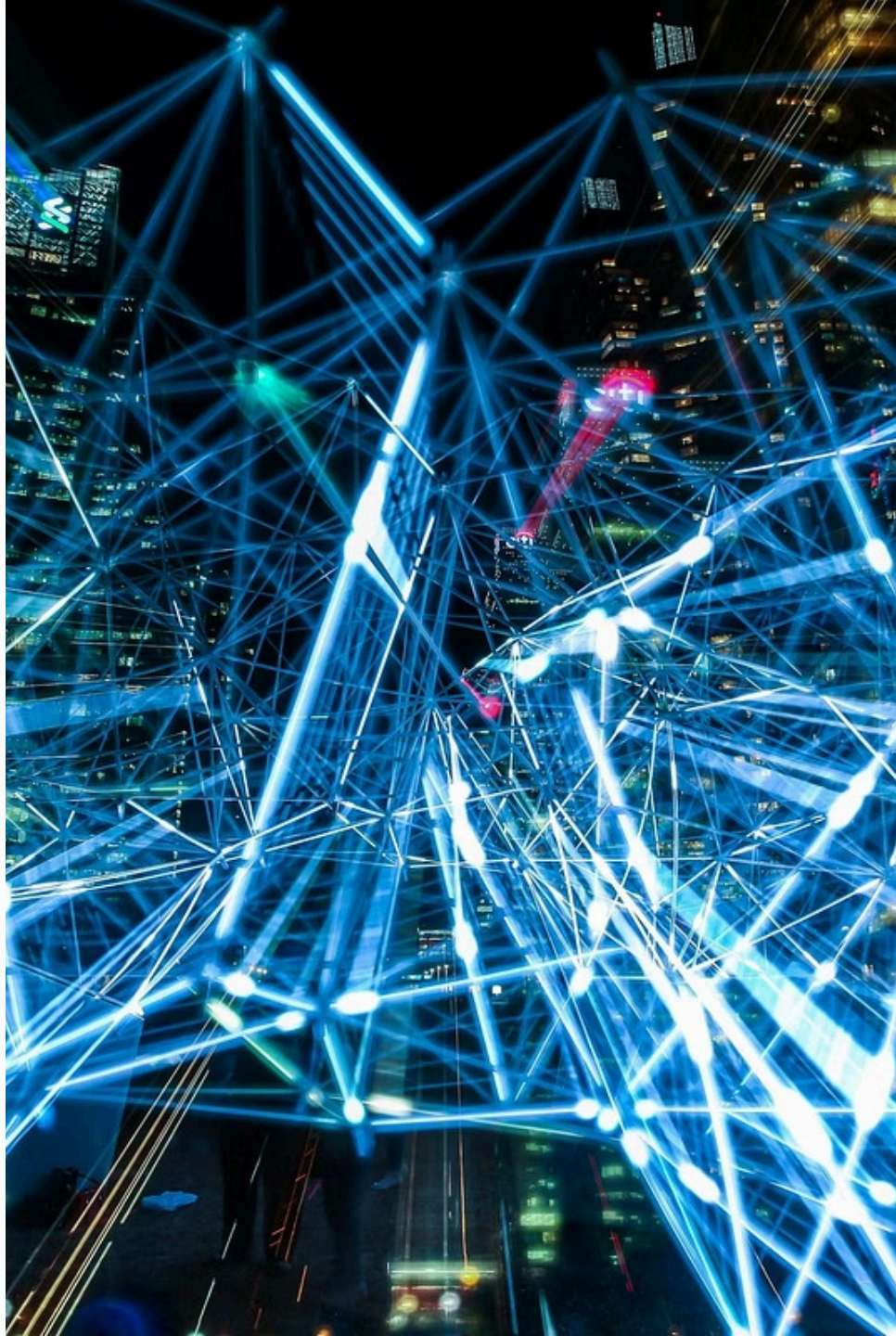
C-AE24 STRATEGIC BUSINESS ANALYSIS MODULE 10

Information System Advisory Part 2: Welcome to the Digital Fortress

Rosalinda E. Perez, CPA, MBA, LPT



The High Stakes of Tech Failure

The Cost of Vulnerability: Why Defense Matters

Retail

Payment servers freeze on Black Friday — millions lost every minute.

Healthcare

Ransomware locks patient records, halting surgeries and triggering regulatory fines.

Finance

Ledger manipulation siphons corporate cash — undetected until it's too late.

Corporate security is no longer a back-room IT issue. It is a core **fiduciary duty**. When systems fail, public trust evaporates, stock prices crater, and CEOs are fired.

FOUNDATION

IT General Controls (ITGCs)

ITGC: The Foundation of Corporate Trust

ITGCs are the massive outer walls of your digital castle. They don't audit individual transactions — they govern the **entire technology environment**: who enters the server room, how code is tested, and how data survives a disaster.

If the outer walls are broken, no data inside the fortress can ever be trusted.

The Four Pillars of ITGC

Four strategic pillars — each protecting a critical survival zone of corporate infrastructure. If one crumbles, the entire system is exposed.

Manage Access

Identity verification and strict user permission controls.

Manage Change

Bulletproof protocols for updating software without crashing operations.

Manage Operations

24/7 network health, error logging, and disaster recovery readiness.

Governance & Compliance

Aligning tech with corporate policy, ethics, and international law.

Pillar 1: Access Control & Identity

The Principle of Least Privilege — every employee accesses only what their role requires, and nothing more.

