Authentic Web®

Empowering Teams for DNS Security and Compliance

Mergers & Acquisitions

M&A Guide to Assess and Consolidate Domain Assets and DNS Networks

A Discussion Brief

"Assessing and consolidating domains and DNS providers are critical "pre" and "post" M&A deal priorities. You are not only buying the valuable assets, you are also buying the cyber security risk."

Peter LaMantia,
Founder and CEO Authentic Web Inc.

How due diligence teams can maximize deal value and mitigate post-close risk and cost.

There are many blogs, webinars, and how-to guides about acquiring domain assets – mostly centered on ownership rights, title, and brand protection during the M&A process. They are mainly useful to legal counsel, finance, and marketing but overlook a gaping area of risk and cost containment.

We're talking about enterprise security and the network operations functions tasked with managing the DNS networks, mitigating risk, and managing integration costs after the deal closes.

Enterprise Value

Security Risk

Cost Containment

In this paper, we'll discuss the known security and operations problems in acquiring domain and DNS assets, and effective ways to solve them. We'll present a modern, best practices approach for companies active in M&A from pre-deal audit and assessment to post-deal consolidation.

If you have questions and would like to discuss how to address risks and apply best practices during both the pre-deal and post-deal stages.

Contact us here →

> "Our company acquired more than a dozen businesses over the last few years. The task to gain control fell on our infrastructure teams to consolidate 100s of domain assets and the DNS. This was not a small challenge. It became clear that we needed a domain, DNS, and certificate partner for this activity and we contracted with Authentic Web.
>
> Authentic Web's guidance, systems, project management and support were exemplary. They guided us through every step and executed. If you are a corporation seeking to consolidate domain assets, DNS and certificates, we highly recommend Authentic Web."

Executive Summary

You are not just buying the assets - you are acquiring cyber security risk.

M&A teams face operational and IT risk when acquiring domain assets and the related DNS networks. The acquirer has a limited time frame to assume ownership of the domains and integrate them into network operations. These domains will have latent operational and security issues, unaddressed by the target company. The acquiring party does not have visibility into the true state, nor will it have any means to assess its security posture. The purchaser will be acquiring all the cyber risk and operational deficiencies associated with the target assets – and it will be largely blind.

Enterprise domain sellers don't know what they've got – neither do the buyers

Few operators have an accurate inventory of their domain assets and DNS network. That's because their domains and DNS are scattered across multiple domain registrars, DNS services, and certificate authorities. Even when companies concentrate their high value domains on a single, corporate domain registrar, they invariably have more domains managed elsewhere. Put 10-20 DNS services into the mix and it's a safe bet that management doesn't have an accurate picture of its own DNS network.

Ignorance is not bliss – your enterprise security is at risk

The M&A team of an acquiring company has no accurate picture of the domain assets and DNS network they are buying, nor do they typically have an easy means to complete network and security due diligence. Hundreds (or thousands) of domains across many registrars and DNS services, require diligently managed zone files and the application of DNS security settings. M&A needs to assess the state of pre-deal DNS configurations for each domain. This includes an assessment of live or missing Name Servers, DNSSEC, DMARC, SPF, CNAMEs, A Records and TLS certificates with related versions and expiry dates.

Pre-deal best practices start with knowledge

M&A teams need reliable pre-deal audit data on the domain assets and DNS network they're acquiring. Commercially available domain audit tools are uncommon. Thankfully, some firms have developed systems and techniques to audit domains and DNS networks. Using these technologies, due diligence teams gain invaluable data during the "pre-deal" phase, providing insights into the asset value, a one-time snapshot into DNS security posture, and a checklist to execute before and after closing.

Post-deal execution leverages pre-deal audit data

Without accurate pre-deal data, M&A teams assume the risks in acquiring domain and DNS assets. Compounding the security risks are the operational issues of absorbing unknown digital assets into the acquiring company's network operation. The buyer already has its own domain and DNS problems. Adding acquisition complexity exacerbates the problems with more registrars, DNS, and certificate authorities.

M&A teams equipped with pre-deal intelligence have a complete assessment of risk and foreknowledge of the resources required to plan and execute ownership control post-deal.

