# Expected Outcomes

NYeC is re-building its capabilities to develop enterprise class software, having abstained from large scale development for several years. The overarching goal of this engagement is to ensure the partners supporting NYeC, and NYeC staff follow a Software Development Life Cycle (SDLC) methodology in a way that creates such evidence as is required by HITRUST and the Department of Health (DOH).

NYeC has engaged multiple technology vendors (“partners”) and wants to facilitate execution across the partners’ artifacts to provide evidence of quality. By demonstrating evidence of execution as required by HITRUST and DOH, the public and other NY State agencies can be confident that NYeC is a high-integrity organization that takes privacy, security, and quality seriously.

To increase predictability of software development execution, NYeC must ensure that its quality management system (QMS) and engineering practices across multiple technology partners, vendors, and consultants can demonstrably prove compliance through robust, systematic, and verifiable evidence collection and management practices.

NYeC is assuming that its technology partners and solutions providers are competent professionals who know how to perform the jobs for which they’ve been hired. What NYeC needs is an approach which ensures that all the technology partners follow a unified approach towards preparing, collecting, and supplying evidence as necessary to support HITRUST.

The evidence that each partner supplies for HITRUST and DOH compliance controls must minimize diversity of approach such that a auditor looking at works from multiple sources would be unaware that NYeC engages multiples parties to achieve software development goals.

To ensure that engineering artifacts are as objective as possible (rather than subjective) an early deliverable will help determine expected outcomes against some of the following types of metrics:

* Potential OKRs – to be discovered / discussed / determined (TBD3)
* Initial metrics to consider:
  + Approved SDLC (also referred to as “Quality Management System” or QMS that is common in healthcare applications)
  + number of QMS / SDLC artifacts reviewed against compliance framework.
  + More TBD3
* Potential KPIs
  + Weekly report on number of SDLC / QMS artifacts reviewed against compliance framework that passed audit and failed audit; group by organization.
  + More TBD3
* NYeC policies to align with
  + Existing NYeC HITRUST library of policies related to SDLC (to be shared with team in initial meetings).
* State/fed regulatory language we are pointing to -- TBD3
* State/fed statutory language we are pointing to -- TBD3

# Agile

Netspective is expected to execute the project using Agile methodologies, emphasizing the MVP (Minimum Viable Product) approach and iterative development. This strategy should be applied specifically to the enhancement of the QMS or SDLC process. The initial focus should be on developing and implementing one or two critical SDLC and QMS steps, along with corresponding artifact guidance, at an early stage. Subsequent audits for compliance should also be commenced promptly, targeting these initial steps, rather than waiting for the comprehensive development of the entire SDLC framework. This approach ensures that improvements are made incrementally and efficiently, allowing for continuous assessment and adaptation.

The Agile objective is to release components of the QMS / SDLC early and often; and then begin auditing compliance of those components (as opposed to a “big bang” approach of deciding everything in advance). Netspective will not wait for a ‘grand unifying’ SDLC or QMS release but rather iterate frequently using the concept of sprints with releases.

# Meetings

Netspective will organize regular gatherings of all involved developers at each release phase of the SDLC. In these meetings, Netspective will provide comprehensive information about the new elements introduced in the SDLC, along with detailed expectations regarding compliance-related documentation. These sessions are crucial for ensuring that all development teams are consistently aligned with the latest SDLC requirements and practices.

Additionally, Netspective is required to share the results of any compliance audits with all stakeholders. This communication should occur on a regular basis, not less frequently than weekly. This will ensure timely dissemination of audit findings, enabling prompt action and continuous improvement across all teams. These meetings should include Ready, Hmetrix, Netspective and NYeC team members.

# Potential Plan to Achieve Expected Outcomes

To create a comprehensive plan focusing on the preparation and generation of evidence to prove to auditors, including HITRUST, that proper engineering is being done and that all artifacts and code meet the chosen compliance regimes' prioritized Anchor Controls, we will focus each step with an evidence-generation mindset. Here's how the plan will be structured:

**1. Compliance Assessment & Requirement Gathering.** Determine if HITRUST is the only compliance regime NYeC is targeting or if there will be others.

* **Interviews with Compliance Teams**: Conduct discussions to understand mandated compliance regime (e.g., HITRUST, FISMA, SOC2). Assume HITRUST is a must but focus on understanding the evidence required for compliance by reaching out to Auditors, asking their opinions, and for sample evidentiary support. While the QE’s are not in scope, their compliance artifacts may be of value to this engagement as templates.
* **Identify Relevant Controls**: Determine specific controls related to software engineering and cloud infrastructure. Document these controls and the type of machine attestation as well as human attestation evidence needed for each.
* **Interviews with Technology Partners**: Conduct detailed discussions to understand which technology partners already have experience with the chosen compliance regimes (e.g., HITRUST, SOC2). Concentrate surveys on how partners already generate machine-verifiable evidence vs. human attestation for controls compliance evidence.

**2. Adopt the** [**Secure Controls Framework**](https://securecontrolsframework.com/)**v (SCF)**. Map controls from various regimes using SCF. Focus on how each control can produce verifiable evidence so that evidence generated for one regime such as HITRUST.

