So You've Been Named the DQI...

NOW WHAT?

A Beginner's Guide to the Designated Qualified Individual

?

THE ACCIDENTAL DQI

A Practitioner's Guide for Newly Appointed Designated Qualified Individuals

in Healthcare, Financial Services & Small Business

A Practitioner's Reference

This guide reflects current regulatory guidance, practitioner experience, and the realities faced by non-technical professionals thrust into the DQI role. What follows is a practical, accurate, and actionable framework for doing the job well.

Introduction: What This Book Is — and What It Is Not

This is a practical guide, not a compliance textbook. If you have just been handed the title “Designated Qualified Individual” — perhaps with minimal ceremony and zero training — this book is for you. It will not recite statutes verbatim. It will not pretend that compliance is simple. And it will not treat you as a passive recipient of rules handed down from above.

What it will do is tell you the truth about the role, give you the tools to perform it with integrity, and protect you from the pitfalls that trip up well-meaning people every year.

WHY THIS MATTERS

Personal liability under GLBA, HIPAA, and state privacy laws can attach to named individuals — not just organizations. The DQI designation is not ceremonial. It carries real exposure.

This guide does not recite statutes verbatim. It does not pretend compliance is simple. And it gives significant weight to the one thing most DQI guidance underemphasizes: what happens when things go wrong and why documentation is your only shield.

CHAPTER 1

The Role of the DQI

Governance, Not Gadgetry

The Designated Qualified Individual — commonly called the DQI, or "Qualified Individual" under the FTC Safeguards Rule — is the person formally accountable for an organization's information security program. In healthcare the analogous designation appears in HIPAA's Security Rule. The function is the same: a named, accountable human being responsible for ensuring that the program exists, operates, and improves.

What the DQI Actually Does

It is worth stating clearly: the DQI is not an IT technician. That bears repeating and sharpening. The DQI's work is governance. Governance means:

- Ensuring a written information security program exists and is current
- Overseeing risk assessments and driving remediation of findings
- Holding vendors accountable through documented due diligence
- Reporting program status to leadership at least annually
- Maintaining evidence that the program is functioning

What governance does not mean: personally configuring firewalls, writing code, responding to active cyber incidents, or making architectural decisions about network topology. If you find yourself doing those things without the credentials to back them up, stop. Document that you were asked. Decline in writing. Escalate.

The Conductor Analogy — Refined

A common analogy compares the DQI to an orchestra conductor. The analogy holds, but it is incomplete. A conductor knows music theory. They can hear when the cellos are flat. They do not play the oboe, but they know what an oboe in tune sounds like.

The DQI equivalent of this is asking the right questions of technical staff and vendors, recognizing evasive or incomplete answers, and knowing when to bring in outside expertise. You do not need to know how to configure a firewall. You do need to know how to ask "When was this last reviewed? What was found? What was fixed? Can I see the evidence?"

KEY PRINCIPLE	Oversight without knowledge is rubber-stamping. Your job is informed governance, not blind sign-off. Learn enough to challenge. Delegate the rest.

What "Qualified" Actually Means

The FTC Safeguards Rule (16 CFR Part 314) uses the phrase "Qualified Individual." The regulation does not define a specific certification or degree. It requires that the individual has the knowledge and experience sufficient to oversee the program effectively. In practice this means:

- Understanding the regulatory framework applicable to your organization
- Familiarity with common categories of risk in your industry
- The ability to assess whether controls are adequate, even without building them
- Willingness to engage outside expertise when internal knowledge is insufficient

If you were appointed to this role without any of the above, your first obligation is to close that gap. This guide is a starting point. It is not a substitute for education, mentorship, or — where the stakes are high — qualified outside counsel.

CHAPTER 2

Your First 30 Days

Stabilize Before You Build

Some guidance proposes a seven-day onboarding plan for new DQIs. That timeline is aspirational. In most real organizations, gathering the information you need to do this job properly takes longer. The goal of your first month is not to fix everything. It is to understand what exists, what is missing, and what poses the greatest immediate risk.