The End-State: A single pain of glass control system

Fragmented suppliers without modern domain and DNS management tools can cause problems for the M&A team. It won't go away before the next M&A event – it only gets worse over time. The only effective solution to the M&A pain of operationalizing acquired domains and DNS networks, is to unify them under a single control system.

Unified control systems are a rarity in the domain, DNS, and certificate space. Most large corporations use multiple registrars and DNS services, none of which integrate. This creates operational and system silos, a security and compliance mess, and pain for the teams tasked with managing the area. Unified control systems are essential to get and keep control of IT security risk, address change compliance gaps and reduce total cost of domain ownership.

A new and modern approach to domain, DNS, and certificate management places all change management under a single, unified, control system, combining domains, DNS, and TLS certificates into a single pane of glass view. With permissioned, secure, role-based access, change history, and security monitoring, no detail can be overlooked. This helps network administration resources day-to-day and facilitates the next due diligence, acquisition, and operationalization of new domain assets and DNS networks.

The traditional, multi-supplier/multi-platform approach to domain asset and DNS management is high risk, high-effort, and high cost. Serial M&A events that pile on more, simply exacerbate the problem.

The solution is:

1. A domain and DNS audit to inform pre-deal schedules and post-deal execution planning
2. A post-deal consolidation of domain assets and DNS network under a single, unified control platform

THE RESULT

Control **Visibility** **Automation** **Security** **Compliance**

Background

Domain portfolios and the DNS networks they run on are inherently non secure despite the best efforts of network operators and IT security staff. Empirical evidence overwhelmingly demonstrates that the DNS is a top attack vector for organizations that have not prioritized activity to fully lock it down. Audits show that every enterprise has vulnerability gaps, unknown to their IT staff. There are two major reasons for this.

ONE

Few companies know their full domain inventory, and virtually none the full extent of their DNS network

The enterprise digital footprint often includes unknown or poorly inventoried domains, registrars, and DNS providers. Access to registrars and DNS access for change management can be unclear or fragmented with related access controls and change management gaps. Accurate zone file enumeration is rarely present. DNS zone files are the junk draw in the infrastructure kitchen (Webinar: DNS Security - The Zone Mess), filled with long-forgotten legacy settings that expose the enterprise to cyber risk.

Problem

You are acquiring a company with a medium to large, digital asset inventory. They cannot (or won't) tell you what they own or have configured on the DNS. Regardless, it will be on your team to gain control and integrate the assets and related DNS network.

TWO

The DNS is a global public network. It is non secure by design. Few teams have comprehensive, effective DNS security configurations in place or a systems-based control environment.

The Domain Name System is the global network available to anyone who wants to look. This is why the DNS is a prime attack vector. It's used in almost all cyber attacks. Domain portfolios that are about to change hands are especially vulnerable. Every company is under watch by third party actors who hunt security gaps and lie in wait to strike. Two companies merging increases that risk since these actors anticipate that institutional knowledge and staff disruption is common to merger events.

Problem

Enterprise DNS networks contain many ungoverned errors and omissions. Any single issue represents a vulnerability and attack vector. Examples include missing or misconfigured SPF, DMARC, and Start of Authority (SOA) records, orphaned ARecords, dangling CNAMEs, or insecure redirects. You must secure the DNS network you're buying. Don't think for a moment that outside parties are not watching.

The Deal Phases

In M&A the acquirer has two phases with distinct activities, summarized as follows:

Pre-Deal
Due Diligence Assessment, Audit and Consolidation/Integration Planning

Post-Deal
Consolidation, Integration Execution and Control System Set Up

Pre-Deal

Pre-Deal is about due diligence and planning on everything from financial statement audits, customers, revenue, cost structure, technology audits, and leadership team assessments.

FACT

Domains and the DNS underpin every enterprise's digital business.

It is critical to understand the scope and condition of these assets and networks. You are buying the assets and the cyber security risks. Risk assessment is required.

PROBLEM

Due diligence in this area is weak, relying on the target company's internal, potentially biased views and incomplete information. Acquirers require a third party equipped with technology to support the pre-deal due diligence assessments and post-deal consolidation integration support plan.

Acquirers need to know and prepare with the following:

1. Digital asset inventory and network audit
2. DNS network security and change compliance risk/maturity assessment
3. Annual recurring Total Cost of Ownership (TC0) (post-deal)
4. Scoping, planning, deal terms and readiness for post-deal domain and DNS consolidation

Pre-deal due diligence aligns with traditional due diligence focus areas covering often overlooked/under assessed Domains, DNS and Certificates.