Multi-Layer Authentication

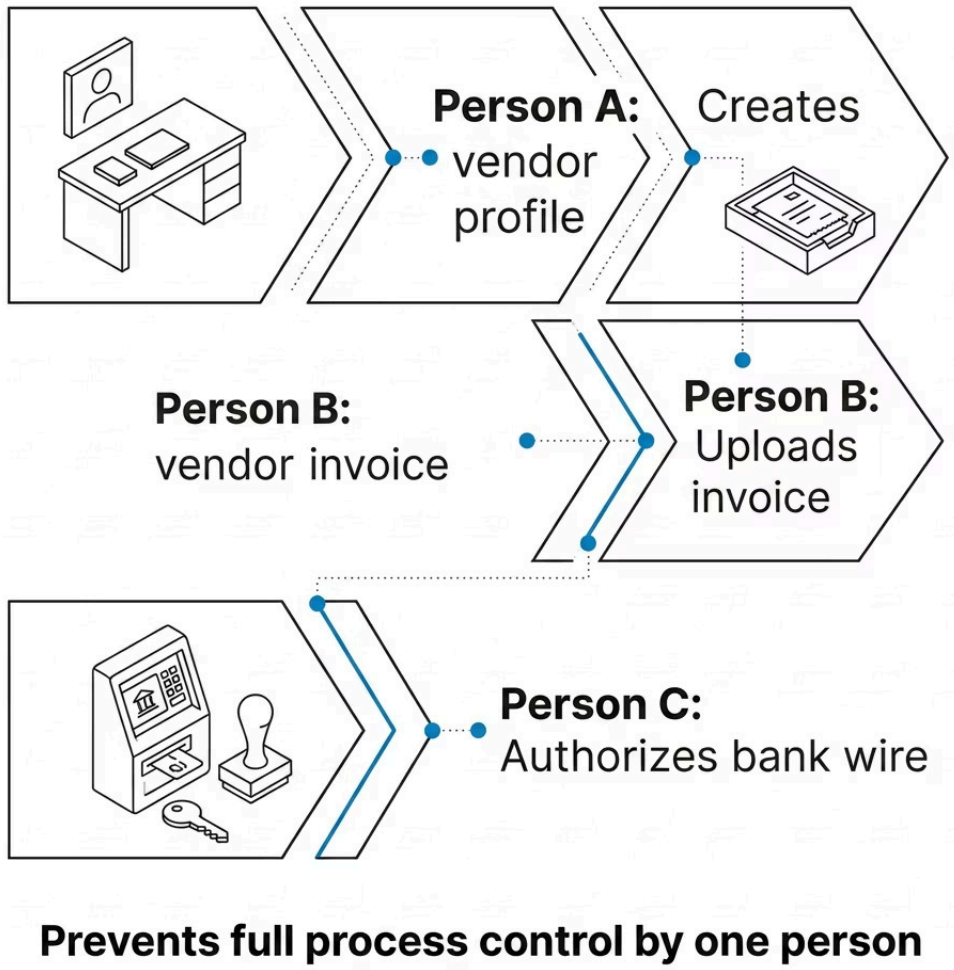
Complex passwords, biometric scans, and one-time mobile token verification.

Quarterly Access Reviews

Managers audit permissions every quarter — departed employees are cut off instantly.

Role-Based Permissions

A cashier processes refunds. A financial analyst reads reports. Neither touches the other's domain.



CRITICAL CONCEPT

Segregation of Duties

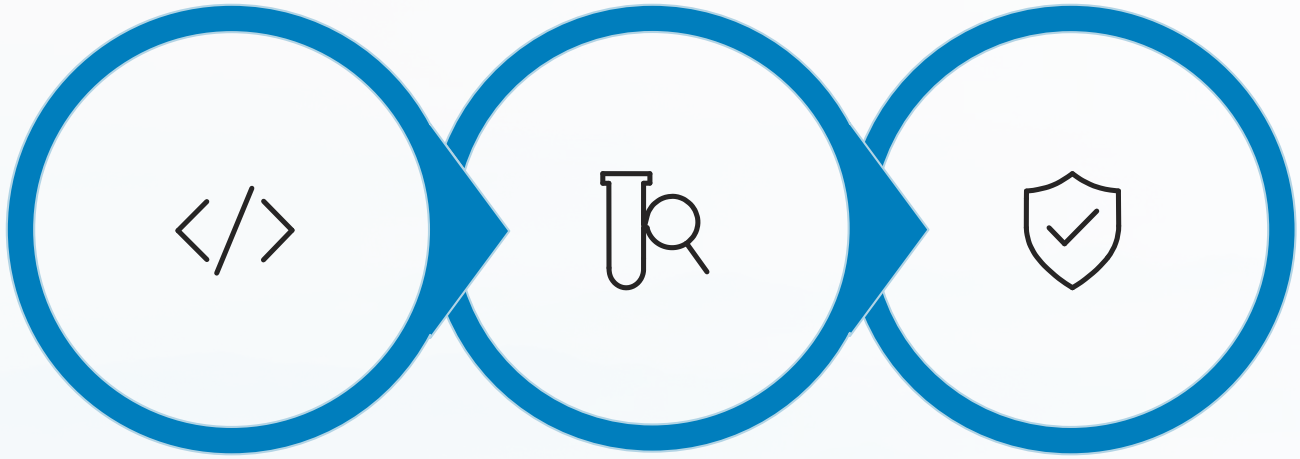
The #1 weapon against corporate fraud. No single person should control an entire high-risk financial transaction from start to finish.

Without SoD, an accounting manager can create a fake vendor, draft a phony invoice, and wire corporate cash to their personal account — unchecked.

SoD forces internal checks at every step, making solo fraud nearly impossible.

Pillar 2: Change Management Protocol

A single typing error in production code can paralyze a global enterprise. Advisors enforce a rigid, multi-stage workflow to protect live systems.



Critically, developers are **blocked from deploying their own code** to production — eliminating both errors and insider manipulation in a single control.

Pillar 3: Managing Operations

The enterprise system is a heavy-duty engine — it demands constant monitoring, maintenance, and emergency protocols.

Real-Time Monitoring

Automated software catches and logs errors the instant they occur.

Disaster Recovery Plan (DRP)

Encrypted backups sync continuously to off-site global cloud servers.

Incident Response

If a server fails at 3 AM, engineering teams are paged before the morning shift arrives.

Pillar 4: Governance & Alignment

The strategic layer that keeps the entire technology ecosystem aligned with corporate policy, ethics, and law.

IT Steering Committees

CEO, CFO, and CIO convene to approve tech budgets and evaluate enterprise risk.

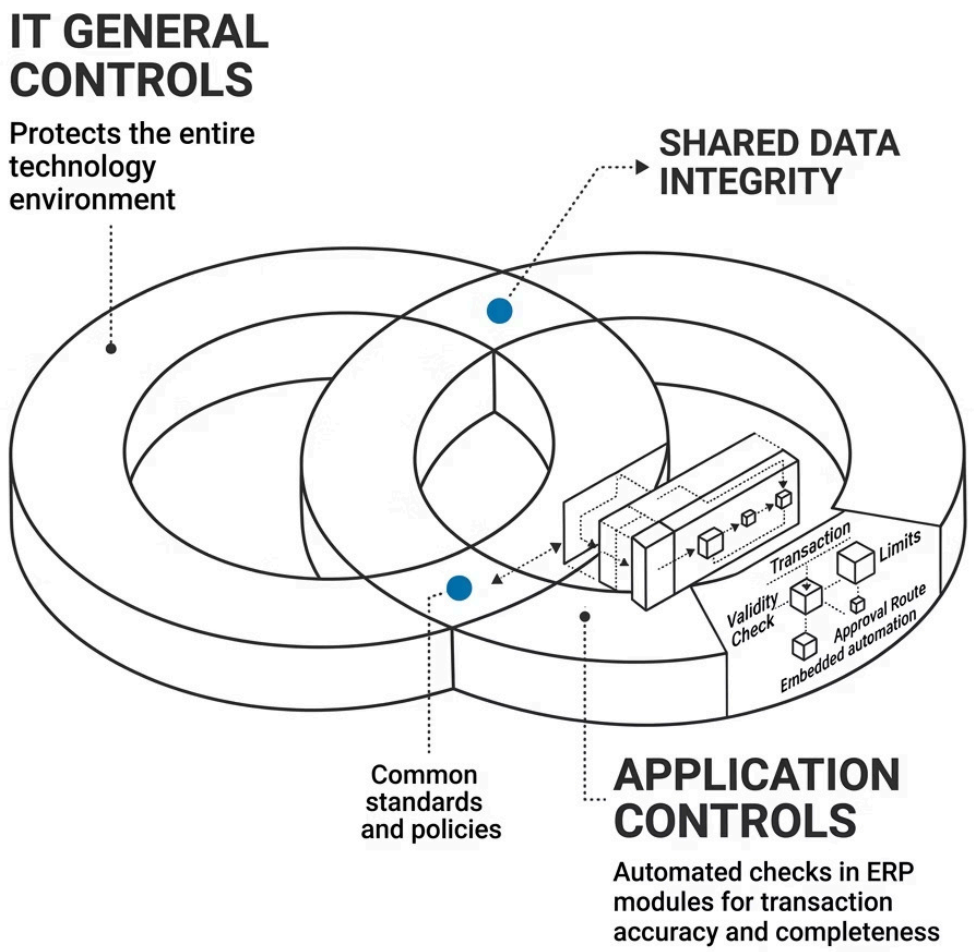
Corporate Policy Manuals

Define data privacy, employee device usage, and AI ethics standards company-wide.

Legal Compliance

Full alignment with frameworks like Sarbanes-Oxley and GDPR — protecting shareholders.

Application Controls vs. ITGCs



Two Layers. One Defensive Grid.

ITGCs are the broad outer walls — protecting the entire company technology environment.

Application Controls are smart digital bouncers embedded inside specific software: blocking negative numbers on expense reports, rejecting future-dated purchase orders, and enforcing mandatory approval fields.

Together, they ensure both the **environment is safe** and the **data inside it is accurate**.

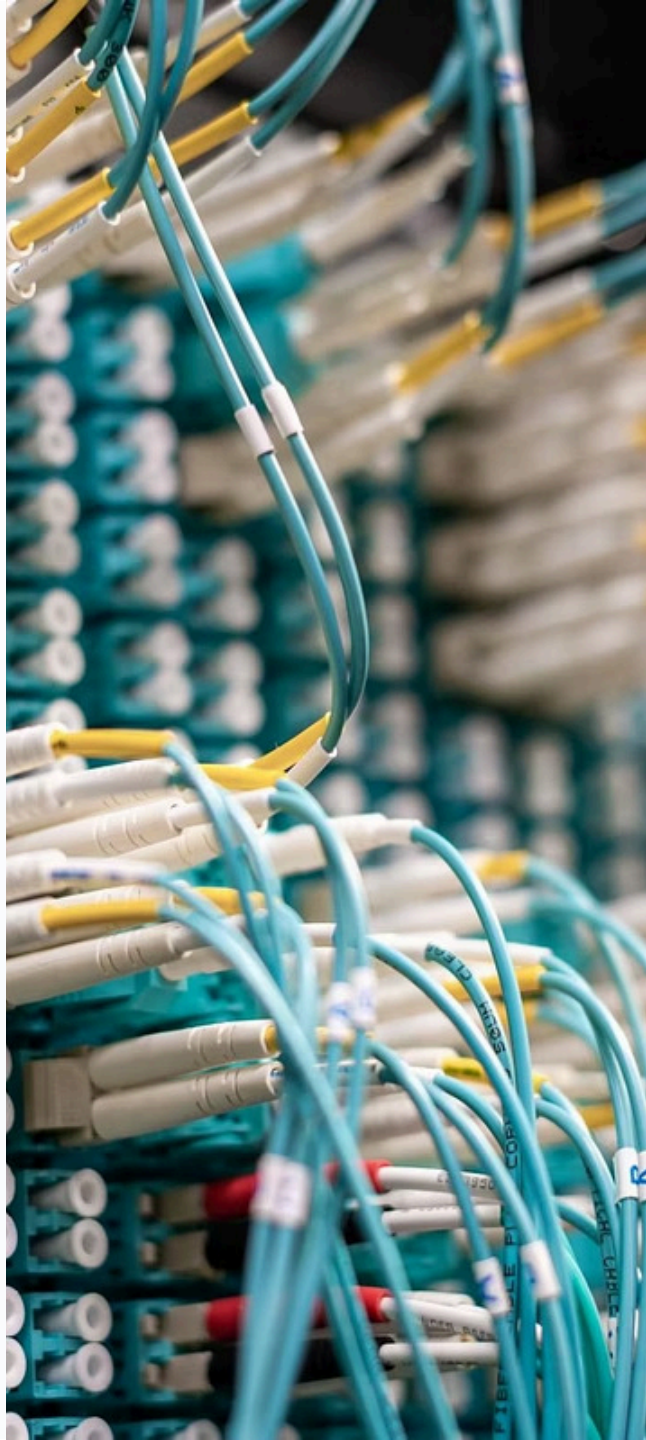
Third-Party Cloud Risks

The Cloud Shift: Outsource Operations, Not Accountability.

Enterprises upload confidential customer data, payroll files, and general ledgers to external cloud giants — AWS, Azure, Google Cloud. Efficiency soars. But risk follows.

> ⚠ If a cloud vendor is breached, your client's business halts. The public will still blame your client — not the vendor.

Golden Rule: You can outsource your operational technology. You can never outsource your legal accountability. Audit your partners relentlessly.



THIRD-PARTY ASSURANCE

Demystifying SOC Reports

A **SOC report** — System and Organization Controls — is an independent, certified security report card issued by elite public accounting firms.

Cloud vendors hire external auditors to inspect systems, test defenses, and deliver an unvarnished review. As an advisor or risk officer, you **demand and analyze this report line by line** before signing any contract.

Never take a vendor's word. Require verified, independent, mathematical assurance.

SOC 1 vs. SOC 2: Choosing the Right Report

Two reports. Two completely different targets. Knowing which to demand is a critical advisor skill.

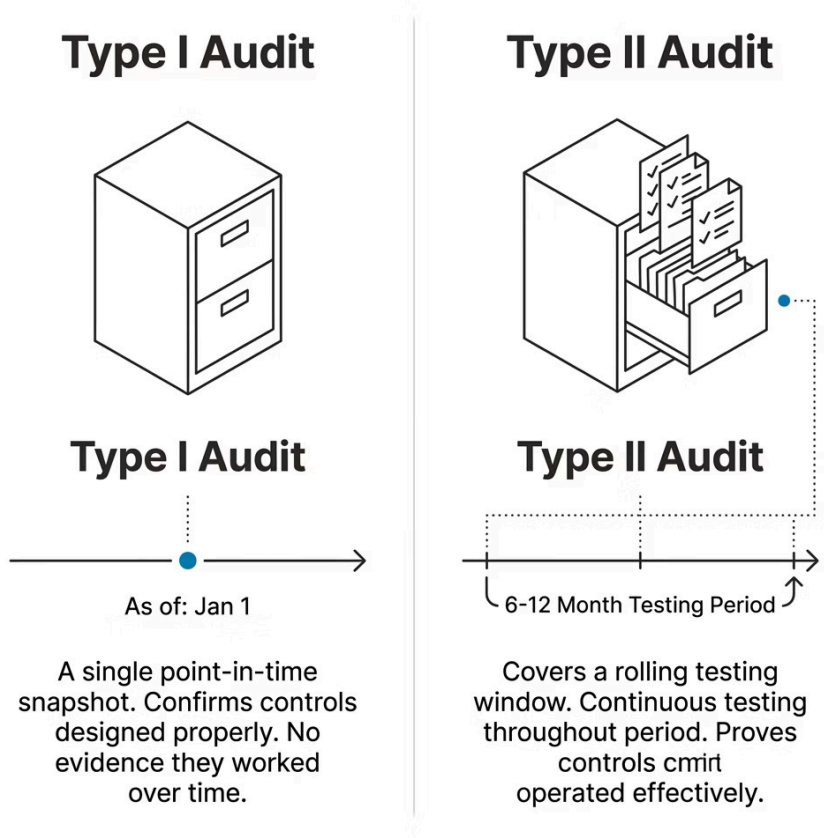
SOC 1 — Financial Reporting

Targets controls that impact a client's **financial statements**. Required when a vendor processes payroll, tax calculations, or ledger entries. Ensures your balance sheet stays clean.

SOC 2 — Operational Security

Evaluates controls across five trust principles: **security, availability, processing integrity, confidentiality, and privacy**. Required when a vendor stores sensitive data — medical records, credit card files, PII.

Type I vs. Type II: Depth of Evidence



Why Type II Is the Gold Standard

A **Type I** report confirms controls were designed correctly on one specific day. Fast — but limited. It proves controls existed on Tuesday. It says nothing about Wednesday.

A **Type II** report proves controls *actually worked* across a continuous 6–12 month testing window, with documented evidence at every stage.

Elite advisors always demand Type II — it delivers genuine, high-velocity assurance.

SOC 3: The Public Scorecard

SOC 1 and SOC 2 reports contain sensitive technical secrets — network maps, server locations, internal control pathways. Publishing them publicly hands hackers a blueprint.

SOC 3 solves this. It strips away all confidential data and delivers a clean, simplified trust certificate stating the company passed an independent audit — without revealing internal architecture.

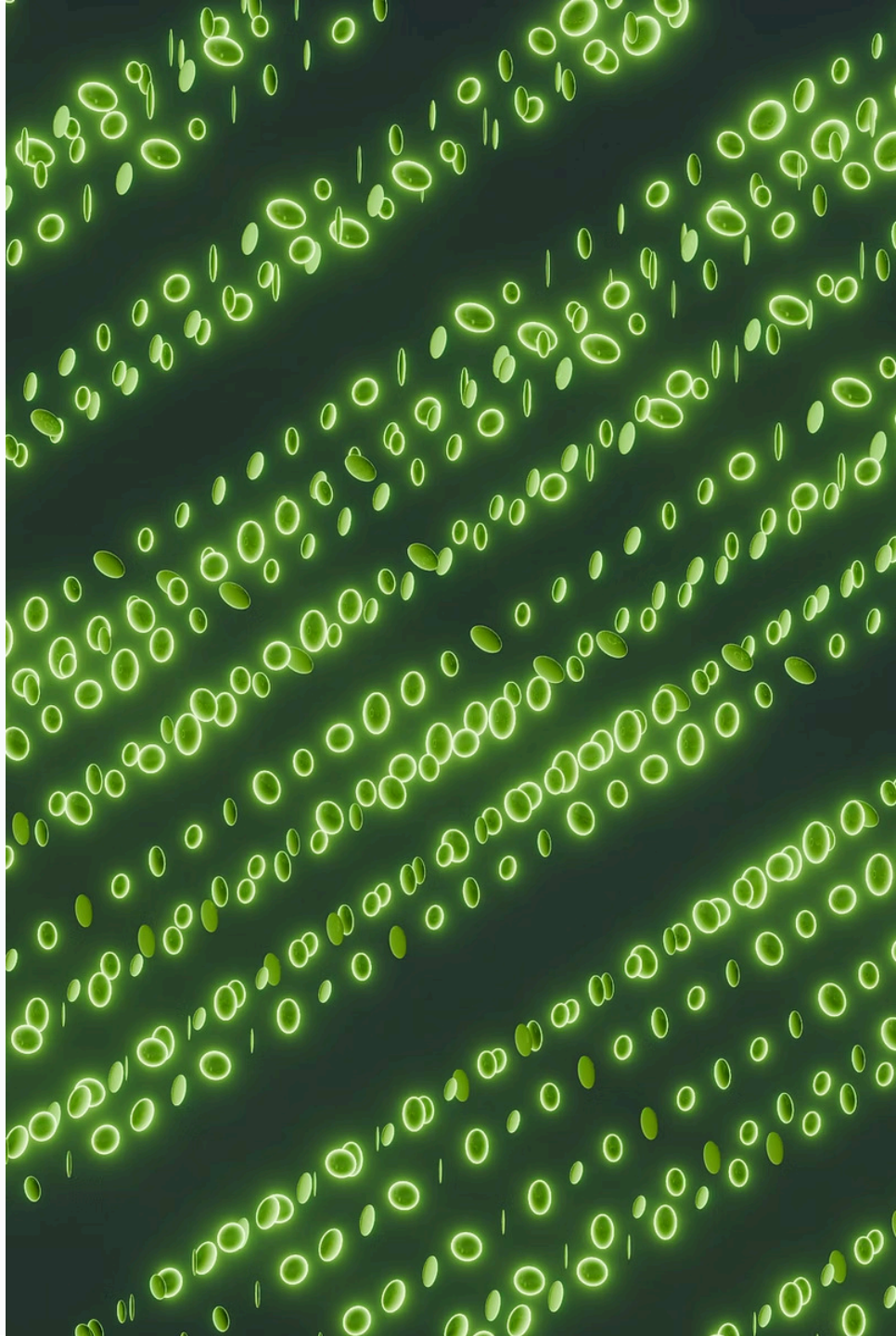
Tech giants post SOC 3 seals on their websites as a **marketing weapon** to win customer confidence. But SOC 2 Type II remains the heavy-duty document required behind closed doors.

SECTION 2

Forensic Analytics: The Digital Detective

Even with the best preventive controls in place, sophisticated bad actors will occasionally penetrate the system. Standard financial reports will miss the crime — because the numbers look perfectly normal on the surface.

Forensic Analytics deploys data science, statistical algorithms, and investigative logic against ERP transaction databases to expose ledger manipulation and catch corporate criminals — red-handed.



The Psychology of Fraud: The Fraud Triangle

To catch a corporate thief, you must first understand what drives them. Corporate fraud only occurs when three elements collide simultaneously.

Pressure

The motivation to steal — crushing personal debt, a gambling addiction, or impossible sales targets set by leadership.

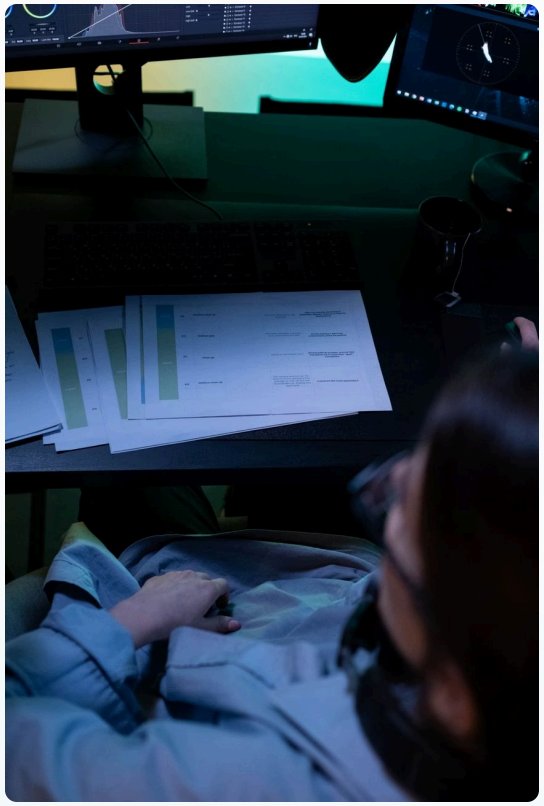
Opportunity

A loophole in internal controls — weak access permissions, absent segregation of duties — that allows theft with low perceived risk.

Rationalization

The internal justification — *"The company underpays me anyway."* The mental gymnastics that preserves the criminal's self-image.

As advisors, our data tools are engineered to ruthlessly **dismantle Opportunity** — eliminating the conditions that make fraud possible.



Diagnostic Forensics: Excavating Hidden Patterns

When criminals manipulate accounts, they leave **data signatures they cannot erase**. Diagnostic Analytics uncovers them.

Midnight Journal Entries

Flag manual entries over $10K posted between midnight and 4 AM on Sundays.

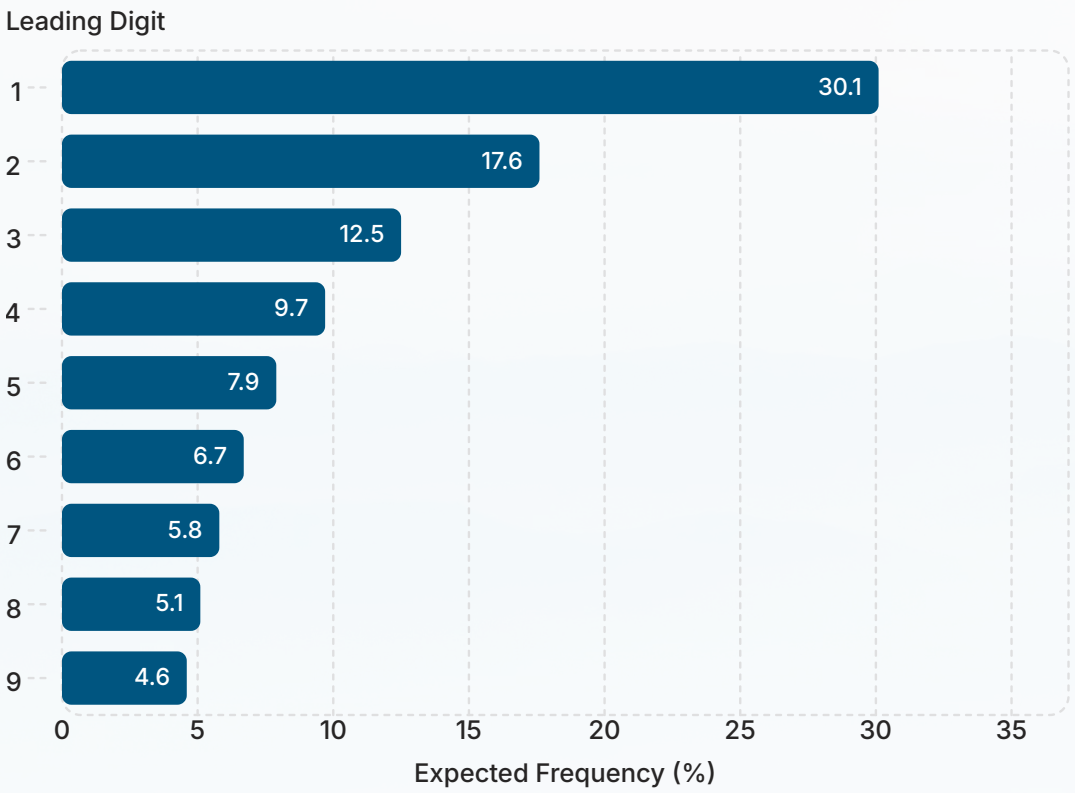
Threshold Manipulation

Expose users processing transactions just below mandatory approval limits.

Impossible Logins

Flag employee logins from two distant countries within hours of each other.

Benford's Law: The Mathematical Shield



Exposing Phony Numbers Naturally

In any organic, unmanipulated dataset — real invoices, real expenses — the digit **1** leads ~30% of the time. The pattern cascades naturally down to **9** at under 5%.

When corrupt employees invent fake transactions, human psychology disrupts this distribution. Numbers are chosen randomly, creating **unnatural spikes** in the chart.

Run a Benford's Law test against millions of vendor transactions instantly. An anomalous spike is mathematical proof of potential fraud.

Outlier Analysis & Duplicate Detection

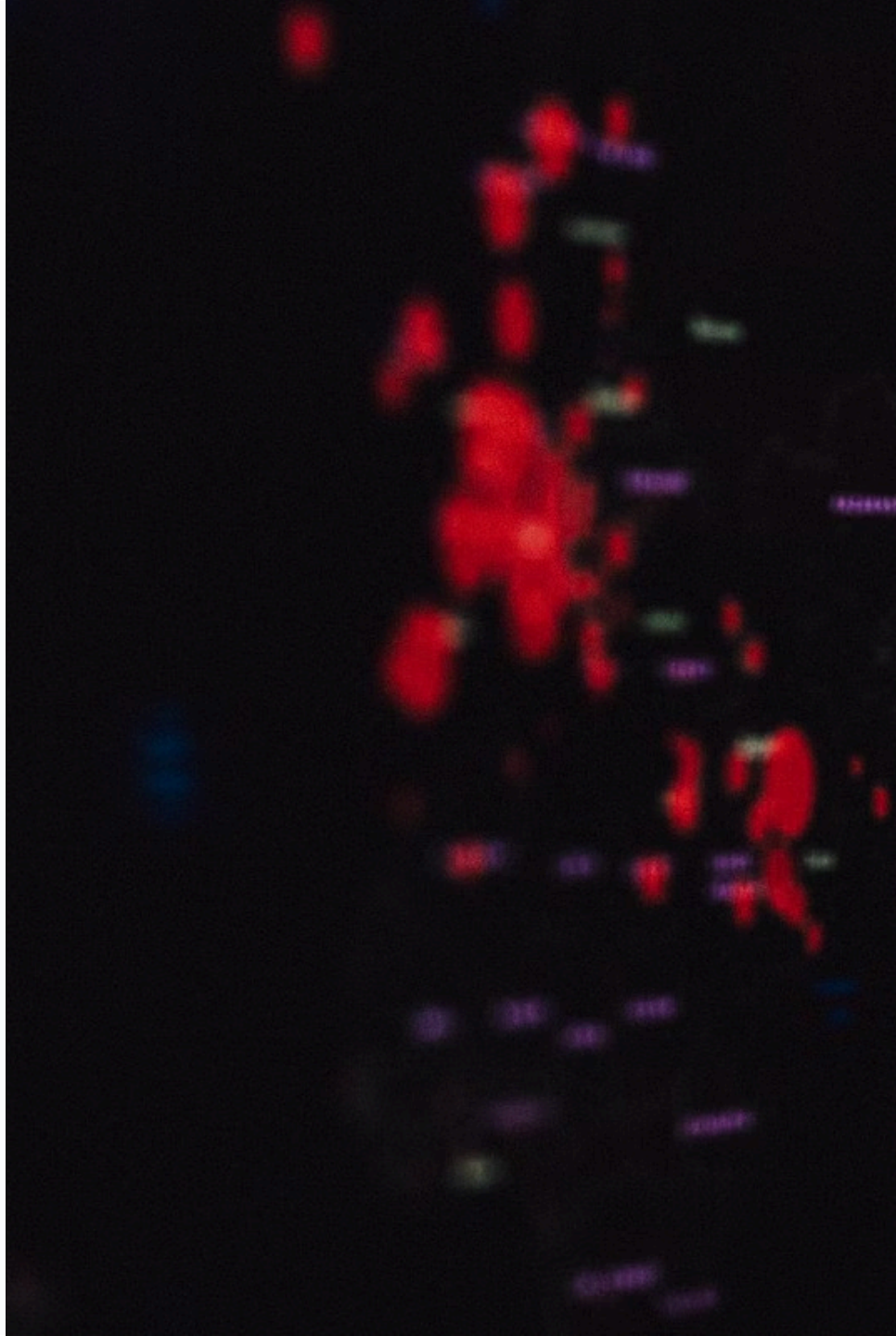
Many thefts are surprisingly simple — they rely on transaction volume to hide basic slip-ups. Two automated scripts catch them cold.

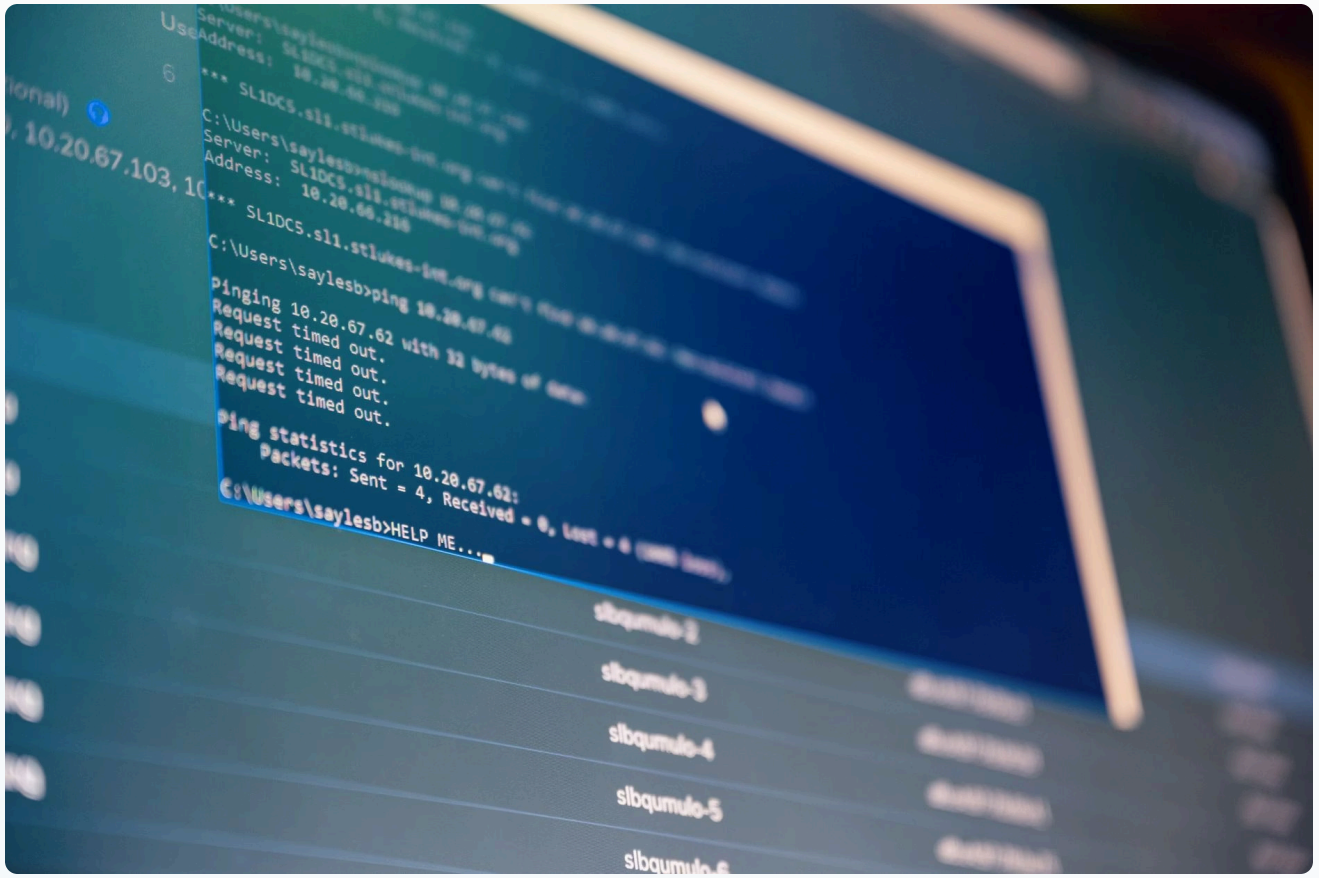
Duplicate Detection

Scans accounts payable for invoices sharing identical amounts, vendor names, or near-identical invoice numbers. Corrupt employees submit the same legitimate bill twice — routing the second payment to a personal account.

Outlier Analysis

Statistical algorithms isolate transactions that deviate massively from baseline behavior. A branch that averages $200/month in supplies suddenly shows a $5,000 purchase — the script pings an alert immediately.





Forensic Visualization: Mapping Collusion

A flat spreadsheet of 50,000 rows cannot expose a fraud network. A **visual link-analysis chart** does it instantly.

Address Matching

Red connection lines fire if an employee's home address matches a vendor's banking address.

Phone Number Flags

A manager's personal number matching a newly approved vendor profile triggers immediate review.

Contract Funneling

Visualize if a single buyer routes contracts to one vendor without competitive bidding.

Continuous Monitoring: The Predictive Radar

The industry is shifting from reactive forensic autopsies to **real-time defense**.

01

100% Transaction Coverage

Every corporate transaction is scored by automated risk scripts the millisecond it is entered.

02

Risk Scoring Engine

Entries are evaluated against pre-set fraud indicators: dollar value, user history, and timing anomalies.

03

Automatic Intervention

High-risk transactions are frozen, funds held, and compliance teams are alerted — before cash leaves.

Part 2 Summary: The Defensive Blueprint

Everything we have covered — integrated into a single master framework.

Domain	Framework	Core Purpose
ITGC Pillar 1	Access Control & SoD	Eliminate internal fraud opportunity
ITGC Pillar 2	Change Management	Protect live systems from code errors
ITGC Pillar 3	Operations Management	Ensure 24/7 continuity and recovery
ITGC Pillar 4	Governance & Compliance	Align tech with legal and executive strategy
Third-Party Risk	SOC 1 / SOC 2 Type II	Verify vendor security independently
Forensics	Fraud Triangle + Benford's Law	Detect and expose hidden criminal behavior
Continuous Monitoring	Real-Time Risk Scoring	Stop fraud before cash ever leaves

The Complete Advisor: Driving Profit, Securing Value

Part 1 — Data Architect

ERP integration, process blueprinting, and BI dashboards that eliminate friction, forecast the horizon, and accelerate margins.

Part 2 — Digital Defender

IT governance, third-party risk analysis, and forensic data science that secure every asset you just built.

Master only one half and you build either a **profitable but vulnerable** business — or a **secure but stagnant** one. The complete, high-value advisor does both. **That is the elite combination.**

Your Future Starts Now

You now speak the language of the boardroom *and* the server room. The demand for professionals who bridge business strategy and system architecture is **skyrocketing**.

Consulting Firms

Apply ITGC and forensic frameworks in high-stakes client engagements.

Public Accounting

Lead SOC report evaluations and IT audit engagements globally.

Corporate Leadership

Sit in the risk committee. Own the governance conversation. Protect shareholder value.