Day 1–7: Learn the Terrain

Do not touch anything yet. Before you change a policy, update a procedure, or send a vendor a questionnaire, you need to understand what is already in place. Ask these questions and record every answer:

- What regulatory frameworks apply to this organization? (HIPAA, GLBA/FTC Safeguards, state privacy laws, CCPA, etc.)
- Has a formal risk assessment ever been conducted? When? By whom? What were the findings?
- Is there a Written Information Security Program (WISP)? Where is it? When was it last reviewed?
- Who are our key IT and security vendors? What do they do? What are our contracts with them?
- Have there been any security incidents or breaches in the past three years?

If the answers are “no,” “I don’t know,” or “we don’t have that” — document that. Those gaps are your initial risk inventory.

CRITICAL	Request all documents in writing via email. This creates a record showing you asked. It also creates accountability in others to actually provide them.

Day 8–14: Assess What Exists

Once you have collected whatever documentation exists, evaluate it honestly. The following is the minimum viable documentation set for a defensible information security program:

Written Information Security Program	The foundational document. Must describe the scope, objectives, and components of the security program.
Risk Assessment	A documented evaluation of threats, vulnerabilities, and controls. Must be current — within 12 months.
Incident Response Plan	A step-by-step guide for detecting, containing, and reporting security incidents and breaches.
Vendor Management Records	Contracts, security questionnaires, and risk ratings for all vendors handling sensitive data.
Access Control Records	Documentation of who has access to what systems, when access was last reviewed, and how terminated users are removed.
Training Records	Evidence that staff have completed security awareness training, including dates and topics covered.
Annual Report to Leadership	A formal summary presented to senior management at least once per year.

If any of these are missing, that is not cause for panic. It is cause for a prioritized remediation plan. Document the gaps. Document your plan to close them. Request the resources to do it.

Day 15–30: Build Your DQI Notebook

The DQI Notebook — whether a binder, a shared drive folder, or a compliance management tool — is the living record of your program. It

should contain everything a regulator, auditor, or attorney would need to see that you are doing your job. Organize it around these sections:

- Program overview and regulatory applicability
- Risk assessment (current and historical)
- Policies and procedures (with version history)
- Vendor inventory and due diligence records
- Incident log (even if empty — an empty log is evidence of no incidents)
- Training records
- Annual reports to leadership
- Resource requests made and responses received

Store this securely. It contains sensitive organizational information. Restrict access to those with a legitimate need. Back it up.

CHAPTER 3

The Six Core Responsibilities

A Deeper Look

The six core DQI responsibilities are: risk assessment, safeguards, vendor oversight, policies, monitoring, and reporting. Those categories are correct. What follows is a detailed and honest account of what each actually requires.

1. Risk Assessment

A risk assessment is not a questionnaire you fill out and file. It is a structured process for identifying what data you hold, what threats it faces, how vulnerable your controls are, and what the likely impact of a breach would be. It must be:

- Documented in writing, not just discussed
- Conducted at least annually and after significant changes to systems or operations
- Followed by a remediation plan that addresses identified gaps
- Reviewed with leadership

The most common failure in risk assessments is conducting the exercise but not acting on the findings. Regulators will ask not just “Did you assess risk?” but “What did you find and what did you do about it?” An assessment whose findings were ignored is worse than no assessment at all — it demonstrates that you knew about the problem.

REGULATORY NOTE	Under the FTC Safeguards Rule, the risk assessment must be in writing and must inform the design of safeguards. Under HIPAA, the Security Risk Analysis is a required implementation specification — not an addressable one.

2. Safeguards

Safeguards are the controls — technical, administrative, and physical — that reduce the risks identified in your assessment. As DQI, you do not implement these yourself. You verify they exist, are working, and are appropriate to the risk.

The most important safeguards for most small and mid-size organizations are:

Multi-Factor Authentication	Required on all systems with access to sensitive data. Non-negotiable. Verify it is actually enforced, not just available.
Encryption	Data in transit must use TLS 1.2 or higher. Data at rest must be encrypted on laptops, mobile devices, and portable media.
Access Controls	The principle of least privilege: users should have access only to what they need to do their job. Access should be reviewed regularly.
Patch Management	Systems must receive security updates promptly. Ask your IT provider for a patch compliance report. Know the cadence.
Backup and Recovery	Data must be backed up regularly. Backups must be tested. The recovery time objective must be defined and realistic.
Security Awareness Training	All staff must receive annual training on phishing, social engineering, and acceptable use. Track completion.
Endpoint Protection	Anti-malware software must be deployed, updated, and actively monitored on all endpoints.

