DIGITAL GOVERNANCE INSTITUTE

POWERING THE ENGINE OF INTERNET TRUST

THE AUDIT ADVOCACY GUIDE

HOW TO SAVE MONEY ON AUDITS

SCOTT S. PERRY, CPA, CISA
DIGITAL GOVERNANCE INSTITUTE

TABLE OF CONTENTS

SCOTT S. PERRY

INTRODUCTION

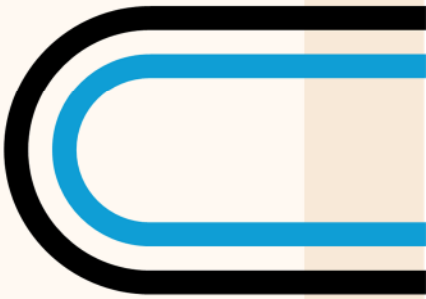
In my over 40-year career working for two Big Four firms, one global consulting, one national audit practice, and ten years running my own CPA firm, I have concluded that all clients are not created equal. While audit fees typically fall within in a general range for specific services, most audit firms do not vary that range depending on how "profitable" or "unprofitable" a client is.

In this guide, I will expose the factors that audit firms use into pricing external audits and ways in which companies can become attractive audit clients where audit firms will want to reduce their fees at least 25% from their standard pricing to maintain their book of business with them. This requires audit clients to be prepared and responsive, and work with an accomplished audit advocate to ensure that they are accountable in their actions in working with their external auditor.

Audit clients have more at their disposal than they realize to reduce audit fees. It may require additional costs to be a "profitable" audit client, but the downstream savings of hard audit fee savings and soft time and efficiency savings will create a well justifiable return on investment over time.

Please read on to learn about the hidden audit costs in greater detail and contact us at the Digital Governance Institute at info@digitalgovernanceinstitute.com to open a dialogue about your specific needs or questions.

EXECUTIVE SUMMARY



While audit fees typically fall within in a general range for specific services, most audit firms do not vary that range depending on how "profitable" or "unprofitable" a client is. Let me explain the context of "profitable" and "unprofitable."

Profitable clients are those that are efficient and predictable, allowing the firm to use a leveraged staff model to recognize their highest return; unprofitable clients are unpredictable, incur expensive senior resource time that may not be fully collectable, and make it difficult for the Firm to recognize a profit using their standard blended rate model.

This Guide explores:

1. The hidden costs incurred by external audit firms,
2. Ways in which companies can be profitable audit clients to the degree that audit firms will want to reduce their fees at least 25% from their standard fees to work with them, such as
   - Signing Up for Multiple Year Engagements,
   - Having an Executive Sponsor,
   - Possessing Knowledge of Audit Process and Scheme,
   - Documenting Audit Controls and Practices,
   - Tying Support Evidence to Asserted Controls,
   - Performing Mock or Internal Audits,
   - Obtaining an Interoperable GRC tool, and
   - Securing an audit advocate.
3. The following Audit Advocacy services that the Digital Governance Institute can provide in helping audit clients reach these savings.
   - Audit Training,
   - Control Process Gap Assessment,
   - Supporting Evidence Gap Assessment,
   - Hyperproof GRC Implementation,
   - Mock Audits and Internal Audit Support, and
   - Audit Engagement Advocacy

INTERNAL COSTS FOR EXTERNAL AUDITORS

An external technical audit against a set of criteria in an established scheme is a professional service. No physical products are purchased, no software is downloaded, and no retainer is procured. For audit clients to better negotiate audit fees, it is imperative that they better understand the costs that external audit firms incur in the delivery of the audit. This section breaks down the key cost factors that are made up of back-end investments and front-end variable costs that comprise the financial commitment an external audit firm takes in delivering audits for its clients. Knowing these factors should help audit clients better understand which costs are immutable and which may be reduced and negotiated based on audit client actions.