Due Diligence Area		Domains, DNS and Certificates
Operational Due Diligence (ODD)	→	Operational Gaps and Risks
IT Due Diligence (ITDD)	→	Operational and Financial Risk
Digital Due Diligence	→	Digital Footprint Inventory
Technology Asset Due Diligence	→	Tech Stack Supporting

Post-Deal

Post-Deal is about business continuity involving people, process and systems. The acquirer's mission after the deal closing must be the consolidation and integration activity to gain cost efficiencies and to operationally execute on the acquisition strategy and purpose.

PROBLEM
Domains and DNS are difficult to manage and consolidate, relying on internal institutional knowledge and cooperation to execute. Acquirers need a post-acquisition integration/consolidation plan to be documented and resourced upon closing.

Acquirers must be prepared ready to execute immediately upon close.

1. Take control of Registrar, DNS Provider and Certificate Authority vendor systems
2. Implement consolidation with a vendor/turnkey service to execute and address security gaps
3. Establish an enterprise control system to empower teams to manage assets and networks

Post-deal consolidation of assets and network controls now moves to project execution.

Consolidation		Domains, DNS and Certificates
Asset Inventory and Network Status	→	Multiple Vendor Consolidation
Turnkey Project Execution Plan	→	Systems Vendor and Team Readiness
Project Management	→	Project Execution
Digital Control System Training	→	Digital Control System - Tech & Support

Control **Visibility** **Automation** **Security** **Compliance**

STILL A FACT

Domains and the DNS underpin every enterprise's digital business.

It is critical to consolidate and gain control over digital assets as soon as possible, post-deal.

The Deal and the Team Story

Let's break down a typical M&A event involving a sizeable domain portfolio in the acquired assets, the teams affected, and the best practices they should follow.

We'll call the target acquisition GlobalCo. Your internal due diligence team has been assembled with senior management representatives from key stakeholder areas. Your CFO and Chief Legal Officer are calling the shots and the deadlines are crazy short. At some point, usually after due diligence, the Network Ops and IT security get pulled in and (as usual!), get the short end of the stick. They were told the deal was happening and now they need to manage an entirely new team, new systems, networks, and all the technical debt and challenges at GlobalCo. They are told to prioritize the revenue and customer-supporting systems and are typically inclined to leave the DNS as is "for now." This is when the problems start.

Evaluating Digital Asset Values and Security Posture – Old School

Getting a handle on the inventory and pre-deal security is prohibitively expensive and difficult even for internal knowledge experts. There are few tools and systems to provide detailed APEX-level accounting for individual domain network and related security settings. Proprietary audit tools are rare, if available at all. Network operations and IT security teams are typically forced to run laborious server-level queries. Approximately 80% of the Fortune 1000 use Excel spreadsheets to snapshot their domain portfolios. These aren't tools. They are manual, time consuming, error-prone exercises that soak up valuable staff time. They commonly miss material data from the "don't know what we don't know" category. Making matters worse, your due diligence team is strictly need-to-know, and under NDA. You don't have access to the staff you need to complete this onerous exercise. The result is that you are buying assets without the required visibility to identify the imbedded risks.

The only way to address this is with an independent third party with specialized systems to provide an assessment record, a risk profile, and an inventory of assets and configurations.

Pre-Deal Phase

Issue one for the M&A team is accurately valuing the digital assets of the target company. GlobalCo may have a combination of a corporate registrar providers with a stated inventory of several hundred domains. More likely they have many retail, and or Corporate registrars and DNS providers. GlobalCo has been acquiring companies for many years – absorbing multiple domain portfolios of their own. It's unlikely the legacy domains acquired have ever been consolidated under a single registrar, DNS network and change control system.

GlobalCo staff may be unaware that they have legacy domains scattered across many registrars due to legacy acquisitions or past IT preferences. Compounding matters, they use multiple DNS providers. This is where things get really messy. Your team doesn't know the true number of domains, what they are, where they are registered, or what DNS service they are running on. Worse, the DNS underpins the digital footprint that cannot be easily inventoried. There are no forensics available to figure it out. Pre-deal due diligence simply accepts the information received (trusted or not) and the deal gets done.

Pre-deal continued ...

Domain asset value is one thing. IT security and control risk cannot be ignored. Your in-house counsel, and CMO are focused on domain ownership, but there's significant risk hiding under the surface of the DNS network. To fully assess your pre-deal risk and adequately plan for the efficient, risk-mitigated integration, it's critical to know what they own, how it's set up, and who has control.

A domain/DNS security posture audit, requires knowledge of:

1. Domain registrars with a review of access and change controls
2. DNS service providers with a review of access and change controls
3. Assessment of DNS security risks with a time-stamped state of the network
4. Mapping of domain and DNS security settings ie: SPF, DMARC, and DNSSEC
5. Risk audit of HTTPS, redirects, CNAMEs and certificate coverage

You must have a time-stamped assessment to know what you are acquiring. There is a critical window between this assessment and the post-close phase during which internal personnel can make changes that could impact the asset value or create new security vulnerabilities. Pre-deal due diligence to closing and the subsequent timeline to gain control and consolidate is a highly vulnerable interval.

You need deal terms with an agreed plan to consolidate and secure the acquired assets in advance. It should be budgeted into the consolidation/integration phase as quickly as possible in the post-deal phase.

Registrars

DNS Providers

Risk Audit

Access Controls

Plans

Systems

Post-Deal Phase

The time for due diligence, rushed as it was, is over. Escrow transfers at midnight and ready or not, you now own GlobalCo, all their domains, DNS operations, and all the value and unseen risk that comes with it. The question is: are you really ready to consolidate and integrate the new DNS footprint? Likely, you aren't. Your team has been on an M&A tear for years and GlobalCo is the latest of many recent acquisitions.

You probably haven't fully consolidated and integrated the last batch of domain assets you acquired, or the one before that. It's the can you've kicked down the road more than once. "We'll get to it when things settle down," you say. But have they ever? Prior to close you need a DNS Security Policy and a plan to establish system-based compliance governance.

Post-deal continued ...

The immediate post-closing phase is fraught with unique risks. Staff can be skittish under new management and turnover of key personnel is common. “The guy who knows about *that* DNS setup and *those* domains just left or got re-assigned.” Pre-deal certainty wasn’t clear and post-deal, it’s even less so as institutional knowledge dissipates with turnover

Common risks post-closing include:

Inventory
Partial inventory of valuable digital assets

Security Risk
Unknown risks you must discover and mitigate

Personnel
Turnover & internal errors exposes the business

Expiring Domains
Valuable assets that fall through the cracks

Expiring Certificates
Expiring ungoverned TLS certificates

Every month after closing, the need to consolidate and integrate domains and DNS operations intensifies, while the passage of time erodes “institutional memory.” Empirical audits of M&A-active enterprises invariably reveal unresolved legacy issues and security-compromising artifacts dating back years.

Post close priorities and actions must include:

Security Policy
Establish a DNS Security Policy and execute a systems-based compliance program

Consolidation
Consolidate to an enterprise grade Registrar, DNS & Certificate provider control system

Full Zone Security
Audit and address DNS security risk once it is fully managed under a single control system

DNS Hygiene
Assess, implement DNS resource record cleanup and set criteria to cull non-valued domains

People and Systems
Establish internal ownership and systems to maintain compliance with DNS security policies

While these priorities and actions are great in principle, they're a classic case of "easier said than done." The same manual processes and lack of tools that impeded a full due diligence exercise on GlobalCo's domains and DNS is as much at play post-deal, exacerbated by the larger and more disparate legacy base of domains that now must be managed.

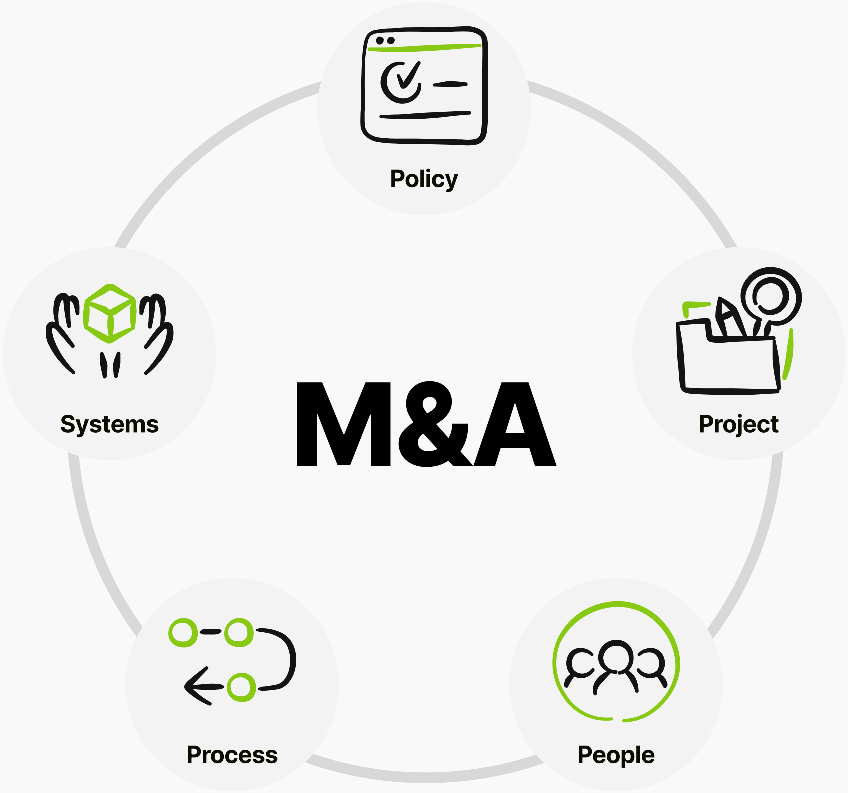
Your existing vendors: Registrars, DNS services, and Certificate Authorities could theoretically help but are sub-optimal for several reasons. Retail domain registrars are singularly ill-equipped to facilitate enterprise domain consolidation. Your principal corporate registrar is the logical candidate to manage consolidation, but they are typically not equipped on the DNS and security side of the picture. That will be on you. DNS and Certificate Authorities provide their commodities but do not get involved to help customers migrate to competitive third party suppliers. Again, it'll be on you.

The most dispiriting aspect of these priorities is the fact that once done (at great effort and expense), the next acquisitions will repeat the same issues and cycles.

Repeatable Process and Systems

You require a repeatable, proven process to maximize asset value, minimize security risk and efficiently manage costs while ensuring business continuity from pre-deal to post-deal to growth.

M&A Playbook for Domain DNS and Certificate Consolidations



Best Practices: A Modern Approach

If the scenario above sounds messy, it's because it is. Senior enterprise network operators and IT security managers frequently admit that their domain and DNS operations likely have several latent problems, yet are best left alone owing to time, staff, cost, and risk of breakage. So, when new domains and a DNS network are acquired, the problem worsens since few companies have the necessary control systems in place.

It doesn't have to be this way. The perpetual cycle of M&A-driven risk and operational angst related to domains and DNS is, at the core, a process problem in change management. If your company acquires companies as part of its success model, then it stands to reason you need a change management process tailor-made for consolidating and managing valuable domains and the DNS networks on which the business operates.

Modern domain/DNS change management systems providers take a much different approach to that of traditional domain registrars.

The foundation of the new approach is:

Control
Change management workflow control and change history

Visibility
Single pane of glass digital asset and network visibility

Automation
Automated, purpose- built tools to manage domain & DNS

Security
DNS security visibility to empowers teams to get and keep control

Compliance
System-based security policy compliance

On these five pillars, every step in the cradle-to-grave lifecycle of an enterprise domain can be reliably and economically managed.

Efficiencies, cost savings, and enhanced security can not only resolve the urgent issues in an M&A event but also apply to day-to-day operations under steady state.

Best Practices by Stage of M&A Event

1. Pre-Deal Due Diligence and Planning Phase

Recall our two areas of concern are:

A. Getting an accurate inventory of digital assets from the acquisition target, and

B. Executing a complete and comprehensive security audit of all domains and the related DNS network.

The complicating factor is, you don't know what the target company has, and neither do they. Your target assets may be a simple case scenario, or an extremely complicated scenario requiring significant effort to absorb. This should be reflected in the purchase price as a cost to realize the asset purchase IRR (*internal rate of return*).

Accordingly, M&A due diligence teams (and their consulting partners) need modern tools that can quickly and accurately discover a target's complete domain and DNS environment. The checklist is:

A. Establish an inventory baseline to include in the purchase agreement schedules
B. Conduct a domain and DNS audit to benchmark current configurations "pre-deal"
C. Articulate business risks exposed by the audit, and potential impacts
D. Prepare a Consolidation/Integration plan and agreement between parties identifying key personnel, vendors, and technologies to be utilized
E. Create and approve a budget as part of the larger post deal consolidation/integration work effort

The benefit in nailing the pre-close due diligence phase is a "once and done" pre-consolidation and integration step. Serial acquisition of disparate domain and DNS portfolios was never a "rinse & repeat" undertaking. It's more accurately, a compounding and postponing of operational pain that never quite goes away.

2. Post-close Integration Phase

Armed with an accurate, comprehensive inventory of digital assets and a detailed audit of the DNS security posture, best practices dictate avoiding two typical scenarios:

A. Bringing new domains and DNS operations in as a bolt-on i.e., status quo

B. Migrating newly acquired domains (tuck-in) to an existing corporate domain registrar

The former will resolve few security issues, provide few economies of scale, and fail to resolve future M&A challenges when acquiring domains. Status quo operations by the acquirer, even with incremental clean up, merely perpetuate the many risks identified above.

The latter approach, migrating to an incumbent corporate registrar, is a partial step to achieving economy of scale. One registrar is preferable to many. The approach leaves unanswered: DNS security (pre-and post-deal), portfolio rationalization, detailed zone file (and resource record) cleanup, and future change management improvements.

Best Practice Steps and Benefits

The superior approach is to use an M&A event as the catalyst for integrating the entire domain and DNS operation under a single, unified change management platform.

Step 1 → Utilize the pre-deal audit to scope a consolidation execution plan and related costs

Step 2 → Identify and lock up the key personnel from the target company for execution

Step 3 → Establish the DNS Security Policies

Step 4 → Follow a best practices domain/DNS consolidation project methodology

Step 5 → Once consolidated, address legacy security gaps to bring into compliance

Step 6 → Use control systems to keep control and provide a destination for the next acquisition

Immediate and long-term benefits are compelling:

- ✓ DNS and **security issues are easily resolved** down to the granular level of sub-domains, all zone file resource records, as a seamless component of the migration process
- ✓ **Eliminate disparate and fragmented providers** including domain registrars, DNS providers and certificate authorities in favor of a single, easier to manage supplier to gain control and reduce costs
- ✓ Go-forward change management **control and security compliance is achieved** for all domain and DNS operations: both legacy, newly acquired, and expected future asset purchases.
- ✓ Business case economics of a unified, consolidated change management platform are highly positive – serial M&A players **experience operational cost savings** that easily fund future domain acquisitions
- ✓ Enforced security compliance and monitoring ensures that newly secured **domain/DNS operations will remain secure** through ongoing organic changes and new M&A events
- ✓ Single pane of glass control system automation over all change management tasks and compliance
- ✓ Equip the business (and M&A stakeholders) with a playbook that repeats success, economically

Control **Visibility** **Automation** **Security** **Compliance**

Summary and Conclusion

Well-managed domains are extremely valuable, branded digital assets. The DNS underpins the entire business and cannot be left to post-deal control uncertainty. You are buying the assets.

You are also buying the cyber security risk. **This must be well managed.**

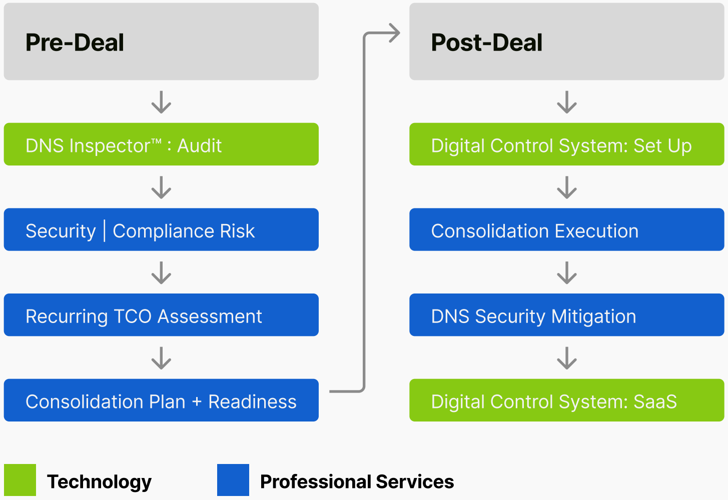
Pre-deal, teams lack the tools to identify domains and understand the scope of disparate DNS services. A complete and accurate audit of the target's DNS security posture is difficult, if not impossible to assess.

Post-deal operational methods perpetuate both legacy security risks and ongoing change management woes. Bolt-on operations merely accept and perpetuate the newly acquired domain/DNS operations as given. Tuck-in integration fails to address the root cause of domain and DNS operations issues, which is a flawed change management control posture across the portfolio and DNS network.

Equipped with effective tools and best practices, M&A players can dramatically improve successive acquisitions. By solidifying legacy domains and DNS on a modern, change management control system, M&A teams become efficient and well-positioned to mitigate cyber risk.

Each M&A event presents a serendipitous opportunity to transform the due diligence effort and post-deal operations playbook. The same exercise can permanently rationalize your legacy domain and DNS operations that successive acquisitions over time have made unsustainable.

Modern technology to support Pre to Post M&A Deals: Domains | DNS | Certificates



Breaking the cycle of bolt-on and tuck-in domain acquisition requires a one-time shift to a pre-deal and post-deal playbook supported by a unified change management control system. Once done, the benefits are significant:

Once done, the benefits are significant:

1. Maximized asset value capture post-close
2. Reduced effort and increased performance of digital asset due diligence teams
3. Immediate, improved security in enterprise DNS operations
4. Assured go-forward compliance and maintained security
5. Reduced TCO (total cost of ownership) of all domains and DNS operations
6. An economical, secure and repeatable platform for ongoing, and future acquisitions

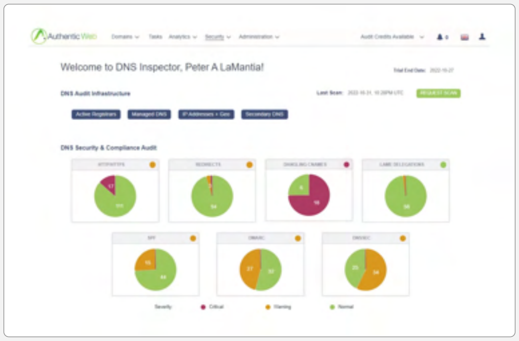
Empower Your People with Authentic Web Systems and Services

Learn how our systems and services will ensure your successful due diligence, post deal consolidation and ongoing security, compliance, and performance on the DNS.

Pre-Deal

Domain & DNS Assessment and Audit Tool

DNS Inspector™



Welcome to DNS Inspector, Peter A LaMantia!

DNS Audit Infrastructure

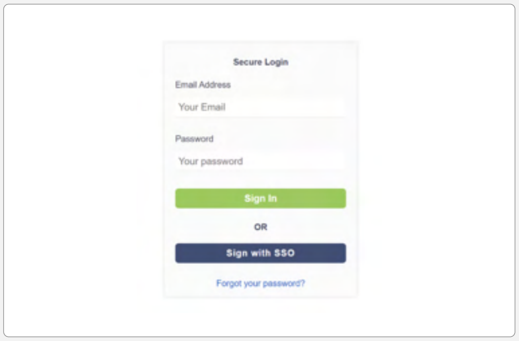
DNS Security & Compliance Audit

Learn more →

Post-Deal

Single Pane of Glass Control System

Domain Name Asset Manger™



Secure Login

Email Address

Your Email

Password

Your password

Learn more →

Trusted by customers around the world

G Adventures — Our world deserves more you.

DESTINATION CANADA

Attindas HYGIENE PARTNERS

CBC

SHL.

EverView

Canadä

pib insurance brokers

> "I have been using the DNAM system extensively since the domain consolidation project. It's simple to use, allowing our teams to manage our portfolio across multiple operating entities with ease. As well as the standard domain management tools it also offers other useful features such as permissions and role management, domain security and SSL certificates. The support I have received from the Authentic Web team has been second to none"

Get in Touch

Book a meeting to discuss your M&A or domain and DNS control challenges.

Learn more about AuthenticWeb.com