3. Vendor Oversight

Vendors who handle your organization's data are an extension of your risk surface. A breach at a vendor is effectively a breach at your organization. The DQI's obligation is to ensure:

- All vendors with access to sensitive data are identified and inventoried
- Contracts with those vendors include security requirements and breach notification obligations
- Vendors are assessed for security adequacy before onboarding and periodically thereafter
- Vendor assessments are documented

Annual vendor reviews are the minimum. High-risk vendors — those with broad access to sensitive data or critical systems — warrant more frequent scrutiny.

4. Policies and Procedures

A policy is a statement of what the organization will do. A procedure is the step-by-step instruction for how it will be done. Both are required. A comprehensive program will eventually require a broad range of policies. Prioritize in this order for a new program:

1. Written Information Security Program (the parent document)
2. Acceptable Use Policy
3. Incident Response Policy and Procedures
4. Access Control and Password Policy
5. Vendor Management Policy
6. Data Retention and Destruction Policy
7. Security Awareness Training Policy
8. Remote Access Policy
9. Physical Security Policy

Do not file policies away and forget them. They must be reviewed at least annually, updated when regulations or operations change, and communicated to staff. A policy that nobody knows about is not a control.

5. Monitoring and Evidence

Monitoring is the ongoing verification that your controls are working. Evidence is the record that they were working. These are not the same thing. You can monitor without collecting evidence — but then you have nothing to show a regulator.

Build evidence collection into your routine. Schedule monthly reviews of:

- Backup success reports
- Patch compliance reports
- Access control review confirmations
- Security training completion logs
- Incident logs (even if empty)
- Vendor correspondence

Store dated copies of all of the above in your DQI Notebook.

6. Annual Reporting to Leadership

The FTC Safeguards Rule explicitly requires that the Qualified Individual report to the Board of Directors (or equivalent senior governing body) at least annually. HIPAA implies equivalent accountability. This is not a memo to your supervisor. This is a formal report to whoever holds ultimate accountability for the organization.

The report should cover:

- The overall status of the information security program
- Risk assessment findings and remediation status
- Any incidents or near-misses during the year

- Vendor oversight activities and findings
- Outstanding resource needs or unresolved gaps
- Plans for the coming year

PROTECT YOURSELF	If leadership receives your report and decides not to fund a remediation you have recommended, document that decision. You have discharged your obligation. The liability for the unfixed gap now rests with those who chose not to act.

CHAPTER 4

The Mistakes That Actually Sink DQIs

Beyond the Obvious

Many common DQI mistakes are well-documented. What follows is an honest accounting of the failures that produce regulatory findings, litigation exposure, and personal liability — drawn from real enforcement actions and practitioner experience.

Treating Documentation as Administrative

Documentation is not paperwork. It is your legal defense. Every time you conduct a risk assessment, review a vendor, update a policy, or report to leadership, that activity should generate a dated, written record. A verbal conversation with your IT provider about a security issue is worth nothing if you cannot prove it happened.

The standard to hold yourself to: if a regulator examined your records eighteen months from now, would they be able to reconstruct what you did, when, and why? If not, the documentation is insufficient.

Assuming Vendors Are Compliant

Vendors routinely overstate their security posture. A signed Business Associate Agreement under HIPAA does not mean a vendor has adequate controls. A SOC 2 report is not a guarantee of current compliance. Your obligation is to verify — not trust. Ask for evidence. Review it. Document your review.

Confusing Activity with Compliance

Attending training, updating spreadsheets, and holding meetings are not compliance. They may support compliance. But a regulator will ask whether your risk assessment was current, your policies were followed, your vendors were vetted, and your incidents were properly handled. If

the answer to those questions is no, the volume of adjacent activity is irrelevant.