EXTERNAL AUDIT ROLES ENGAGED IN YOUR AUDIT

For a sizable external audit firm, it takes a village to propose, contract, plan, execute and report on your audit. Depending on the scope and complexity of your audit, a wide assortment of external audit resources may be working directly with your organization or supporting the visible team in the background. This section outlines the various roles external audit firms deploy to serve your organization:

- **Quality Control or Subject Matter Partners**: These individuals are typically high cost but appear within audits at limited times during audit planning and reporting to ensure that the audit team meets its own methodology guidelines, industry scheme requirements or bringing a complex audit issue to closure.
- **Engagement Partne**r: This high-cost professional drives the sales process and oversees planning, fieldwork, and reporting processes. The amount of time an Engagement Partner spends on an audit depends on the value of the client/audit firm relationship, the scope and complexity of the audit and the bumpiness of the audit rhythm requiring their direct involvement. Engagement Partners do not typically charge for their sales time and their audit time can be minimized if the project remains on-time and within budget without unanticipated issues.
- **Director / Senior Manager**: These roles are moderately expensive and get involved in audits mostly on the planning and reporting phases of the audit. The better Director / Senior Managers are excellent time managers as they are often working on multiple audits at the same time, juggling between your audit and other audits of the Firm.
- **Manager**: Each audit has a dedicated Audit Manager who typically acts as the prime, consistent point of contact between the Firm and your company after the audit is contracted until the audit report is delivered to you. They incur a lower cost to the Firm;

Good Managers are worth their weight in gold if they can successfully manage audit and client expectations without needing higher-priced personnel.

- **Specialized Delivery Staff**: If specialized industry or a unique audit scheme is in scope for your audit, the Firm may deploy specialized delivery resources. Depending on the specialization required, their internal cost can be as high as a director-level practitioner.
- **Staff Resources**: Staff is typically engaged in audit fieldwork where repetitive tasks and a strong methodology reduces audit firm risk. They tend to be the lowest cost resource to the Firm. Inexperienced staff often cause clients some concern when they are deployed on complex audit engagements with unprepared clients that need more seasoned professionals to guide the audit process.

FULLY LOADED COSTS FOR AUDIT PROFESSIONALS

When an auditor is assigned to your audit, the audit firm is paying them a variety of known and lesser known costs to keep them engaged and committed to the firm and to your project. To attract and retain qualified and experienced talent, firms are typically paying for the following in addition to a competitive salary:

- Bonuses
- Medical Benefits
- Paid Company Incentive Trips
- Retirement Contribution
- Paid Time Off
- Professional Membership, Certification, and Training
- Tech Reimbursement for Home Office

All of these costs must be recouped in the fees charged to clients.

SALES AND AUDIT TIME COSTS FOR AUDITORS

External audits require physical time needed by trained professionals that are dedicated to the project at distinct phases of an audit. During that allotted time, resources cannot be assigned to any other activity. The following is a breakdown of the sales and audit delivery phases, and the typical resource allocation that external audit firms expend to meet the needs of each phase:

- **Sales / Contracting**: 10% of the overall engagement time performed by Director-level or Engagement Partner supported by sales and internal legal resources.
- **Audit Planning**: 10% of the overall engagement time performed by Senior Manager
- **Audit Fieldwork**: 50% of the overall engagement time led by a manager and supported by Senior Associates and staff.
- **Audit Reporting**: 20% of overall engagement time performed by Manager with involvement of Senior Manager, Director, Engagement Partner, and Quality Control Partner.

AUDITOR QUALIFICATION COSTS

Not every audit firm is qualified to perform the audit you need. To determine the kinds of audits the Firm is willing to offer the market, it must first analyze the market potential (the number of audits needed by the scheme ecosystem and the frequency of those audits). It then analyzes expected fees it can charge and the costs that the Firm must invest in order to become fully qualified to perform the audit. It also must consider the influence a governing party, audit accreditor or industry association has in encouraging or mandating audits to take place and if there are qualification costs associated as prerequisites in offering the audit to the market. These research and development costs can be steep, including:

- Auditor Certification Fees
- Training Fees
- Marketing & Eminence Building Time/Expense
- Certification Time, Tests and Fees

It is important to better understand underlying fees and costs for prevailing audit / certification schemes. Here are some examples:

- **SOC 2**: Registered CPA Firm fees including the cost of a triennial CPA Peer Review.
- **FedRAMP**: A2LA Accreditation Fees, mandatory training, passing real-time assessment.
- **ISO27001**: Certification Fees to an ISO Accreditation Body, ISO/IEC 17021-1 compliance requirements.
- **WebTrust**: CPA Firm (see SOC 2), deep technical experience auditing certification authorities.
- **CMMC**: Cyber-AB Accreditation Fees, two sets of mandatory training (CCP & CCA), passing real-time assessment from DIBCAC.

