Risk Management, Audit, and Compliance Experience for Daniel Giacomelli

My auditing experience started when I was a Senior Consultant at CSC, subcontracted to “The National Registry” for the Project Management Institute ISO 9001 certification. I was part of their initial data gathering initiative for their audit which they obtained in 1999. Risk Management experience also started within CSC as a consultant working for Dupont, auditing their Agricultural testing processes for [FIFRA compliance](https://www.epa.gov/sites/production/files/documents/apcol-fifra.pdf).

For CDI Corporation, as part of our strategic account toolkit, we created many tools to help assess risk, scope, and aid with budget and contract negotiations. We used ITIL as a framework to define and enable managed IT services and service levels. If needed, we relied on COBIT to help with IT governance and bridge the gap between the business and IT investments for some clients. The following are a few samples which can be provided of the tools\deliverables used:

* ITIL Service Support and Service Delivery Audit Worksheets (available upon request). These were then included as part of the Innovantage 90-day assessment (Nektar 90 Day Assessment v1.1.ppt).
* Microsoft Operations Framework (MOF) Assessment (MOF Assessment v1.0.xls, based on ITIL)
* Small Office Home Office Checklist (CDI Innovantage SOHO.checklists.xls)
* Site Audit Guidelines (Site Audit Guidelines v1.1.doc)
* Security Self-Assessment (Security Self Assessment.doc); Firewall Checklist (FirewallChecklist.doc);
* Managed Technical Operations Project Risk Characteristics (MTOps Risk Assessment v1.8.doc)
* For one Client in particular, I was part of a special security audit and Social Engineering testing for [Eclipse Aviation](https://en.wikipedia.org/wiki/Eclipse_Aviation) which resulted in the company adopting Common Criteria *ISO/IEC 15408:1999.CC 2.0* as part of their FAA Certification. Our two deliverables became templates for other clients. (CLIENT Common Criteria v1.1.doc and CLIENT Policies and Procedures v1.1.doc)

While at Canon, I was part of an audit team for the Project Management Institute PMI.org redesign, which resulted in the company adopting [ISO 27001:2005](https://www.iso.org/standard/42103.html) standards with [CIS Benchmarks](https://www.cisecurity.org/cis-benchmarks/) as part of their internal technical audit.

With CIGNA, while launching the new Individual plans, we needed to modify the Online Application to adhere to new Industry Compliance for both Federal and individual state regulations for Health Insurance as changes were being made for Obamacare. We successfully created plans for each state, for each compliance item. (IR446 OLA Compliance PDF Revised Project Plan 2011-01-13.pdf). We also identified a risk which turned into a large issue with capacity and turn-around times within Underwriting. We identified options for improvement including BPR, automation, and outsourcing, then I devised a plan, created metrics and model to track impact and trending analysis to eliminate the backlog. (Underwriting Capacity and Backlog Elimination Summary 2009-07.ppt)

While at FirstLab, I was brought in to revamp the entire Infrastructure and ensure PCI Compliance and Annual Audit success. Using the tools created from CDI, I created initial IT Policies, PMO and Governance models, and performed a variety of internal and external audits. The first external penetration test and audit for security discovered 15 severe issues, all of which were mitigated. HIPAA training was never performed prior to my arrival, which became a requirement for all employees, and included HITRUST training for all IT employees. First Software audit resulted in the IT department to obtain Microsoft Gold Partner to save over $200k annually in licensing fees, and avoid additional costs owed (FirstLab Information Technology and Security.docx). As a result, the first Business Continuity and Disaster Recovery plan was created for both FirstLab and Genomind (RID BC-DR Plan 2011-10.doc). I was part of the team to have FirstLab become a Certified - Third Party Administrator (C-TPA) by the Substance Abuse Program Administrators Association (SAPAA). For Genomind, the infrastructure upgrades, governance and policies established the foundation for services to work with the College of American Pathologists (CAP) for accreditation to ensure our 3rd party labs hold certification to perform highly complex testing under the Clinical Laboratory Improvement Amendments (CLIA).

For the City of Philadelphia, implementation of the EHR needed to comply with Meaningful Use (MU) and HIPAA Security Rules to receive MU credits. The SRA tool references components of the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-66 and 800-30 as guidance for a security risk assessment to identify conditions where Electronic Protected Health Information (EPHI) could be disclosed without proper authorization, improperly modified, or made unavailable when needed. This information is then used to make risk management decisions on what reasonable and appropriate safeguards are needed to reduce risk to an acceptable level. I was responsible to perform these annual audits and assessments; and as the tool and program matured, so did my responsibilities to provide Monthly Operations and Security audits, and annual asset\inventory audits. Using TOGAF to create the big picture enterprise architecture helped with risk and impact analysis for these audits. This information also supported the [City of Philadelphia DPH achieving accreditation](https://www.phila.gov/2018-10-31-public-health-accreditation/). From previous experience, I authored the EHR policies and governance models including support, escalation, BCDR, and Access agreements. Sample Documents include:

* Facility Walkthrough Checklist - PDPH-AHS-HCx.doc
* Health Center PHI Assessment EXEC Summary 2018.docx
* AHS EHR OCR HIPAA TOC 2019.xlsx
* DPH AHS EHR SRA 2019-11.pdf
* EHR Monthly Security Ops 6-2020.pdf

Being an Architect has provided many opportunities as a SME or Lead for Operational and Technical Audit projects and initiatives. Defining the ‘current state’ within the ‘big picture’, moving from Going from conceptual to logical and physical diagrams, makes it more intuitive to see gaps, risks, and impact areas, and identify mitigations, improvements, and solutions. Always taking a People, Process, and Technology approach to whichever framework and tool is used. Regardless of role\title, I have always assisted or lead projects. Seems I have a knack for creating requirements\checklists and devising plans. Many projects came out of the initial City SRA Audit to achieve MU credits and accreditation. In 2019, City OIT decided to look to NIST audit tools using SCAP content for Microsoft.

At Talkiatry, we decided to use the SRA for establishing benchmarks and showing progress, but also: NIST SP [800-30](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final), Guide for Conducting Risk Assessments; the Prose [Azure Security Benchmark 1.0 Checklist](https://ncp.nist.gov/checklist/954); and review [NIST SP 800-53](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final) Security and Privacy Controls for Information Systems and Organizations.

I’ve learned to use what is appropriate for Strategic Planning and Design, which may be different from Tactical analysis and Delivery: NIST with Core, Tiers, and Profiles; ITIL for IT Service Management and Governance; COBIT to increase quality and reliability, reduce risk, with better agility and collaboration; TOGAF to organize and manage technology through Architecture.

*Items in* Courier Font denote sample artifacts *which may be provided upon request and approval*.