Performing Technical Work Beyond Your Competence

This point deserves direct emphasis. If you lack the technical credentials to configure a system, conduct a forensic investigation, or evaluate the adequacy of network architecture — do not do those things. If you are pressured to do them, decline in writing. If you do them and something goes wrong, your lack of credentials will not be a defense. It will be an aggravating factor.

Not Escalating Unresolved Gaps

If you identify a risk, request resources to address it, and are denied — escalate. If escalation does not resolve the problem, escalate again. Document every step. Your goal is not to be comfortable. Your goal is to ensure that the decision-makers who have authority to act have been informed, have decided, and own the consequences.

Assuming “We’re Too Small”

Ransomware operators do not discriminate by organization size. Healthcare offices, credit unions, and professional services firms are among the most common targets precisely because their defenses are often weakest. The FTC has brought enforcement actions against small organizations. State attorneys general have done the same. Size is not a shield.

CHAPTER 5

The DQI Toolkit

What You Actually Need

You do not need elaborate technology to run a defensible information security program at a small or mid-size organization. You need the right documents, the right processes, and the discipline to maintain both. The following is a practical inventory.

Essential Documents

Written Information Security Program (WISP)

The WISP is the central document of your program. It should describe:

- The scope of the program (what data, what systems, what locations)
- The roles and responsibilities of those who implement it
- The risk assessment process
- The safeguards in place
- The incident response procedures
- The vendor management process
- The training program
- The review and update schedule

The WISP is a living document. It must be updated when regulations change, when the organization changes, or when the risk landscape changes. An outdated WISP is evidence of a program that has lapsed.

Risk Assessment

Conduct your risk assessment using a structured methodology. NIST SP 800-30 is freely available and widely accepted. For most small organizations, a simplified version using the following framework is adequate:

Asset Identification	What data do we hold? Where is it stored? Who has access? What systems process it?
Threat Identification	What could go wrong? (Unauthorized access, ransomware, insider misuse, accidental disclosure, vendor breach, physical theft)
Vulnerability Assessment	What weaknesses exist in our current controls? (Missing MFA, unpatched systems, weak passwords, untrained staff)
Likelihood and Impact	For each threat, how likely is it? If it occurred, how severe would the damage be?
Remediation Planning	For each significant risk, what will we do? By when? Who is responsible?

Incident Response Plan

An incident response plan does not need to be long. It needs to be clear and usable under pressure. At minimum it must define:

- What constitutes a reportable security incident
- Who is notified internally when an incident is detected
- Who leads the response
- How the incident is contained and investigated
- When and how external parties are notified (regulators, affected individuals, law enforcement)
- How the incident is documented and reviewed afterward

Under HIPAA, a breach of unsecured protected health information generally triggers notification obligations within 60 days of discovery. Under many state laws, notification timelines are as short as 30 days or even 72 hours. Know your obligations before an incident occurs.

Vendor Management Records

For each vendor with access to sensitive data, maintain a file containing:

- The executed contract, including security requirements and breach notification provisions
- A completed security questionnaire or equivalent due diligence record
- The date of last review
- Any findings and follow-up actions

Recommended Policies

A comprehensive program will ultimately require a broad policy library. For organizations building a program from scratch, start with these eight and add the rest over time:

- Acceptable Use Policy
- Access Control and Password Policy
- Incident Response Policy
- Data Retention and Destruction Policy
- Remote Access Policy
- Vendor Management Policy
- Security Awareness Training Policy
- Physical Security Policy

LANGUAGE MATTERS	Policies must use mandatory language: ‘must,’ ‘will,’ ‘is required.’ Policies written with ‘should’ or ‘may’ are aspirational, not enforceable. A regulator reading ‘employees should use strong passwords’ will note that no one was required to.

Operational Tools

The following tools are the operational infrastructure of your program. Most are low-cost or free for small organizations.

Password Manager	Required. Use one that supports organizational vaults and auditing. LastPass, 1Password, and Bitwarden are common choices.
Multi-Factor Authentication	Required. Microsoft Authenticator and Google Authenticator are free. Authy is widely used. Enforce it at the identity provider level.
Compliance Calendar	A calendar — even a shared Google Calendar — with reminders for all recurring compliance activities. Annual report due. Risk assessment due. Vendor review due. Policy review due.
IT Ticketing System	Any system that creates a written record of technical requests, changes, and incidents. Even a shared email inbox with labels can serve this function at small organizations.
Backup Monitoring	Automated alerts from your backup system. Verified restoration test records. You must be able to prove backups work, not just that they are scheduled.
Evidence Folder	A structured file system — local, cloud, or both — containing dated records of all program activities. Restricted access. Regular backup.

CHAPTER 6

Building a Defensible Security Program

Five Pillars

A defensible security program is one that can withstand scrutiny — from regulators, auditors, insurers, and attorneys. 'Defensible' does not mean perfect. It means documented, reasonable, and consistently maintained. These five pillars are the structure.

Pillar 1: Policy — State Your Intentions Clearly

Every component of your program should be grounded in a written policy that states what the organization intends to do and why. Policies set the standard against which your actions are measured. Without them, there is no baseline. With them, you have a framework for accountability.

Keep policies current. A policy last updated five years ago is evidence of a program that was never maintained. Schedule annual reviews. Document the review even when nothing changes.

Pillar 2: Procedure — Turn Policy Into Practice

A procedure answers: given this policy, what do we actually do? Procedures make programs repeatable. They survive staff turnover. They enable training. They produce the consistency that regulators want to see.

Where possible, attach procedures to the policies they implement. When a policy says "all terminated employees will have access revoked immediately," the associated procedure describes who does it, how, what system they use, and what record they create.

Pillar 3: Controls — Implement the Safeguards

Controls are the actual safeguards that reduce risk. The DQI's role is to verify they exist, are appropriate to the risk, and are actually functioning. Verification requires evidence. "Our IT provider told us MFA is enabled" is not evidence. A configuration report showing MFA enforcement is evidence.

Pillar 4: Monitoring — Verify That Controls Work

Controls fail silently. Backups stop running. MFA enforcement lapses. Patches go unapplied. Without monitoring, you do not know until a breach reveals what was broken. Build monitoring into your calendar. Make it routine. Document what you check and what you find.

Pillar 5: Evidence — Prove That You Did It

If it is not documented, it did not happen. This is the operating principle of regulatory enforcement. Evidence collection is not administrative overhead. It is the mechanism by which your program defends itself. Collect it as you go. Organize it. Retain it for at least the period required by applicable law (typically three to six years depending on framework).

CHAPTER 7

Regulatory Expectations

What the Frameworks Actually Require

The regulatory frameworks most relevant to DQIs are HIPAA, the FTC Safeguards Rule under GLBA, and state privacy and breach notification laws. What follows highlights the points that matter most in practice.

HIPAA Security Rule

The HIPAA Security Rule applies to covered entities (healthcare providers, health plans, clearinghouses) and their business associates. The Rule's requirements are organized into required and addressable implementation specifications. The distinction matters:

- Required specifications must be implemented as stated. There is no discretion.
- Addressable specifications must be implemented if reasonable and appropriate, or the organization must document why an alternative measure was adopted instead.

The Security Risk Analysis — the formal assessment of risks to electronic Protected Health Information — is a required specification. It is the most commonly cited deficiency in OCR audits and enforcement actions. If you have not conducted one, or have not conducted one recently, it is your first priority.

The Security Rule does not require perfection. It requires that safeguards be reasonable and appropriate given the size, complexity, and capabilities of the organization. A solo medical practice and a regional health system face different expectations. Document your rationale for the choices you make.

FTC Safeguards Rule (GLBA)

The FTC Safeguards Rule, as amended in 2023, applies to financial institutions as defined by GLBA. The definition is broader than banks: mortgage brokers, payday lenders, tax preparers, auto dealers, and certain other entities are covered. The Rule requires:

- A written information security program
- A qualified individual to oversee it
- A risk assessment in writing
- Specific safeguards including encryption, MFA, secure development practices, and monitoring
- Vendor oversight
- Incident response planning
- Annual reporting to the Board or equivalent
- Periodic testing of key controls

The 2023 amendments added specificity that was absent from the prior version. MFA, encryption, and penetration testing are now explicitly required for covered entities above certain size thresholds. Know whether those thresholds apply to your organization.

NOTE ON THRESHOLDS	Financial institutions with fewer than 5,000 customers are exempt from some — not all — of the 2023 amended requirements. The core program obligations still apply. Confirm your organization's specific obligations with qualified legal counsel.

State Privacy Laws

State privacy law is a complex and rapidly evolving landscape. California (CCPA/CPRA), Virginia, Colorado, Connecticut, Texas, and many other states have enacted comprehensive privacy legislation. Most share these common features:

- Consumer rights to access, correct, and delete personal data
- Data broker registration requirements in some states
- Security requirements for personal data
- Breach notification obligations with specific timelines

Breach notification laws exist in all fifty states. Timelines vary from 30 to 90 days, and some states require notification to the Attorney General in addition to affected individuals. Know your state's law. Build notification procedures before you need them.

CHAPTER 8

Personal Liability and Self-Protection

The Stakes Are Real

Personal liability deserves direct treatment. The DQI designation creates personal accountability. In enforcement actions and civil litigation, the question of whether the named individual acted reasonably and with appropriate diligence is a live one.

The Four Shields

Four practices collectively constitute your primary protection against personal liability. None is sufficient alone. Together they create a defensible record.

Shield 1: Document Everything

Every action you take in your DQI capacity should generate a written record. Meetings, risk assessment findings, vendor reviews, policy updates, training sessions, resource requests, and leadership reports — all of it, dated, organized, retained. When a regulator or attorney asks "what did the DQI do?" the answer is your documentation.

Shield 2: Report Formally to Leadership

The annual report to leadership is not a formality. It is the mechanism by which you transfer accountability upward for decisions that require resources, authority, or organizational change. If your report identifies a critical risk and leadership chooses not to fund the remediation, that decision is theirs. Document it. Your obligation is to inform and recommend, not to guarantee outcomes you do not control.

Shield 3: Request Resources in Writing

When you identify a gap and need budget, staff, or external expertise to address it, make the request in writing. If it is denied, document the denial. This record demonstrates that you identified the problem, sought to fix it, and were constrained by decisions made at a level above your authority.

PRACTICAL ADVICE	A simple email to your supervisor or executive leadership stating "I am requesting approval to engage an external vendor to conduct an annual penetration test at an estimated cost of $X. This is required to address the following risk identified in our risk assessment..." creates a record whether the answer is yes or no.

Shield 4: Engage Independent Assessment

An annual independent risk assessment — conducted by a qualified external party — serves two purposes. First, it identifies risks that internal review may miss. Second, it demonstrates that you took the program seriously enough to subject it to outside scrutiny. The report becomes part of your evidence file.

For organizations under HIPAA, third-party assessments are particularly valuable because OCR audits frequently probe the Security Risk Analysis. Having an externally validated assessment is stronger than an internally conducted one.

What Not to Do

Do not perform technical work that exceeds your qualifications. Do not respond to incidents without qualified incident response support if the situation warrants it. Do not sign certifications or attestations whose underlying basis you cannot verify. Do not accept vendor representations without evidence. Each of these creates exposure that your documentation shields cannot protect against.

CHAPTER 9

Your 90-Day Roadmap

From Overwhelmed to Operational

This chapter provides a structured 90-day plan for the newly appointed DQI, with specific deliverables and decision points at each stage.

Days 1–30: Stabilize and Assess

The objective of the first month is to understand the current state of the program — or its absence — and create a documented baseline.

Week 1	Collect all existing policies, procedures, contracts, and compliance documentation. Request in writing what you cannot locate.
Week 2	Identify applicable regulatory frameworks. Confirm with legal counsel if uncertain. Map data flows: what data do you hold, where does it live, who has access.
Week 3	Conduct a preliminary gap analysis: what required documents or processes are missing? Prioritize by regulatory requirement and risk severity.
Week 4	Present your baseline findings to leadership in writing. Identify the top three to five risks requiring immediate attention. Request resources to address them.

Days 31–60: Strengthen and Remediate

The objective of the second month is to close the most critical gaps and strengthen the foundations of the program.

Weeks 5–6	Initiate or complete the formal risk assessment. Engage external support if internal capacity is insufficient. Document all findings.