As you can see, all have hard dollar costs and take dedicated investment time from otherwise billable audit practitioners. In considering offering these audits as a service, audit firms need to understand the payback period needed to recoup these startup costs.

TRAVEL AND SUBSISTENCE COSTS

Before the pandemic, all audits required some processes to be performed on-site. Travel and subsistence costs include:

- Mileage
- Airfare / Train / Bus
- Hotel
- Meals
- Rental Cars
- Taxi / Uber / Lyft

Audit Firms either charge separately for this or build them into their fixed rates or fees. These costs can accumulate into the thousands per week.

Since the pandemic, most planning, reporting, data gathering interview sessions and evidence presentation sessions can be conducted on-line through videoconference services saving audit time and out-of-pocket costs. However, some audit activities still require in-person observation. They include:

- Data Center Physical Security and Environmental Controls
- Witness Ceremonies
- Disaster Recovery Exercises

In-person observations provide the most pertinent and persuasive evidence for these controls. In planning your audit, it is critical to better understand the techniques needed for evidence gathering and the requirements for in-person observations. In certain cases, it may be easier and more efficient to perform some of the procedures on-site and in-person, even if the initial up-front costs (travel, hotel, etc.) appears expensive. Keep in mind that an efficient audit client wins on the large items and cedes on the smaller items. Covering travel costs may be inconsequential if it reduces the overall hours higher-priced resources, partners, and technical staff require on the audit.

ADMINISTRATIVE FEES

For over twenty years, consulting firms and now more recently, all sizable audit firms, have been charging an additional fee within their invoices to recoup their back-end overhead costs. These costs are for personnel used in contracting, invoicing, collecting and office management. Depending on the firm, these additional charges can range from 5-10% of the service fees. These fees are often a surprise to audit clients, so it is important to understand early in the solicitation process whether they will be added to your invoices. Audit firms do have some discretion in either waiving the fee for the first year or waiving them permanently if the audit/client relationship is right, so it is best to discuss this openly with your audit firms during solicitation.

REDUCING AUDIT COST

Sometimes unbeknownst to audit clients is that their responsibility within an audit is more than the auditors. The audit client is responsible for asserting that they are meeting the control requirements of an audit scheme and must document those controls and provide pertinent and persuasive evidence that they are meeting those requirements.

Most audit firms charge a fixed fee based on the market rate for a particular audit and some reasonable assessment of the time and resource mix needed to deliver the service. That helps audit clients that have fixed budgets since, unless there are extenuating circumstances, audits will not cost more than the stated fee (and Travel and Admin fee). This also means that the longer an audit takes, the less profit the audit firm will make on your audit. What if you can negotiate the audit fee based on minimizing the time the audit takes based on your readiness and responsiveness? The following are actions that audit clients can take to reduce audit firm time or costs on audits and could be used to negotiate audit fees down:

SIGN UP FOR MULTIPLE YEAR ENGAGEMENTS:

If your company knows that it is committed over the long term to continuous yearly or tri-annual audits, plan on longer audit engagement commitments with your auditor. You'll save administrative time contracting. Audit firms typically offer up to 25% off the yearly fees if you establish a longer-term commitment. You can even establish a right to cancel the commitment with proper notification.

EXECUTIVE SPONSORSHIP

How are external audits considered within your corporate culture? Are they checkboxes to fill? Does management take a leadership role in making time and priority for participating in audits. Support from top management to all levels of staff regarding audit participation is a key factor in speeding up an audit and reducing time and commitment of all parties.

Most companies do not prioritize audits. Priorities are rather placed on strategic imperatives, launching products and services, fighting fires, and taking needed time off. However, without a committed executive sponsor and available staff, your audit will take longer than budget and will drag your auditor in wasteful use of their time.

KNOWLEDGE OF AUDIT PROCESS AND SCHEME

During audit sales calls, most times prospects would say, "I need (or I was told I need) a SOC audit or a PCI audit, and I don't have the foggiest idea about it". This is an invitation to a disastrous audit. It implies that the role of the auditor is to guide the auditee through the audit process. **It is not**. It invites a significant amount of education and overhead time by the auditor to explain the process and educate the audit client on what their role and responsibilities are. It would be more suitable to engage with an audit advocate who will lead the audit client through

the audit process and fulfilling their role and responsibilities. We'll discuss this further in the next section.