**3**. **Evaluate and Select Universal Evidence Preparation, Collection, and Sharing Strategy**. Because the central premise of the Technology Coordination activities is to drive compliance HITRUST, alignment is necessary on how evidence is prepared, collected, and validated against compliance controls. Centralized governance around how SDLC compliance evidence is to be shared, allowing each technology partner to have flexibility to decentralize implementation of their SLDCs.

* **Determine Machine Attestation Evidence Formats**: Consider formats such as [Test Anything Protocol](https://testanything.org/) (TAP) and other machine-readable formats like JSON and XML with strong schemas (such as at [schema.org](https://schema.org)).
  + All technology partners must prepare and submit their evidence of controls compliance in well-known machine-readable formats whenever possible.
  + Machine Attestation submissions such as [TAP](https://testanything.org/), JSON, XML, or others may be done with embedded certificates or other digital rights management (DRM) signatures to ensure that evidence has not been tampered with.
* **Determine Human Attestation Signature Formats**: Decide how evidence will be submitted for compliance controls that do not easily allow machine attestation. Options include e-signatures of executive management at technology partners or Excel Workbooks, or other MS Office formatted files that are AI-parseable.
* **Create Comprehensive Guides on Evidence Collection**: Provide clear documentation and training on how to generate and maintain evidence for compliance.
* **Evidence Templates and Tools**: Provide templates and tools for consistently documenting evidence across teams and partners.

**4. Prioritization of Anchor Controls.** Because HITRUST contains hundreds of controls with multiple overlapping evidentiary support requirements we will need to work with NYeC compliance officials to get their opinions on the most important controls for which each Technology Partner should demonstrate evidence.

* **Select a limited number of top Controls**: Prioritize the most critical controls for initial focus. Document the rationale and type of evidence (machine attestation vs. human attestation) required for each.
  + *These will be known as “Anchor Controls” and will form the basis for the “Pilot” program. After the pilot program is completed, we’ll expand to hundreds more controls as necessary (to fulfill all HITRUST and other compliance regimes’ requirements).*
* **Define Attestation Requirements**: Specify detailed machine and human attestation requirements. Plan how evidence will be captured, stored, and presented for these controls using the selected file formats.

**5. Standardizing Development Practices for Evidence Generation for Anchor Controls.** NYeC would like to align and standardize policies, procedures, and processes across its various technology partners and generate evidence of controls in a standardized manner. Doing so for a large number of controls at once may not be possible so the starting point will be to do so for the prioritized Anchor Controls.

* **Anchor SDLC Frameworks**: Choose frameworks (such as Microsoft or Blackblot) that emphasize traceability, documentation, and compliance. Ensure that the framework facilitates the capture and storage of evidence throughout the development cycle.
* **Anchor Tools Selection**:
  + **Issue Tracking System**: Utilize Jira to log all activities and decisions. Create such Jira reports and logs as are necessary for compliance evidence.
  + **Version Control System**: Use Git with strict branch and commit guidelines to ensure traceability of changes. Ensure commit logs are clear and link back to compliance requirements and generate appropriate evidence.
  + **RCS Hosting Service**: Select a service that offers robust logging, security, and compliance features. Assume that Atlassian BitBucket is the selected tool for the canonical repositories but leave the final decision to NYeC executive leadership team in case any of the steps above demonstrate that BitBucket might not be as useful as another choice).
* **Development and Testing Standards**: Implement coding and testing standards that emphasize creating verifiable, compliant artifacts. Document test plans, results, and code review findings in an audit-friendly manner.
* **CI/CD Pipeline**: Design pipelines that automatically log deployments, testing results, and code quality metrics.
* **Security and Compliance**: Integrate automated security scanning and compliance checks into the CI/CD pipeline. Ensure evidence is generated and Machine Attestable whenever possible.

**6. Engagement with NYeC Technology Partners (“Vendors”):**

* **Partners' Compliance Alignment**: Work with NYeC staff and partners (Ready Computing Hmetrixand Netspective) to ensure their understanding of and alignment with the evidence generation requirements. Document their compliance commitments and plans.
* **Collaborative Evidence Collection**: Establish processes and tools for partners to submit compliance evidence regularly and systematically.

**7. Implementation & Monitoring for Evidence:**

* **Gradual Rollout with Evidence Tracking**: Implement the Anchor Controls with continuous monitoring and evidence collection. Ensure all actions are logged and traceable.
* **Continuous Evidence Review**: Regularly review the collected evidence to ensure it meets compliance standards and is ready for audits.

**8. Feedback Loop and Continuous Improvement for Prioritized Anchor Controls:**

* **Regular Compliance and Evidence Reviews**: Establish a schedule for reviewing the compliance stance and the quality of evidence collected. Use feedback to improve processes and evidence collection methods.
* **Adapt Tools and Processes**: Continuously assess and update tools and processes to better support evidence generation and compliance.

**9. Expand Process Beyond Anchor Controls.** Once the prioritized Anchor Controls have been established and evidence is shared with proof that audits are possible during the “Pilot” phase, expand to more and more of the HITRUST or other compliance regime controls using the same procedure followed for the Anchor Controls.

By focusing each step of this plan on the preparation and generation of compliance evidence, NYeC can ensure that its engineering practices not only meet the required standards but also that it can demonstrably prove compliance through robust, systematic, and verifiable evidence collection and management practices. This approach will facilitate smoother audits and increase trust among stakeholders, regulatory bodies, and partners.