Week 6	Draft or update the top-priority policies identified in your gap analysis. Review with legal or compliance counsel where applicable.
Weeks 7–8	Conduct vendor reviews for all vendors with access to sensitive data. Prioritize those with the broadest access or handling the most sensitive data.
End of Month 2	Deliver a mid-point report to leadership summarizing progress, outstanding gaps, and resource needs.

Days 61–90: Mature and Systematize

The objective of the third month is to move from reactive remediation to proactive governance.

Week 9	Finalize the Written Information Security Program. Ensure it reflects the actual state of your controls and processes.
Week 10	Complete the compliance calendar for the next 12 months. Every recurring obligation should have a date, an owner, and a reminder.
Week 11	Conduct or schedule the first security awareness training session. Documented attendance and content.
Week 12	Deliver the first formal annual report to leadership or the Board. Even if the program is still maturing, report on what exists, what is in progress, and what remains outstanding.
REALISTIC EXPECTATION	A 90-day plan does not produce a mature program. It produces a program that is documented, organized, and defensible. Maturity takes years. The goal of the first 90 days is to demonstrate that you took the role seriously and acted with reasonable diligence from the start.

A Final Word

The DQI role is not glamorous. It does not come with adequate resources, clear predecessors, or forgiving timelines. It comes with a title, a regulatory obligation, and — if you are reading this — a determination to do it right.

The frameworks in this guide are not compliance theater. They are the practical infrastructure of a program that can defend itself when something goes wrong — because something will go wrong. The question is not whether your organization will face a security incident. It is whether, when it does, you will be able to demonstrate that you did your job.

Documentation is your evidence. Escalation is your protection. Independent assessment is your validation. Reporting to leadership is your accountability mechanism. Together, these practices do not guarantee a perfect outcome. They guarantee that you acted with the diligence the role demands.

That is enough. Start there.

Appendix: Quick Reference

Regulatory Frameworks at a Glance

HIPAA Security Rule	Covered entities and business associates. Required: Security Risk Analysis, written policies, safeguards, workforce training, contingency planning. Enforced by HHS Office for Civil Rights.
FTC Safeguards Rule (GLBA)	Financial institutions under GLBA. Required: Written ISP, Qualified Individual, risk assessment in writing, specific technical safeguards, annual Board reporting. Enforced by FTC.
State Breach Notification Laws	All 50 states. Triggered by unauthorized access to personal information. Timelines vary: 30–90 days. Some states require AG notification.
CCPA / CPRA (California)	Businesses meeting size or data volume thresholds collecting California resident data. Consumer rights: access, correction, deletion, opt-out. Enforced by California Privacy Protection Agency.
State Privacy Laws (Others)	Virginia, Colorado, Connecticut, Texas, and others have enacted comprehensive privacy laws. Requirements vary but share common consumer rights framework.

DQI Annual Compliance Calendar

Q1 (January–March)	Conduct or update the formal risk assessment. Review all policies for currency. Confirm vendor security questionnaires are current.
Q2 (April–June)	Deliver security awareness training. Review access control lists. Confirm backup restoration testing has occurred.

Q3 (July–September)	Mid-year review of open risk remediation items. Vendor contract renewals due diligence. Update incident response plan if needed.
Q4 (October–December)	Prepare annual report to Board or senior leadership. Review and update the Written Information Security Program. Plan following year's budget and resource needs.
Ongoing / Monthly	Review backup monitoring reports. Review patch compliance reports. Log any incidents (or confirm no incidents). Update DQI Notebook.

Minimum Viable Evidence File

The following documents, if current and organized, constitute the minimum defensible evidence file for a DQI program audit:

- Written Information Security Program (dated, signed by leadership)
- Most recent Risk Assessment with remediation tracking
- Incident Response Plan
- Vendor inventory with last review dates and due diligence records
- Access control review records (current year)
- Security awareness training completion records (current year)
- Backup validation records (current year)
- Patch compliance reports (last 12 months)
- Annual report to leadership (current year)
- Resource requests made and responses received

Keep this file secure. Restrict access. Back it up. Retain for a minimum of six years.