DOCUMENT AUDIT CONTROLS AND PRACTICES

In order to demonstrate conformance to audit criteria, a company must design and communicate its control practices that it asserts meets the requirements of an audit scheme. To do so, it must know the objective of the audit requirement and how the client application meets that standard. There are tools and services that can be used to document those assertions that we will cover in the next section. If an audit client does not have a complete set of controls to meet audit requirements, the auditor will need to expend extra time and resources to finalize the control set.

TIE SUPPORTING EVIDENCE TO ASSERTED CONTROLS

It is not sufficient to only assert controls to meet audit requirements, an audit client must also be able to present evidence that the control is designed to meet the requirement and that (if engaged in a period of time audit) is it operating consistently over the audit period. Evidence of the control presented to an auditor must be pertinent to the control and persuasive in proving that control meets the requirement. If an audit client does not have a complete set of evidence to map to their controls, the auditor will need to expend extra time and resources to finalize the evidence set.

PERFORM MOCK OR INTERNAL AUDITS OF CONTROLS.

Many organizations have functional internal audit departments or can contract with consulting firms that can pre-test the design and operational efficiency of controls prior to an audit. This can identify audit non-conformities or give the audit client confidence that it is truly ready for an external audit.

OBTAIN AN INTEROPERABLE GRC TOOL

Over the last five years, we have seen the growth of robust governance, risk, and compliance (GRC) tools being offered to audit clients that have features that can save them and their auditor time during audits. They include:

- **"Cross walking" -** a common set of control practices to a wide range of audit schemes reducing the redundancy of mapping the same control to each audit scheme they assert compliance.
- **Risk Assessment –** a built-in risk assessment tool that identifies risks and matches controls to mitigate those risks.
- **Assertion and Evidence Management –** the ability to organize, design and manage your compliance posture under a single pane of glass.
- **Documented Internal Testing –** Some tools have the ability to document the internal testing of controls to give audit clients confidence before the audit that controls are

designed effectively and are performing consistently. It also may highlight control deficiencies it can correct prior to the start of an audit.

- **Plugins to Auditor's Software –** API's and spreadsheet mappings that easily integrate into the auditor's audit methodology tool reducing wasteful, mundane tasks of an audit.

SECURE AN AUDIT ADVOCATE –

An external audit advocate represents its clients in the planning, scheduling and negotiations between them and their auditor to reduce friction, fees and wasteful time spent by both parties. The Digital Governance Institute (DGI) acts as an audit advocate for its clients. In the next section, we will present services that we perform to help clients be better prepared for audits, saving them critical time and external costs.

AUDIT ADVOCACY SERVICES

In this section, we will describe the set of audit advocacy services that the Digital Governance Institute provides its clients so that they can be optimally ready for their audits and can save substantial costs for external audits over time.

AUDIT TRAINING

We can hold training sessions for executives, compliance professionals and subject matter experts on the nature of various audit schemes and how best to prepare. We will introduce a number of concepts and processes described in this section.

CONTROL PROCESS GAP ASSESSMENT

The first step in meeting compliance requirements is for an audit client to convey its policies and practices to meet audit requirements. Our efficient diagnostic analyzes your company's policies and practices against a stated set of audit requirements to identify gaps. The diagnostic is presented as a worksheet that can be used to populate a Governance Risk and Compliance tool and/or to present to the external auditors as part of their process. The diagnostic includes all audit requirements and identifies controls practices that meet the requirements. If the audit client has controls established, our diagnostic rates each control against the following ratings:

- Compliant -The control implements the functionality specified for this audit requirement.
- Not Compliant: The control does not satisfy the functionality specified for this audit requirement.
- No data to be analyzed or
- Not applicable: Either there were no controls to be analyzed in the section or it did not pertain to the scope of a compliance analysis.

SUPPORTING EVIDENCE GAP ASSESSMENT

To sustain audits, companies must present pertinent and persuasive evidence to auditors. In this diagnostic, we will inventory and assess available evidence to support compliance against audit requirements and identify gaps. After analysis, we will categorize evidence against the following ratings:

- In Compliance: The control evidence provided met the audit requirements. assertions.
- Partial Compliance: The control evidence provided only partially met the

audit requirements. Either some aspect of the control was not covered by the evidence, or the evidence did not completely address the control requirement.

- Not in Compliance: The control evidence provided did not meet the audit requirements. assertions.
- Not Tested or Applicable: The audit requirement did not have evidence to test, were not auditable or did not contain assertions to audit.

HYPERPROOF GOVERNANCE RISK AND COMPLIANCE IMPLEMENTATION

Using our partnership with Hyperproof, we can implement a comprehensive compliance platform that consolidates all compliance schemes that companies must comply with enabling the company to significantly reduce the cost of compliance. Hyperproof provides a complete compliance operations platform to help companies plan information security, data privacy, and compliance projects, execute them and monitor progress and keep records:

- **Record-Keeping:** Hyperproof serves as the single source of truth for all of your risks and compliance activities. Hyperproof can be where you house all infosec compliance requirements and standard frameworks (e.g., SOC 2, ISO 27001, PCI, etc.), controls universe and evidence. Evidence retrieval is easy with Hyperproof, and your organization will be well-prepared for a spot audit at any time. If you choose, you can also use Hyperproof to keep track of your risks. Risks can be mapped back to existing controls — allowing you to understand how well existing risks are managed.
- **Planning:** You can use Hyperproof to determine your scope of work and what needs to be done to meet compliance frameworks' requirements (e.g., what controls need to be created), identify owners and contributors to the work, create timelines, and assign tasks. Equally important, Hyperproof will help you identify existing controls you can leverage to meet requirements for new compliance frameworks.
- **Workflow optimization and automation:** Cut the time your team spends on manual tasks by up to 70 percent, and free up time to work on the most impactful activities. With Hyperproof, you can improve productivity by automating manual tasks (e.g., collect evidence automatically, set automated reminders for others to submit evidence) and remove friction points from collaborative processes.
- **Reporting and monitoring:** Hyperproof makes it easy for everyone within your organization to get on the same page about what the current state of your compliance efforts are and where improvements are needed. With real time analytics, your team knows exactly where they should spend their time and energy. Potential problems, such as outdated controls, are identified early before they metastasize into costly incidents.
- **Scaling:** Hyperproof helps organizations easily scale up their information security compliance programs and manage multiple audits. With Hyperproof, you can map a control to multiple frameworks' requirements and re-use evidence across multiple audits.

MOCK AUDITS AND INTERNAL AUDIT SUPPORT

If we have not performed audit readiness on your control design and evidence mapping, we can act as your Internal Auditor by conducting mock testing against audit requirements or conducting internal audits. We can assess control practices and evidence using our diagnostics to quickly identify gaps and non-conformities prior to exposing your organization to external audit findings it must disclose to your relying parties.

AUDITOR ENGAGEMENT ADVOCACY

We can act as your advocate during audits in planning and evidence gathering sessions. We can work with you to defend your compliance posture with external auditors and address non-conformities that arise during the audit. Here is how we advocate for our clients during each phase of an external audit:

- **Planning:** We can participate in audit planning meetings with the audit firm to help ensure that the audit activities will flow frictionlessly.
- **Fieldwork**: We can act as a back-room advisor to the audit. This will include participating in interim meetings with the Audit Firm regarding findings encountered during fieldwork and working with management to develop audit remediation plans.
- **Reporting**: We can participate in all status meetings with the Audit Firm to advise management on proper posture and response. We can also participate in the drafting of any management assertion and representation letter which may be a client responsibility for the audit.

CALL TO ACTION

If you would like to learn more about how the Digital Governance Institute may help you to save money on your technology audits, please contact us at info@digitalgovernanceinstitute.com.

Scott Perry is the Founder and CEO of the Digital Governance Institute where he provides a variety of governance solutions in the emerging space of governance of digital assets. Scott is a recognized global leader in digital identity, blockchain, and verifiable credential governance and accreditation. He has worked with the world's most respected SSL-certificate issuers, aerospace and defense companies, and government agencies such as the US Senate Sergeant at Arms and Federal Aviation Administration.

He is a Co-Chair the Trust Over IP Foundation's Governance Stack Working Group where he has authored and contributed to most of its governance and assurance publications driven to create standards and accountability in decentralized identity and verifiable credential networks.

As a hands-on governance and cybersecurity consultant and auditor, Scott provides deep and impactful advice that you would expect from a leader in the field.