC.