Taking a Product from Napkin to SOC2 Certified & TSA Trusted

How a Mobile Drivers License App Became a Boarding Pass

Fall 2025

Who Am I?

https://duffy.dev

Background in **development, architecture, mathematics, team leadership, marketing, and strategy**

If you've:

- Made an **Interac purchase**
- Bought a **lottery ticket**
- Visited a **hospital**
- Used your **passport at a border**
- …you've likely used my work

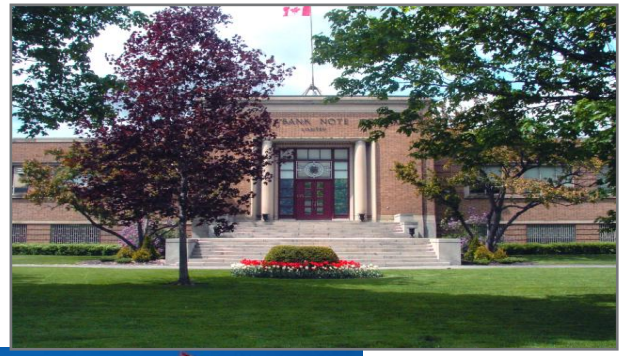
Led **security and development** for systems protecting **hundreds of millions** across **80+ countries**

Passionate about **deep research**—recognized by **OCIPEP** for outstanding work in secure networks

Led teams behind industry firsts:

- **First high-security ePassport**
- **First driver's license with printed digital signature**
- **First public Mobile Driver's License**

Founded 1897 - CBN is an Ottawa-based Company



We deliver secure solutions for **Payment**, **Identity**, and **Lottery** markets worldwide.

Our team: 2200 employees worldwide across 16 countries including Canada, US, and Europe.

Our reach: 80 countries, millions of daily users, and systems with 50,000+ active nodes.

Our users: citizens, technical teams, frontline staff, and plant operations.

Our capabilities:

- Firmware & cryptography
- Biometrics & penetration testing
- Classified network security & malware analysis
- Manufacturing systems & physical product design
- Digital printing, RF, and optical technologies

Agenda

1. Overview
2. Pilot
3. Standardizing for Rollout
4. Certifying
    1. Scorecard
    2. ISO/SOC
    3. Pipeline
    4. Threat Modelling
5. TSA approval and Conclusions

Current Security Feature Set for the 2025 release of the Mobile Drivers License

Security Response: Mobile Drivers License (MDL/MiD) 2025

Enterprise-Grade Cloud Infrastructure

- **Primary Hosting**: Secure datacenter with direct DMV integration
- **Microsoft Azure Disaster Recovery**: Full disaster recovery environment deployed as Software-as-a-Service (SaaS) in Microsoft Azure cloud, providing:
  - Global enterprise-grade security and compliance
  - Advanced threat protection and monitoring
  - Automatic security updates and patching
  - 99.9% availability SLA with geographic redundancy
  - Azure's comprehensive compliance certifications (SOC, ISO 27001, and more)
- **Network Segmentation**: Components segregated across DMZ services, secured mDL VLAN, and protected database environments
- **Web Application Firewall**: Cloudflare protection manages traffic volume and secures all connections from mobile applications

Advanced Authentication & Identity Verification

We use **multi-factor authentication** to confirm your identity through:

1. **Physical ID Verification**: You capture an image of your physical ID card's PDF417 barcode for identity verification
2. **Live Biometric Authentication**: Advanced liveness detection technology ensures the selfie image is from a genuine human, preventing presentation attacks
3. **1:1 Facial Recognition**: Your live selfie is compared against your official DMV photo of record using sophisticated facial recognition technology

Privacy & Data Protection Commitments

Minimal Data Retention

- **No PII Storage**: Our system does not retain your personal information after processing
- **On-Demand Credentials**: Digital credentials are generated only when requested, not pre-cached
- **Automatic Data Purging**: All transaction data is automatically wiped after completion
- **Temporary Processing**: Enrollment images are temporarily stored and removed immediately after processing, regardless of success or failure

ISO 18013-5 Compliance

Our solution is fully compliant with the international ISO 18013-5 standard for mobile driving licenses, ensuring:

- Standardized security protocols
- Interoperable credential format

Strong Encryption & Data Protection

Data in Transit:

- All communications between system components use TLS encryption with client certificates
- Every device receives a unique TLS client certificate bound to your unique ID for secure communications

Device Binding Security:

- Your credential is bound to your specific device through multiple security layers
- Each device gets a unique identifier required for all mDL account actions
- If you enroll a new device, the previous account is automatically deactivated for enhanced security

Advanced Security Features

Secure Key Management

- **FIPS 140-3 Compliant Hardware Encryption**: Two dedicated FIPS 140-3 compliant Hardware Security Modules (HSMs) deployed for certificate management - one for root certificate authority operations and one for issuer certificate management, providing the highest level of cryptographic security
- Sensitive key material for document signing certificates stored in secure key store
- Document signing certificates ensure credential authenticity and integrity

Presentation Attack Detection

- Advanced anti-spoofing technology prevents fraudulent enrollment attempts
- Real-time analysis ensures biometric samples are from live individuals
- Protection against photo, video, and mask-based attacks

Audit & Monitoring

- Comprehensive logging and monitoring of all system activities
- Regular security assessments and third-party validation

Third-Party Security Validation

Our security measures have been independently validated by leading testing organizations:

- **UL (Underwriters Laboratories) Testing**: Comprehensive testing using the UL mDL Application Test Suite against ISO/IEC 18013-5:2021 standards, validating security mechanisms, data model compliance, and use case functionality
- **FIME Certification**: Independent testing and certification against ISO/IEC 18013-5:2021 standards for mobile driving license compliance
- **SOC 2 Type 2 Audit**: Comprehensive evaluation of security, availability, confidentiality, and processing integrity controls
- **TSA Risk Control Benchmarks**: Meeting federal transportation security requirements for trusted identity credentials

Your Control & Privacy Rights

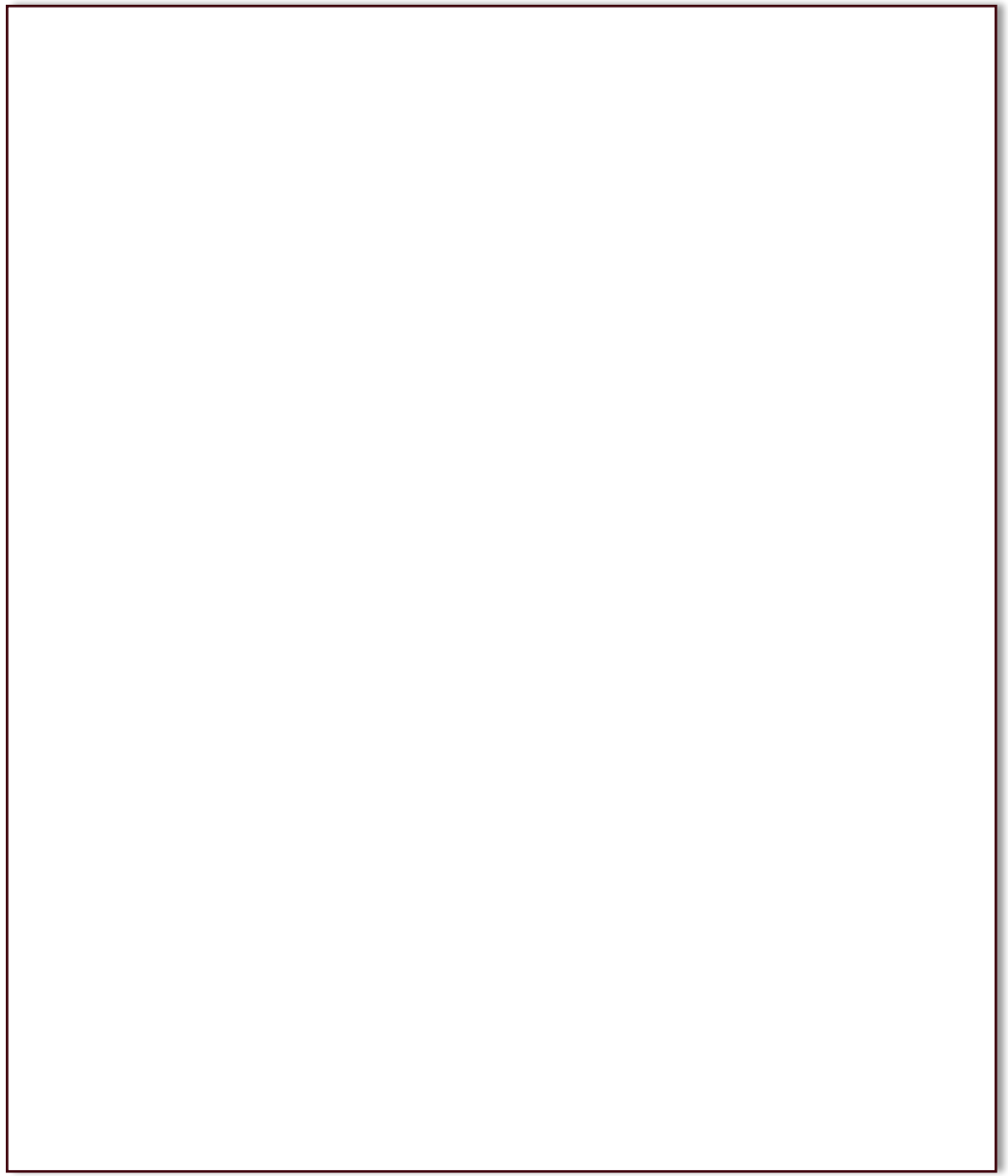
- **Selective Disclosure**: You control which attributes to share when presenting your mDL
- **Offline Verification**: Your credential can be verified without internet connectivity in many scenarios
- **Account Management**: You maintain full control over your account and can revoke access at any time

Continuous Security Improvement

We continuously monitor and enhance our security measures, including:

- Regular security updates and patches
- Ongoing threat assessment and mitigation
- Compliance with evolving industry standards and regulations

Proposed Security Feature Set for Mobile Drivers License 2017



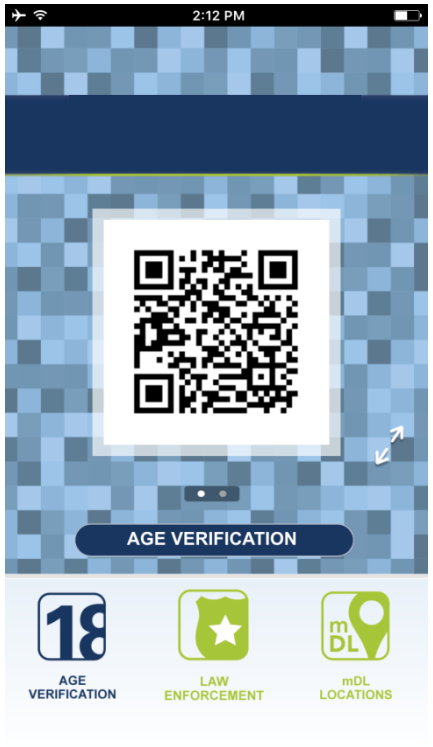
What is an mDL

- App version of wallet ID
- Real-time DMV data
- Context-sensitive disclosure (roadside stop vs. bar entry)
- Trusted identity foundation for eGov & voting

Big Challenges: Secure, Compliant, on Time

Multiple Stakeholders: State Government, Law enforcement, auditors, TSA

Huge Consequences: Government identity forgery – denied services, delayed entitlements, national security issues



From Idea to Trusted Product: Four-Phase Security Playbook
Pilot → Standardize → Certify → Leverage

Pilot

1. Identify 5 Worst Risks
2. Limited scope / Controlled Environment
3. Prove Value; Build Momentum

Standardize

1. Interoperability: Find where this has been done
2. Support extra functionality
3. Communicate progress; build trust

Certify

1. ISO for adoption
2. Add custom controls (NIST 800-53)
3. SOC2 for Operations

Leverage

1. Use existing certifications / evidence
2. Map matrix to asks
3. Package everything for customers/regulators

Why Certify?

🌎 **Customers:** "Acceptance Snowball" – each step leverages previous trust
- TSA Approval built on SOC2, SOC2 built on ISO, ISO built on NIST 800-53

💼 **Business Teams:** Can create a competitive moat – chip manufacturers use this strategy

💡 **Technical Teams:** Security = Product Acceptance
- Every onboarding meeting asks: "Do they have a security certification?"

🛡️ **Security Teams:** Every security person will probably tell you - it makes you better

Pilot: Why this matters

1. The pilot phase let us understand the initial problems
2. A limited scope allows us a better chance to succeed
3. Pilots are necessary to build momentum

Late night bar conference planning session with app vendors and our customer

This conference had several demos that yielded a great of enthusiasm

The creative platform on which this epiphany was based:

- People have phones
- Data can be transferred wirelessly
- People don't like carrying things
- We already have sensitive data on phones
- Third parties will automatically adopt it as it's easier

Estimated Effort (Worst-Case): 3 months

Governments had some concerns - they needed a proving-ground

There are Privacy concerns

- LINDUNN analysis reveals agencies could tell a Roadside Stop vs Age Verification

Where was the data retained?

- Governments need to be the system-of-record

Could Government do this?

- Legislation needed to be developed to both allow operation and guide product compliance

Our customer was willing to work through this on a trial-basis

- First general-use MDL POC delivered by CBN
- Responsive web app on Android tablets
- ~5,000 public users across multiple sites
- Convenience stores, breweries, law enforcement
- Ran several months → ended early 2017

Customer Requirements Have Significant Security Impact

Pilot Step #1: Surveyed stakeholders with their top concerns

Ended up with key requirements:

- No PII on devices
- Prohibit Screenshots of App
- Consent required for information release
- Protect confidentiality & integrity of transmitted data
- ID can't be copied

Big Questions

Should the mDL work in both online & offline modes?

- Offline requires data on the device which can be exfiltrated

One device or two device system?

- Securely display of ID is difficult in one-device system due to spoofing and (App) re-origination

What data are we sending to the verifier?

- User must authorize profile creation
- Age verification: Over 18+/21+
- Road-side Stop

How long to retain information on device and verifier?

- Closed Program: DMV controlled pilot verifiers using MDM
- We generated a barcode with OTP and limited lifespan
- Verifier App held data (an image) for 30s.
- Rendered data into an image

OAuth was supposed to solve our problems. Instead, we broke a law of software security – we rolled our own auth.

Securely bootstrap in the event of a man-in-the-middle

- Due to issues with Server-Side TLS and STS there is no secure bootstrap.
- Email as shared-secret to securely transfer device token.

Protect a brute-force attack against a 4-digit PIN

- Device had Public/Private Keypair – Public was stored only on server-side
- Instead of classic Salt|Hash in password database, we only stored Public Key
- Stored Private Key encrypted by Hash(PIN)
  - Brute forcing PIN only yields indistinguishable random keys
  - Server needs to be involved

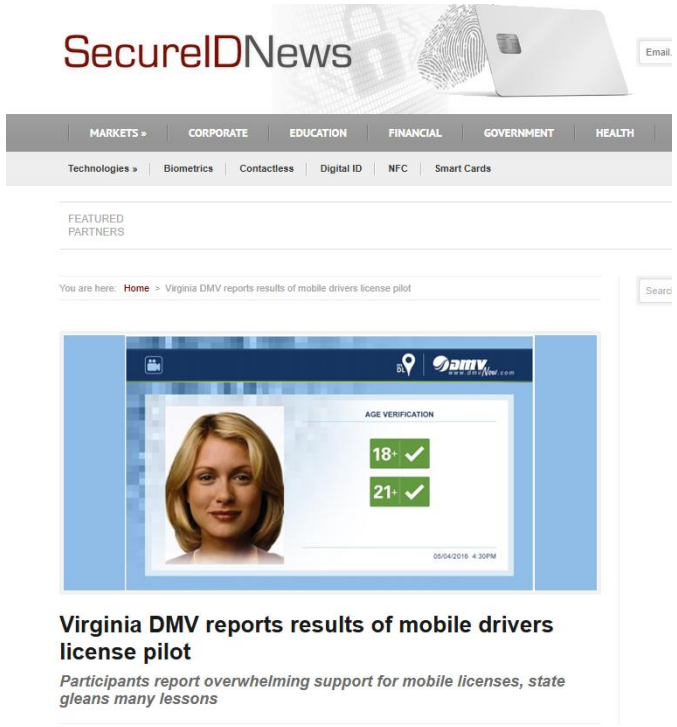
Mobile DL credentials cannot be copied

- After successful authentication, device token was XORed with last challenge
- If local storage is copied, the first authentication will then "break" the original users' device. Only one device will ever have access to the information.
- A very technical solution to a high-level customer security objective!

Final Result: Many Lessons Learned, tons of momentum

Decision	Security Control	Lessons Learned
Prevent Reuse Fraud	**One Time Barcodes**	**One-Time Codes work great for security but are a nightmare for support** • **Largest number of calls were due to expired OTPs**
Maintain data integrity of users	**Tight control over PII endpoints**	Personal Data could be harvested by untrusted verifiers • **Verifiers controlled by DMV via MDM** Cameras on web browsers can be co-opted • **Controlled pilot let us restrict mDL to pre-enrolled users via DMV website**
Prevent data harvesting	**Rate limiting / Auditing**	Rate limiting needs to be monitored and tuned • **We locked support out during a SEV 1 due to limits**
Security Assurance	**Pen Test using OWASP WSTG**	Leveraging Certs Helps Adoption • **Hosted from ISO environment w/ ISO Personnel**

mDL Pilot Created Momentum and Demand – but Security, Interoperability and Markets Evolved for Production Rollout



Government Security Requirements Matured Rapidly

- **Self Assessed Frameworks**
  - BSIMM
  - NIST CSF
  - OWASP Top 10 / WSTG

→

- **Audited Standards**
  - ISO
  - SOC 2
  - NIST 800-53

Interoperability

- **SC 17/WG 10 began creating ISO 18013-5 to standardize**
- **Examined other implementations**
  - **Credit Cards (PCI)**
  - **ePassport (ICAO 9303)**
- **3rd Party Verifiers**

Market Changes

- **No longer Standalone Product**
  - Part of larger ecosystem
- **Move to Fully Vendor Hosted**
  - From Customer Supported to Vendor Managed (requires auditing)
  - Enrollment became part of product
- **SSI (and W3C VC) mainstreamed**

Standardizing: Why this matters

1. Other groups will take an interest in this space due to the pilot
2. When other groups make mistakes, it can impact you
3. More scope = more work → Communicate, don't just put your head down

The Barcode Contents and Data Transmission Changed from Pilot to Rollout – now anyone can verify

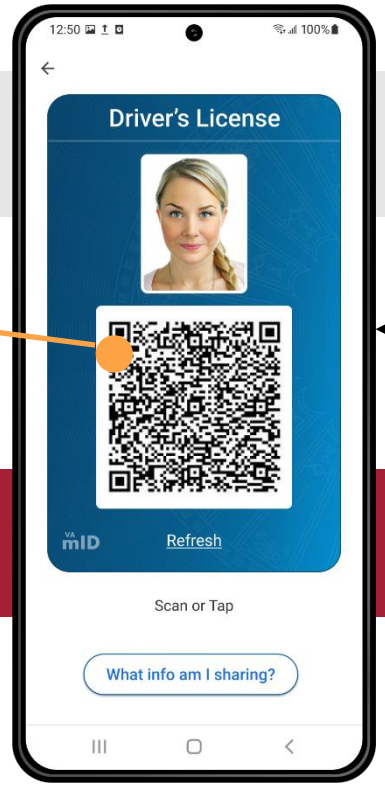
Pilot

Barcode had Retrieval URL

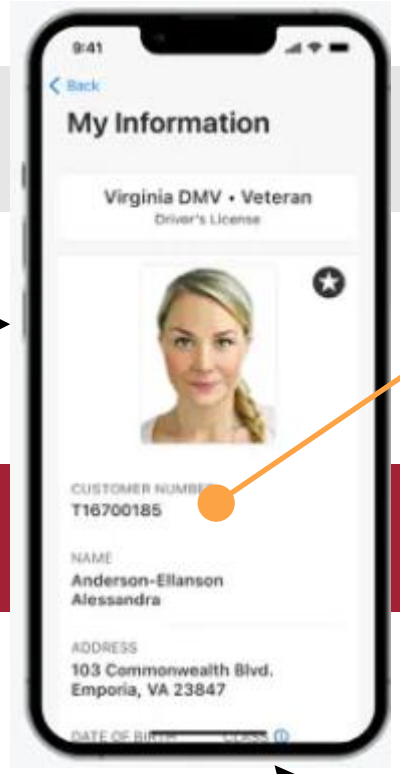
Rollout

BLE/NFC/Wifi Engagement

Device Key Attestation



ECDH + AEAD



Data Contents
Relied on Controlled mTLS
MDM System for Tablets

Request Attributes
Mobile Security Object
Device Auth

PKI Validation

AAMVA

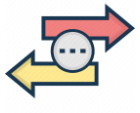
mDL DTS
MOBILE DRIVER'S LICENSE DIGITAL TRUST SERVICE

Standards work increased interoperability – but also demonstrated large supporting requirements for Rollout

Included in Standards…

- Privacy Mechanisms
- Protocol Security

- Interoperability
- Provisioning



- Presentation
- Transmission

- Verification
- Validity Management

… but defining a program requires

- Accessibility
- Usability

- Auditing
- Data Policy

- Governance
- Entitlement

- Key Management
- Certificate Policy

- Support
- Communications

- Lifecycle
- Updates

- Use Cases
- Relying Parties

- Government Wallet
- OEM Wallets

Enrollment became part of the offering

- Initial version used pre-vetted web portal to ensure authenticity
  - Now we needed to handle users with no pre-existing relationship

- New version involved scanning the PDF417, performing FR, and issuing a credential
  - PDF417 on back of card contains a digital signature of the barcode information.

- Too easy to spoof a camera in web apps especially when FR vendors had already figured out liveness detection
  - **Edge detection** improved for masking
  - Native apps could **bolt camera selection** to known devices
  - **Root / Jailbreak detection APIs** became trustworthy
  - **Signed packages** generated for server with nonces, several images

We could now verify an attested app on a non-tampered device captured this within seconds using a built-in camera with liveness signals

We thought SSI would provide built-in 3rd Party Verifiers. Learning: 3rd Party Verifiers that validate incorrectly kill trust.

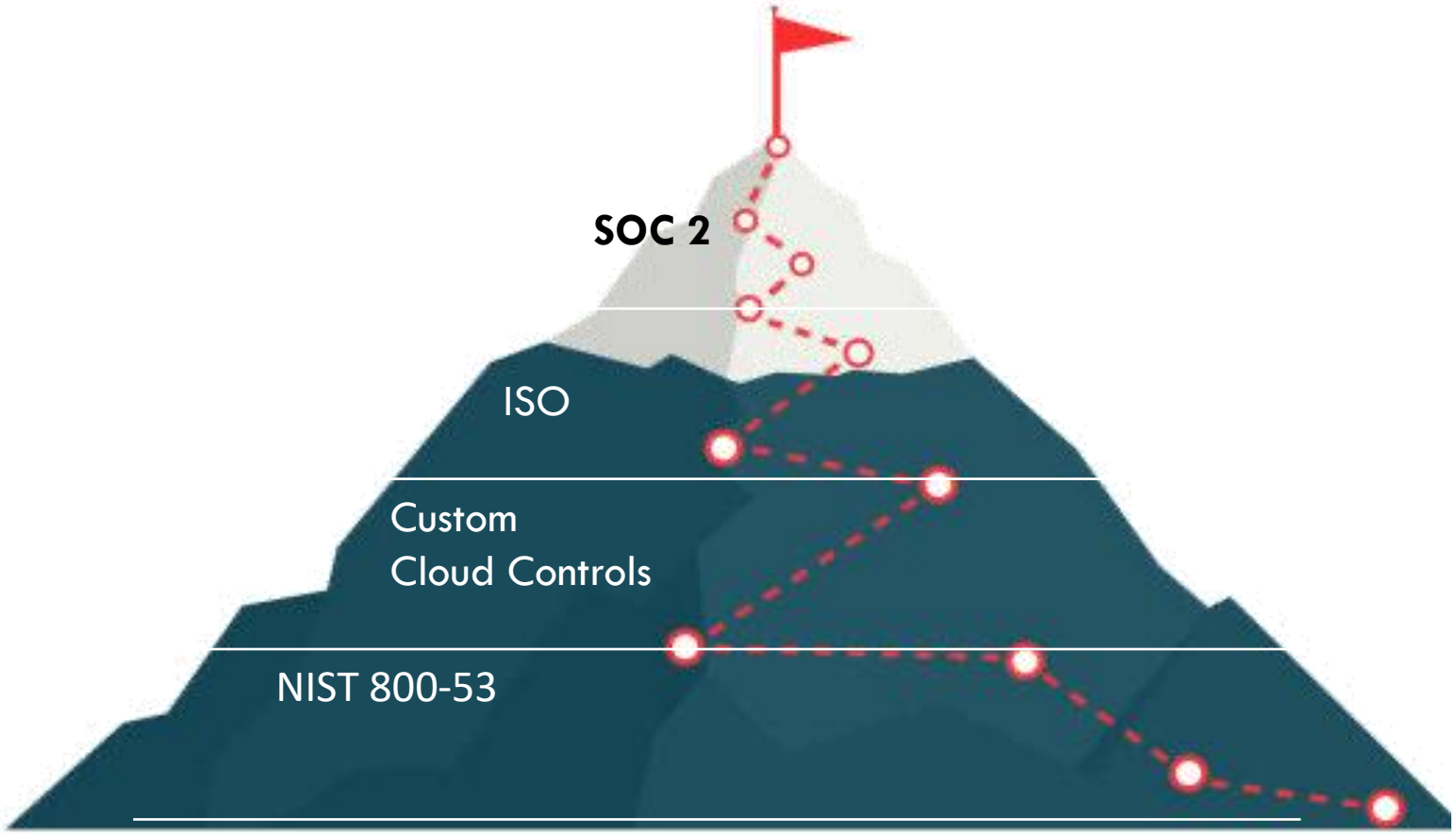
- This is where SSI and 3rd party Verifiers let us down

- For SSI, we looked at implementing Sovrin
  - Governments are not fans of relying on components they can't control - Sovrin went under in 2025
  - Availability vs Permanence – if you encode data elements they can't be changed, if you store pointers, your database better be operational.

- Sovrin has many 3rd party verifiers
  - Uptake has been low as verifiers must be vetted
  - BC Government used this but designed their own verifiers
  - It's challenging when self-asserted information is mixed with government asserted

- The issue with 3rd party verifiers is – it's still your fault.
  These issues made the paper due to bad certificate checks:
  - Covid cert
  - Elvis Attack

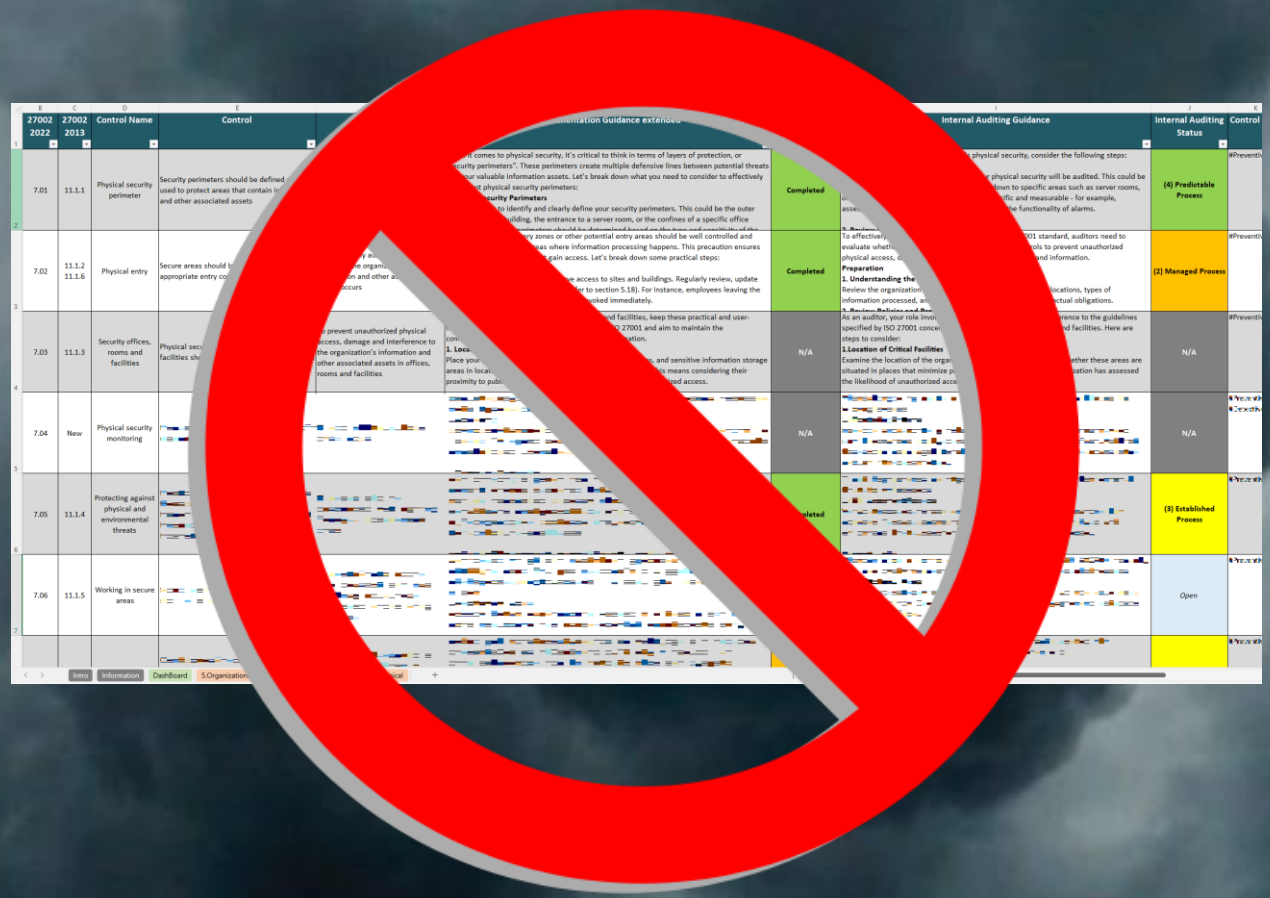
We also had to Summit Mount Compliance, Height: 1583 controls. The Storm Clouds began to blow.



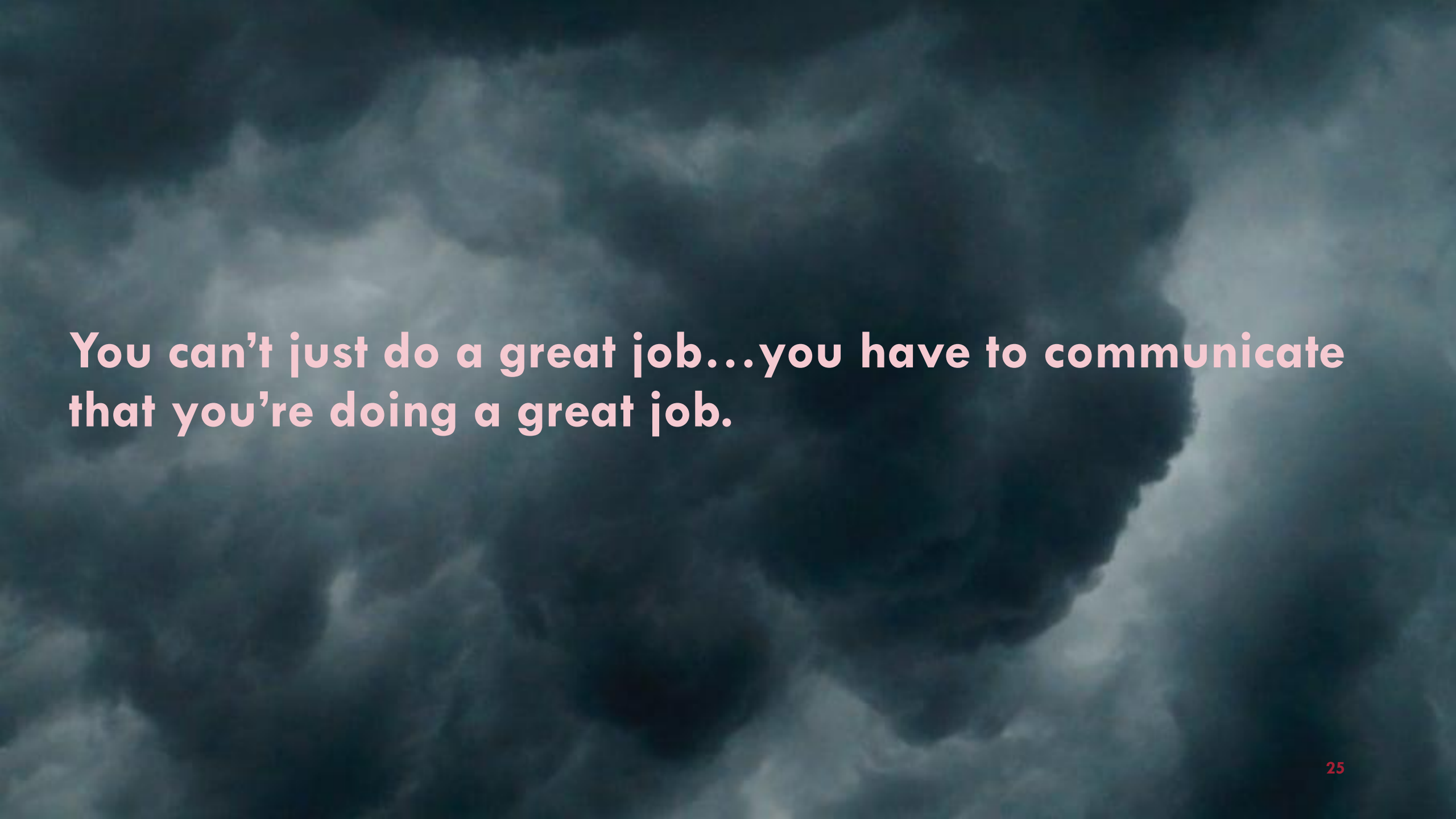
The Compliance Journey

1. Define the scope
2. Map to the frameworks
3. Itemize the controls
4. Assess the gaps
5. Assign owners
6. Implement
7. Internal Audit
8. External Audit

Mistake #1: Using Excel – OR – not using a GRC Tool



Mistake #2: We put our heads down and started working – OR – We Stopped Communicating


You can’t just do a great job…you have to communicate that you’re doing a great job.

We launched three efforts: Scorecards for Updates, Plan for Compliance, Pipelines to Help Implementation

Scorecarding

- Risk Appetite
- Business Objectives
- Evolve 1 pager

Compliance Work

- Scope
- Plan
- ISO
- SOC2

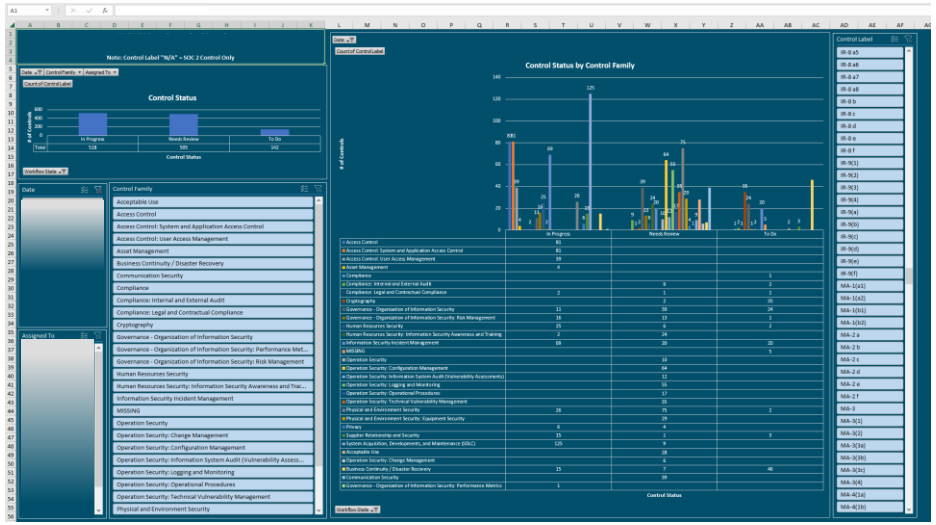
Pipeline Enhancements

- Enforce Audit Rules
- Increases feedback
- Centralize security checks early
- Provide agility for new requirements

These operational tracks start during Standardize and run through Certify.
They're the machinery under the hood.

Status Updates Were Needed – Dashboards to the Rescue!

- We started with a dashboard of the number of controls we have addressed
- Some of these however had implementation items attached, so we then added implementation coverage (Hardening/Logging/etc)
- Then we had Vulnerability Coverage
- Then we had pen test results



Scorecards should be more

- Key questions asked:
  - Are there attacks?
  - Are we doing enough compared to others?
  - Are we making progress?
- **Don't overwhelm with problems. Goal is to leave two impressions:**
  - **You know what you're doing**
  - **The organization is in good hands**
- Pair visuals with **narratives and scenarios** to make risks feel real (e.g., revenue loss during peak failure).
  - Fear, uncertainty and doubt may work short-term. Focus on confidence and trust – not raw metrics
- **Every message should tie back to business objectives and risk appetite**
- **Build trust as a confident advisor**

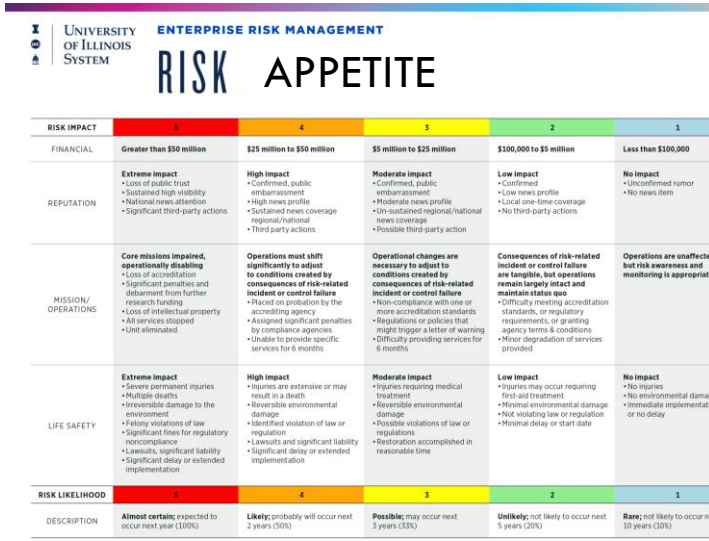
Building a Risk Scorecard Framework

Step #1: Risk appetite

- Start with **"doomsday scenarios"** from each business unit to define real concerns.
- Categorize risks to match risk appetite: Important for language
- Layer heat maps and scorecards for a multi-audience view; include narratives and scoring.

Step #2: What are the key objectives?

- **Establish Control Set:** NIST 800-53 + SOC2 + ISO Controls
- **Implement Security Controls:** Hardening, SIEMs, IAM, Scanners
- **Test security controls:** Threat Modelling, Penetration Tests, Vulnerability Scanning
- **Demonstrate Compliance:** Evidence for the designated controls



University of Illinois System

ENTERPRISE RISK MANAGEMENT

RISK APPETITE

RISK IMPACT	5	4	3	2	1
FINANCIAL	**Greater than $50 million**	**$25 million to $50 million**	**$5 million to $25 million**	**$100,000 to $5 million**	**Less than $100,000**
REPUTATION	**Extreme impact** • Loss of public trust • Sustained high visibility • National news attention • Significant third-party actions	**High impact** • Confirmed, public embarrassment • High news profile • Sustained news coverage regional/national • Third party actions	**Moderate impact** • Confirmed, public embarrassment • Moderate news profile • Un-sustained regional/national news coverage • Possible third-party action	**Low impact** • Confirmed • Low news profile • Local one-time coverage • No third-party actions	**No impact** • Unconfirmed rumor • No news item
MISSION/ OPERATIONS	**Core missions impaired, operationally disabling** • Loss of accreditation • Significant penalties and debarment from further research funding • Loss of intellectual property • All services stopped • Unit eliminated	**Operations must shift significantly to adjust to conditions created by consequences of risk-related incident or control failure** • Placed on probation by the accrediting agency • Assigned significant penalties by compliance agencies • Unable to provide specific services for 6 months	**Operational changes are necessary to adjust to conditions created by consequences of risk-related incident or control failure** • Non-compliance with one or more accreditation standards • Regulations or policies that might trigger a letter of warning • Difficulty providing services for 6 months	**Consequences of risk-related incident or control failure are tangible, but operations remain largely intact and maintain status quo** • Difficulty meeting accreditation standards, or regulatory requirements, or granting agency terms & conditions • Minor degradation of services provided	**Operations are unaffecte but risk awareness and monitoring is appropriat**
LIFE SAFETY	**Extreme impact** • Severe permanent injuries • Multiple deaths • Irreversible damage to the environment • Felony violations of law • Significant fines for regulatory noncompliance • Lawsuits, significant liability • Significant delay or extended implementation	**High impact** • Injuries are extensive or may result in a death • Reversible environmental damage • Identified violation of law or regulation • Lawsuits and significant liability • Significant delay or extended implementation	**Moderate impact** • Injuries requiring medical treatment • Reversible environmental damage • Possible violations of law or regulations • Restoration accomplished in reasonable time	**Low impact** • Injuries may occur requiring first-aid treatment • Minimal environmental damage • Not violating law or regulation • Minimal delay or start date	**No impact** • No injuries • No environmental dama • Immediate implementat or no delay
RISK LIKELIHOOD	**5**	**4**	**3**	**2**	**1**
DESCRIPTION	**Almost certain;** expected to occur next year (100%)	**Likely;** probably will occur next 2 years (50%)	**Possible;** may occur next 3 years (33%)	**Unlikely;** not likely to occur next 5 years (20%)	**Rare;** not likely to occur n 10 years (10%)

Scorecard

Obviously Sanitized

Business Objectives	Risk / Category	Cause / Source	Current Status / Metric	Risk	Trend	Status
Preventing Data Leakage	Security Feature Implementation	Delay in rollout, resource constraints	70% implemented across apps	Low	↗ Increasing	In progress
Preventing Data Leakage	Risk Register Issues	Unpatched systems, weak patch mgmt.	32 open	Medium	↘ Improving	Key Issues Need Actioning
Third Party Verification	Pen Test Vulnerabilities	Insecure coding / config issues	2 critical unresolved	High	↗ Stable	Under remediation
Acceptance	NIST 800-53 Controls Triaged	Privacy Controls, rev5 SR Mapping	95% evidence collected	Low	↘ Improving	In Progress
Acceptance	Evidence Collection for NIST 800-53 Controls	Missing documentation, control gaps	30% evidence collected	Medium	↘ Improving	Awaiting Resources

Priority	Topic	Scenario	Operational Issue	Compliance	Customer Impact	Action
High	**Pen Test Vulnerabilities**	If these 2 critical vulnerabilities are exploited during Q4 peak usage we could face outages	Potential loss from 4-hour service outage	Potential SOC2 audit findings	Disclosure to 3rd party verifiers	Dev Team allocated, patches expected within month
Medium	**Evidence Collection Gap**	30% evidence collection puts us at risk missing customer and compliance targets		Potental SOC2 audit findings	2 verifiers expecting compliance proof	Dedicated compliance resourced onboarded to mitigate

- Started with the Doomsday Scenarios and mapped to “Business Objectives”
- Metrics go through phases: **Coverage, Detection, Exceptions** and **Response** (and sometimes **Value**)

- Bad scorecard styles:
  - CVSS counts/sheets shouldn’t be the only item. Vulnerability discussions can rabbit-hole.
  - General risk register items – the list is too long and it’s hard to show progress

Scorecard

- Show positives and progress, not just risks and issues
- Forward Guidance is usually unexpected from a “First Responder” style group
- Think Trends, Impact and Risk Posture
- Bad scorecard styles:
  - Charts on raw numbers with no context: “We had 5432 alerts!”
  - Lack of Targets & Tolerances: where are you going?

Obviously Sanitized

Confidence Indicators

✅ **What's Working:**

Vulnerability management improved 40% over last quarter
Zero security incidents in 90 days
Ahead of compliance timeline by 3 weeks

🎯 **Strategic Wins:**

Prevented potential $800K breach through early threat detection
Completed SOC2 prep 2 months ahead of schedule
Security training completion: 94% (vs 67% industry avg)

Forward Guidance

Prediction: With current trajectory, we'll achieve "Green" status on 4 of 5 objectives by Q4, well ahead of regulatory requirements.

Investment Recommendation: Additional $150K for automated security tooling will accelerate evidence collection and put us at peer leader levels

Certify: Why this matters

1. Understand the reasons behind certification asks.
   - Customers wanted to demonstrate trust to others repeatedly
   - They were really smart to ask for this as TSA eventually required it.

2. Ask Security; it makes you **way** better.
   - We had to adjust how we worked. This meant pipeline changes.

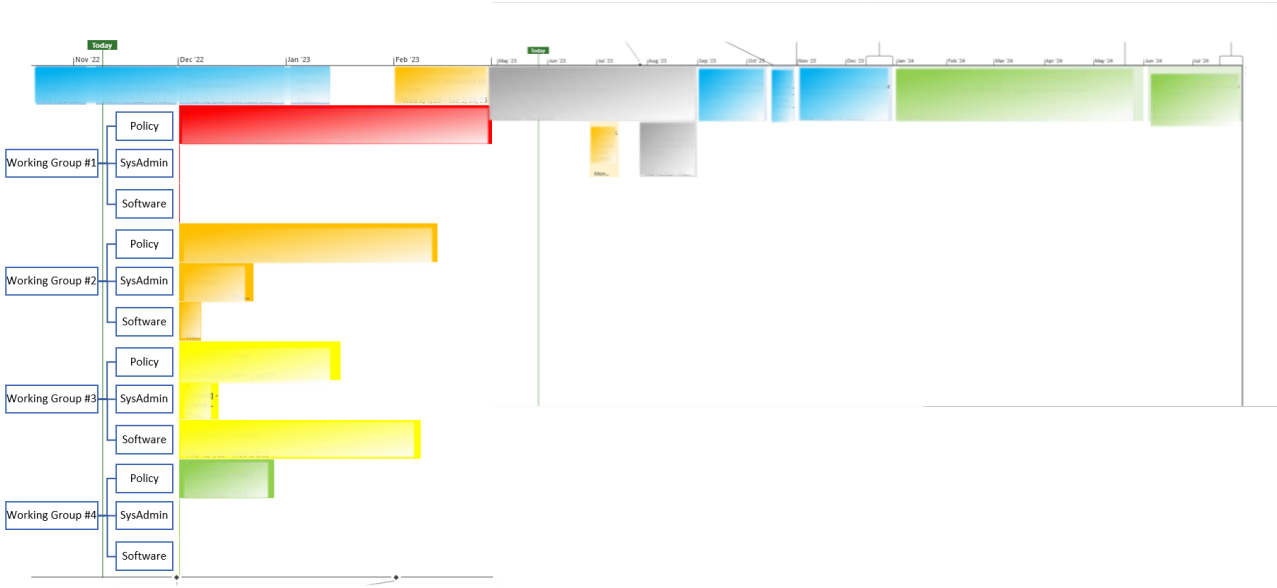
3. It's an advantage, but you must leverage it.

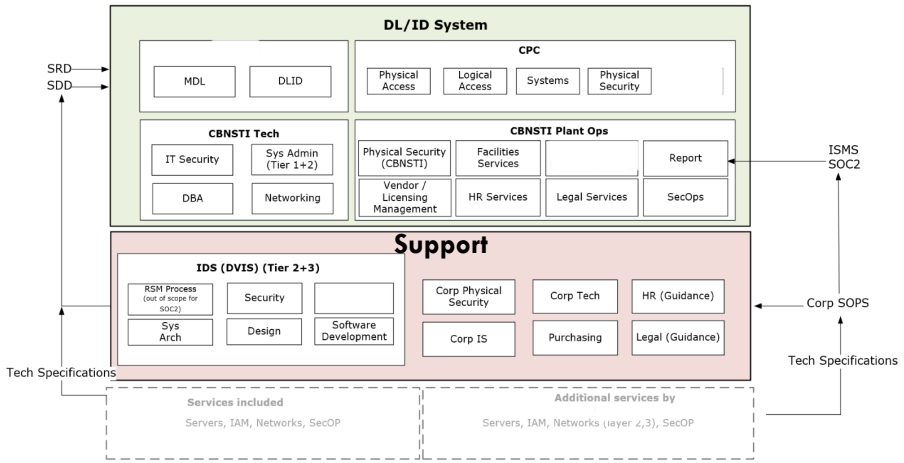
Compliance struggles to be agile
Before anything: Define a Scope & Plan

It's hard to avoid trying to wrap your arms around every framework and every control.

Scope: Helps us limit who's involved and the blast-radius of changes.
Plan: Allows us to know where to direct issues to

Trying to start before you have these two items caused us several restarts.





What is the ISO process?

Statement of Applicability (SoA)

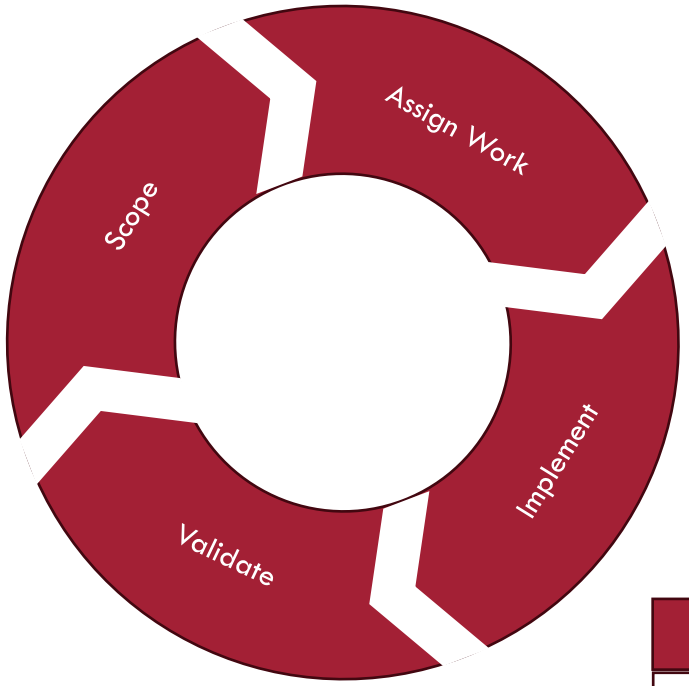
- Map each Annex A control (93 in the 2022 version, 114 in 2013).
- State whether each control is:
  - **Applicable** → then you must implement it.
  - **Not applicable** → explain why.

Governance

- Appoint an **ISMS owner/committee.**
- Approve an **Information Security Policy** (top-level statement of intent).
- Show **management commitment** (resources, budget, review).

Define Scope and Context

- **Decide what's in scope**
- Identify **stakeholders** (customers, regulators, internal teams).
- Define **ISMS boundaries.**



Risk Management

- **Identify assets, threats, and vulnerabilities.**
- Carry out a **risk assessment** (choose a method—qualitative or quantitative).
- Decide how to **treat risks** (avoid, mitigate with controls, transfer, or accept).
- Maintain a **risk treatment plan**

Validate & Update

You don't need *every* Annex A control, only what's relevant—but the auditors expect at least:

- Information Security Policy
- Risk Assessment & Risk Treatment results
- Statement of Applicability
- ISMS Scope Document
- Evidence of training & awareness

Implement Core Controls

Access control (user accounts, least privilege)
Asset management (inventory, ownership)
Cryptography (password hashing, data protection)
Operations security (patching, backups, logging)
Supplier security (vendor risk management)
Incident management process
Business continuity / disaster recovery basics
Physical security (office, datacenter, devices

ISO Hints and Tricks

Hint #1: Start small and work outwards. Share the plan with the auditor.

- Scope and SoA you need to get right. Work iteratively as much as possible.
- If things aren't done, share this upfront

Hint #2: Don't do everything at once. Start with a core environment and add systems iteratively

- You can make systems external if a system "reaches out" and sanitizes from a "DMZ"
- ISO is Management of Controls: a contractual SLA can be enough for ISO.

Hint #3: Internal Audits are not a Report Card – they provide forward guidance

- Run at least **one internal audit** of your ISMS.
- Conduct a **management review** (meeting minutes count).
- Any issues (audit nonconformities, incidents), log them and track remediation via committee.
- If it's in your risk register, "you're working on it"

Hint #4: Schedule your audit early and talk to the auditor

What is the SOC2 process?

Define Scope and Context

System boundaries: Identify in-scope services, identify subservice providers and carve-outs.

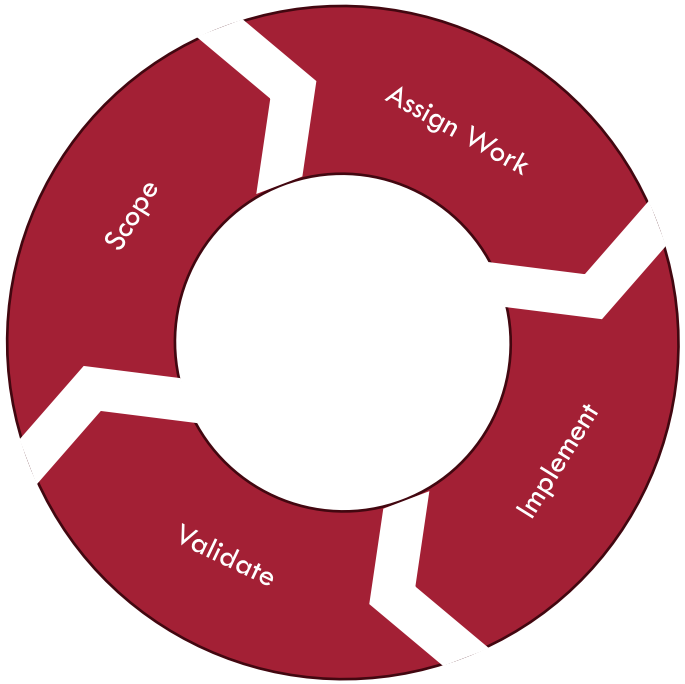
- Define Scoped Data and identify data handlers
- DFDs show system components
- Organization Responsibility Map shows personnel / carve-outs

Trust Services Categories (TSC): Which trust principles do you need **now**? Security is required - Availability, Confidentiality, Integrity and Privacy are add-ons.

Build the SOC 2 control matrix

Map Controls to Criteria: Use crosswalks to align operational controls with **COSO principles** and **Trust Services Criteria (TSC)**. Assign clear control owners and define sample evidence for each control.

Document CUECs : Record the **Complementary User Entity Controls** expected of customers, and identify any vendors that fulfill these responsibilities on your behalf.



Develop Documentation

Run Workshops: Use swimlanes for key SOPs (eg: Access Control, Vulnerability Management). Document the process, RACI and evidence

System Description: Start writing your System Description and update each cycle

Implement Controls

If you already have ISO, new controls include:

- Monitoring/alerting evidence
  - MFA/logging/alerts
  - Change approval records (tickets/PRs)
  - DR/backup test results
  - Data classification matrix + encryption configs
- Employee lifecycle (background checks, NDAs, offboarding)

Validate & Update

Ticketing System is the heart of retention: This provides coverage of all activities. Annual Reviews have tickets. Access Control flows have tickets

Readiness Assessment: Do a dry-run test of design & evidence with an auditor. There will be critical findings and the evidence can often be reused to shorten Type 1 audit time.

External audit: Do a Type 1, and then a Type 2. Type 1 gives you temporary coverage and preps for the Type2.

Continuous monitoring: Perform ongoing monthly checks of tickets and key checks such as vendors

Availability

- Capacity monitoring
- DR test evidence
- Uptime monitoring
- SLA Evidence

Confidentiality

- Documented data classification scheme
- Key management
- Data disposal procedures

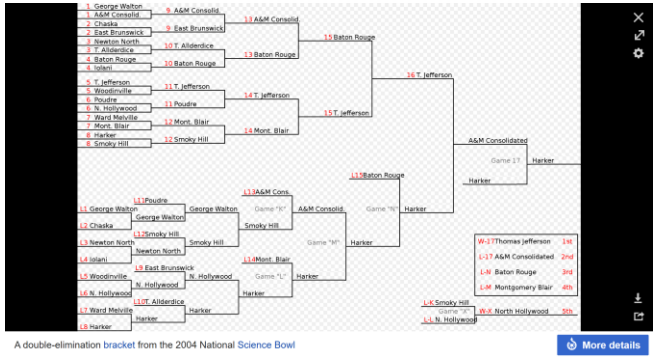
Integrity

- QA/Testing Evidence
- Error Handling Logs
- Process Monitoring

Privacy

- DPIA
- Privacy Policy
- Consent Capture
- Rights Requests (SARs/DSRs)
- Retention Enforcement
- Disclosure Tracking

SOC2 Hints and Tricks



Hint #1: Think of Readiness Assessments and Type 1 as a tournament

- It improves findings and provides interim assurance
- Teams get faster at evidence gathering - through reuse or examples

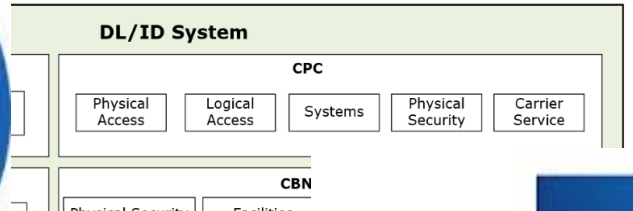
Hint #2: Communicate with everyone: Perfection is not the goal

- Make sure stakeholders (and customers!) know the goal is “reality on the ground”
- Any findings should be presented beforehand and immediately disclosed when found.
- Disclosures and plans that are approved by Steering Committees often reduce severity
- **Make sure you understand why customers need compliance**

Hint #3: Soak Time

- Put time in your plan for the system and processes to solidify
- Tightly monitor during the soak period and update stakeholders

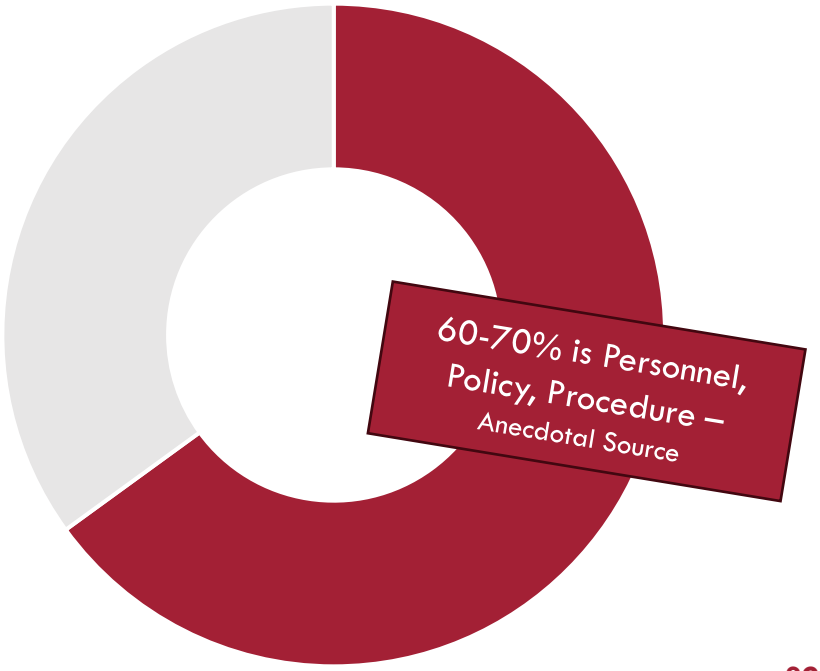
Compliance in Numbers



- 10 groups – 150 people
- 3 Plants
- 2 Data Centers + Azure
- 200 Servers
- 290,000 LoC

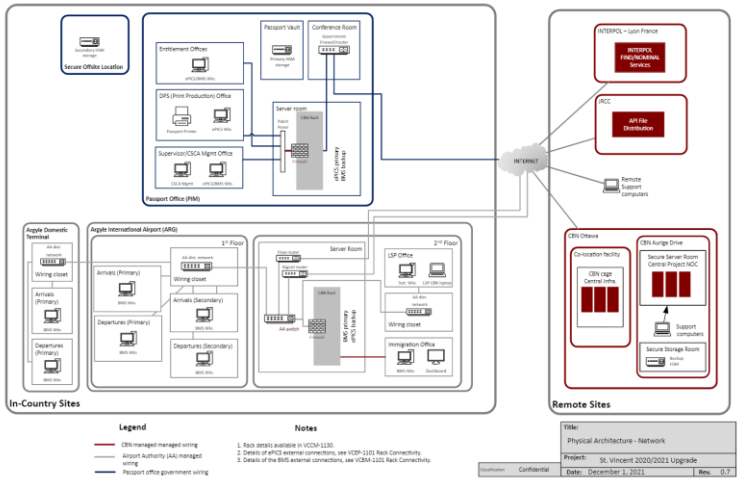
Learnings - #1: Technical Controls are the small part

Policies/SOPs/People are the lions share of the effort.
Technical tooling ≠ compliance.

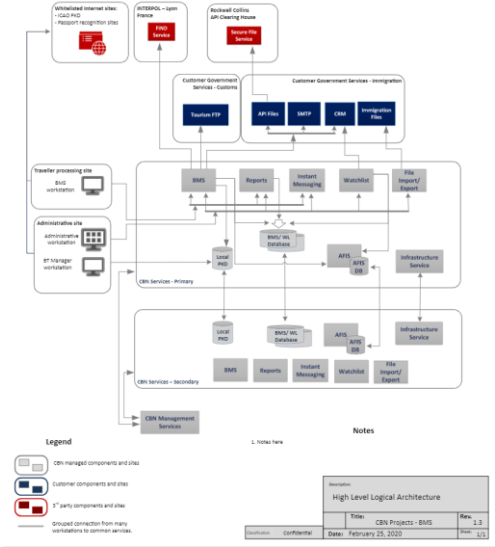


#2: Diagrams and Documentation are Critical

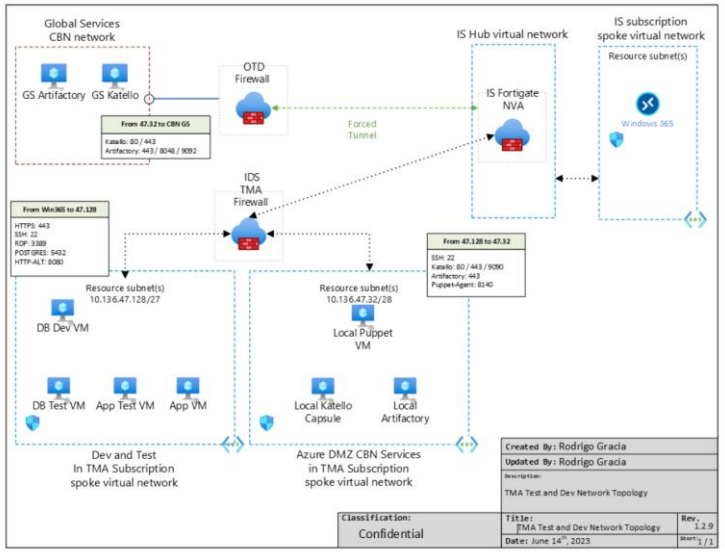
Scope and features are dependent on the design.
Can't be in someone's head – needs to be discussed.



- Physical Diagram
  - Shows locations of datacenters, plants and front offices
  - Where is the data stored / processed?
  - Are there external dependencies?



- Software Architecture Diagram
  - Shows the services, APIs and data flows
  - What data is sent/where?
  - What data is stored?



- Logical "Network" Architecture Diagram
  - Shows the devices, data flows, subnets and ports.
  - What services are available?
  - What ports/protocols are used?

#3: More Standardization, More Reuse

mDL and existing system had standard infrastructure

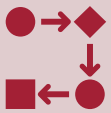
Same operational team for both

Same policies/SOPs across systems

#4: Push controls to platform (and vendors!)

- Vendors who have certifications are preferred as they simplify the process. Push carve-outs to them.
- Cloud platforms have already done the certification for their products. We don't want to reimplement.
- Unicorn vendors can sometimes be descoped with a risk assessment – especially if not involved in operations. Always have a certified backup.

#5: There's always a new standard. Choose one, align and gap.



As new specifications emerge we need an internal reference point and then gap.

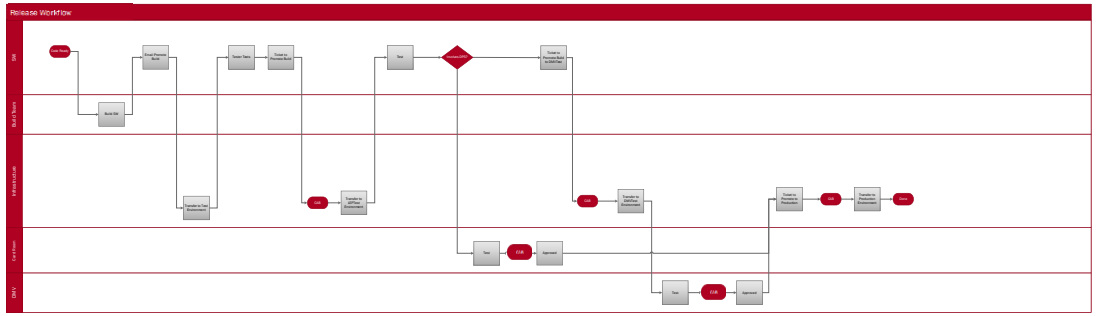
A common frame of reference helps minimize work.

Leveraging ISO worked to move work through our groups as teams were familiar with it.

#6: Long release times means large upfront planning

- "Release" doesn't mean more product.
  - For Software this is a set of features in a build.
  - For Infrastructure this is any adjustment to the environment.

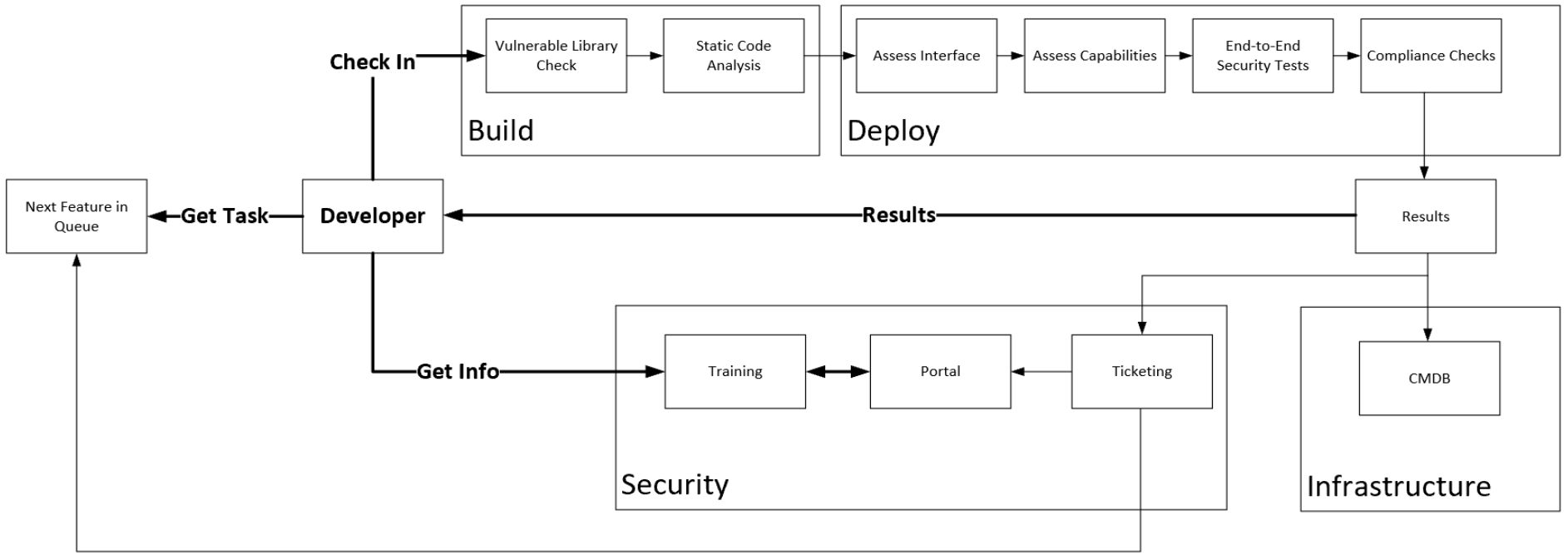
- Long release times are built on: Avoiding Bugs (QA), Avoiding Outages (CAB Approval) and Manual Processes (Transfer).



Pipeline for Certifications: Why this matters

1. Pipelines give early results – “big bang compliance” at the end leads to findings
2. These are often “quick wins”. Adjustments to the pipeline give tangible results
3. Consistency: findings in an audit can be offset with compensating controls. This gives enhanced traceability

Iterative Compliance Means New Requirements Daily - This meant a new Release Process



Success: a developer checked in code, SAST flagged a bug, it got ticketed, they read it from JIRA, fixed it, checked it in and it closed. **Without. Security. Involvement.**

Workflow

- Clone repo / checkout branch (GitHub access controls enforced)
- Make change in code or infrastructure-as-code (e.g., Puppet)
- Submit Pull Request (PR) with description, risk assessment, and checklist
- Automated scans run (linting, Snyk, config validation)
- Testing in testlab → regression, functional, TLS/cipher checks
- Promotion to production after approvals

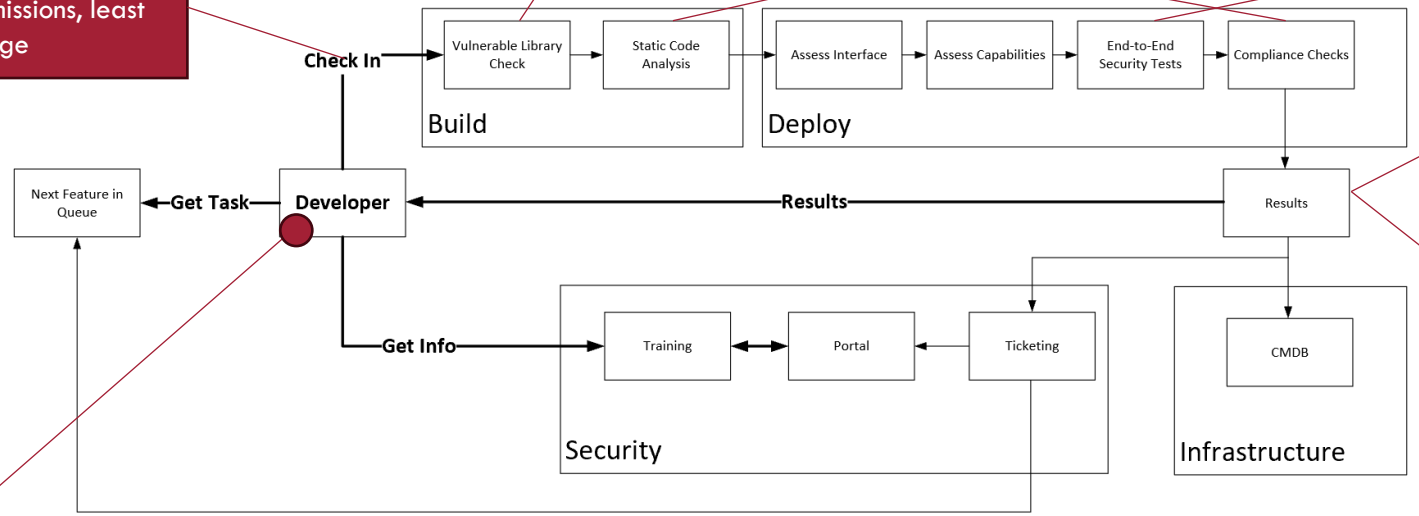
Developer Workflow Under ISO 27001

Development & Support Security (A.8.25) – scans, code review

Data Protection (A.8.10) – secrets management, no sensitive data in code

Secure Engineering (A.8.28) – enforce cryptographic standards (TLS 1.3)

Access Control (A.5) – GitHub role-based permissions, least privilege



Change Management (A.5.23) – PR reviews, approvals, audit trail

Audit & Accountability (A.5.10) – PR history, logs, traceability

PR Description

Clear description: what, why, impact
Risk assessment: risks, likelihood, impact, mitigations, residual risk
PII Impact Checkbox: Yes / No
Testing & validation evidence
Compliance checklist: ISO controls, policies, ticket links
Approvals: Dev lead + Security team

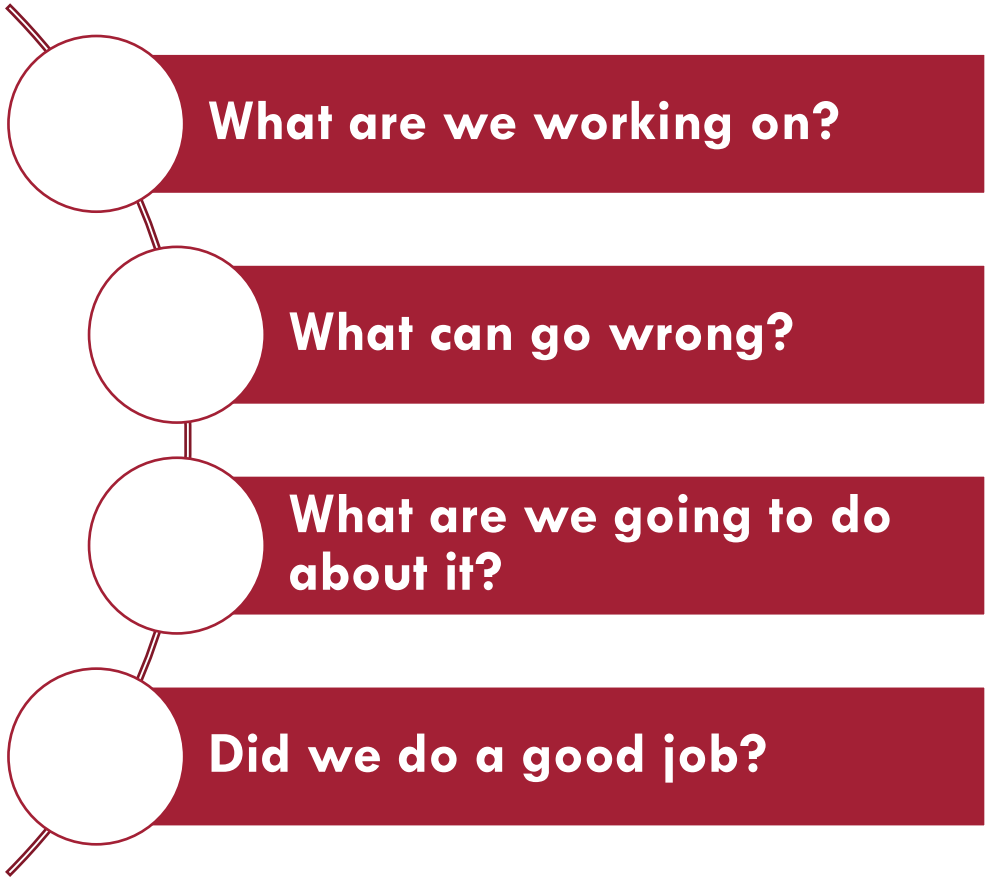
Security Team Role

Review flagged PRs (risk/PII checkbox = Yes)
Validate risk assessments are complete and mitigations sufficient
Cross-check compliance with privacy principles (data minimization, lawful processing, secure handling)
Approve or request revisions before merge

Risk and Testing Practices

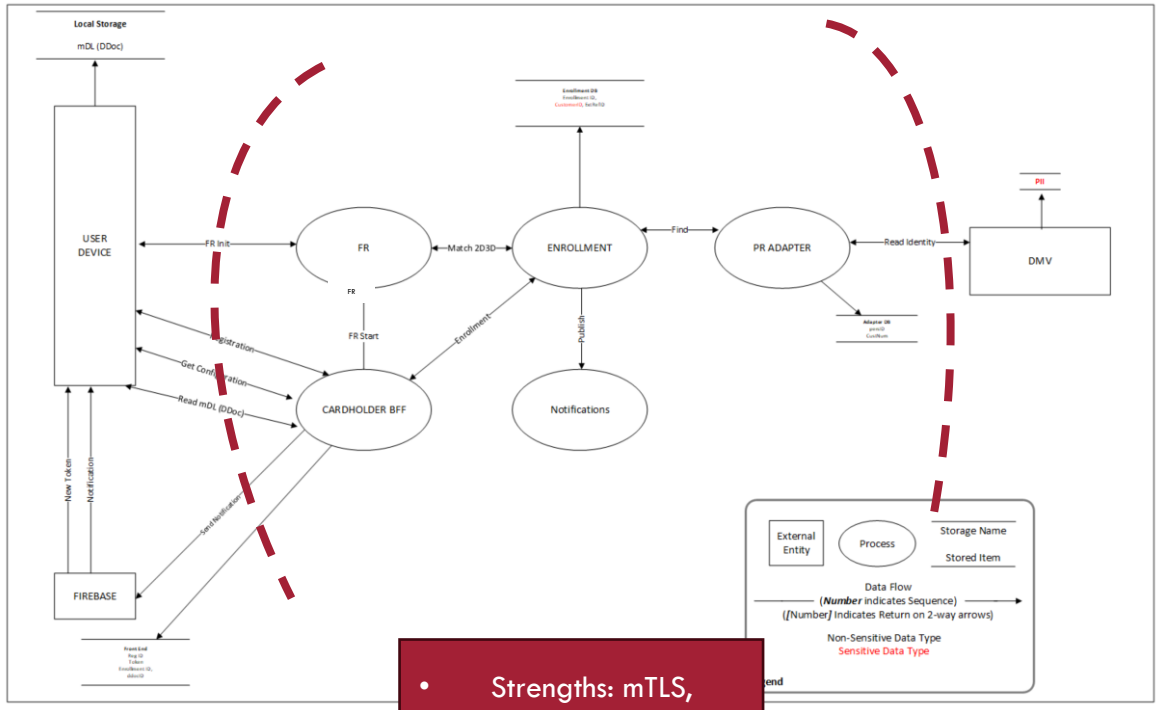
Automated Scans: SAST, SCA, DAST
Testlab Validation: TLS enforcement, client compatibility checks
Periodic Pen Testing: Quarterly manual review
Monitoring & Alerts: Vulnerabilities trigger alerts in Ticketing
Residual Risk Sign-off: Documented and accepted

How to handle Architectural Risks? Threat Modelling is about answering 4 questions



- **Threat Modelling is answering these 4 questions**
  - 3 sessions / 2hr each - 2 weeks calendar time
  - Don't go too deep. Looking at the trust boundaries is often enough.
  - You'll miss things. That's ok. It's iterative just add them.
- **Lots of methods (STRIDE, PASTA, OCTIVE) – just pick one and start.**
- **Add issues to a central list with an approximate risk.**
  - Mitigations should be listed
- **Review with the team! -** Risk Assessments are highly variable - this is a great artifact to demonstrate due diligence
  - ✓ DFD with trust boundaries
  - ✓ Threat List – ideally mapped to STRIDE or another framework
  - ✓ Strengths and Weaknesses
  - ✓ Mitigations & prioritized risks

Scope the system – start with Architecture Diagrams



- Strengths: mTLS, MFA, logging, WAF
- Weaknesses: DDoS has cleartext, Data Retention

1. Define the system
   - Show Actors, Processes, Data Stores and Flows
2. Identify Trust Boundaries – where trust levels change
   - Transitions are “Hot spots” for threats
3. Document the strengths and weaknesses for each trust boundary
4. Security can overlay Compliance
   - LINDDUN application found shared IDs over backend connection

Leverage: Why this matters

1. All the work to this point comes together here
2. 3rd parties depend on security certifications *and how they connect to their requirements*
3. Having a package ready-to-go with evidence and compliance matrix helps customers

Being Trusted by Relying Parties
TSA Approval took bringing all this work Together

TSA announces final rule that enables the continued acceptance of mobile driver's licenses at airport security checkpoints and federal buildings

Rule allows for continued use of mobile driver's licenses for identity verification in support of REAL ID enforcement, which starts on May 7, 2025
National Press Release
Thursday, October 24, 2024

TSA developed a set of requirements based on NIST, IETF, ISO and agency specifications.

- We were involved in initial consultations and provided feedback on requirements

Everything we talked about was needed

- Modelling was used to describe solution
- Pipeline provided data and assurance
- Certifications were key to acceptance

Additional components used were Scanning from Pipeline, Threat Modelling and Assessment Data.

SOC2 demonstrates controls meet Operational Security

TSA requirements can be mostly mapped to NIST 800-53. Evidence can be reused and submitted.

ISO provides the first set of checks and buys time for the pilot.

Compliance is Looking Like Data Engineering: One Clean, Continuously Validated Control Layer → Mapped Repeatedly

Core Control Set

NIST 800-53

ISO 27001

Continuous Compliance

GRC On-Demand Tooling

Pipeline Analytics

Evidence Gathering

Packaging

SOC2 Reports

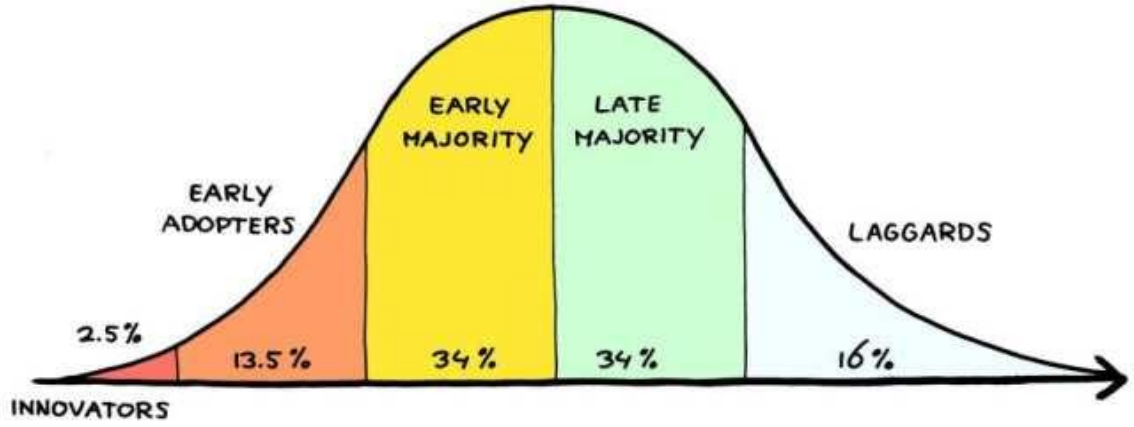
TSA Approval Packages

Other Verifier Mappings

Next Time: What do we do if this is one of 50 projects?

- Scope is essential – you don't have to solve the CEO's problems - focus on your area of control
  - Empathy is key – strive to create a "pocket of magic"

- Spread Security Capabilities/Functions – use your security champions
  - Train operational and implementation teams on Modelling. (*Side benefit: this helps identify champions*)
  - High performing teams draw attention, and practices spread as members get promoted to other teams Teams are built to be broken!



- Selling security is **<u>hard</u>** - focus on the innovators and early adopters. Tipping point will occur naturally.
  - We had the benefit where this project had a number of early adopters
  - As others see what you create it will spread organization wide

From Idea to Trusted Product: Four-Phase Security Playbook
Pilot → Standardize → Certify → Leverage

1. Identify 5 Worst Risks
2. Limited scope / Controlled Environment
3. Prove Value; Build Momentum

1. Interoperability: Find where this has been done
2. Support extra functionality
3. Communicate progress; build trust

1. ISO for adoption
2. Add custom controls (NIST 800-53)
3. SOC2 for Operations

1. Use existing certifications / evidence
2. Map matrix to asks
3. Package everything for customers/regulators

How to Start? Next Slide: The First 90 Days

Your First 90 Days – Getting to Traction and Early Proof

0-15 Days

Identify Key Relationships / Top 5 "doomsday scenarios"
Determine (Limit) Scope: Itemize your Scoped Data and use the DFD to watch where it goes
Map the People Scope: See Slide "Before Anything…"
Select Control baseline: determine your reference standard
Scorecard v0.1 (2–3 metrics).
Artifacts: scope doc, initial threat list, SoA draft, Scorecard v0.1.

Days 16-30 – Lay the Groundwork

Wire the pipeline: PR checklist, SAST/SCA, ticketing links.
Tools: Decide on Tools for Pipeline and GRC
Workshops: Run workshops with ops teams on existing processes
Risk decisions: document residual risks & owners.
Threat Modelling: Run 2-3 DFD Modelling Sessions
Artifacts: PR template, scan policies, auditable tickets, residual-risk log.

Days 31–60 — Prove & Iterate

Tabletop & spot checks: one restore test; one access review; trace one prod fix from ticket→code→tests→approvals.
Scorecard v1.0: add *Confidence + Forward Guidance*
Readiness pass: mini SOC2/ISO walkthrough on 3–5 controls to validate evidence quality.
Artifacts: test reports, traceability pack, scorecard v1.0, readiness findings.

Days 61–90 — Package & Leverage

Finalize Scope, SOA and Compliance Plan
Evidence pack mapped to your key stakeholders
Operating cadence: monthly checks (vendors, access, DR tests), metric targets, comms rhythm.
Handoff: Develop gap assessment for any increased scope
Artifacts: draft evidence bundle (GRC Tooling), Scope/SOA statement, Gap Assessment

“We started with a pilot in a brewery. Now, our credential is trusted by the TSA. That journey wasn’t linear—it was **layered**, **audited**, and **hard-earned**.”

Thanks to the passionate teams at DMV and CBN, auditors, ISO contributors and TSA partners who turned an idea into a real Digital ID.