ObservePoint

The Digital Governance Framework

Understanding & Implementing a Digital Governance Solution

The amount of analytic, marketing, and privacy software on your website means digital governance is essential to safeguarding a dynamic and secure online presence.

Malfunctioning software and broken, duplicated, or missing tags can cause:

- Faulty data
- Bad customer experiences
- Wasted investments
- Suboptimal insights leading to poor decisions
- Data leaks and privacy violations

Digital governance is a discipline focused on testing and monitoring the functionality of your third-party MarTech, so you can trust your implementations and act on validated data. Digital governance solutions:

- Test and validate your technologies to ensure accurate data collection and insights
- Audit your cookies and tags for privacy compliance
- Find and alert you to journey interruptions, so you can optimize user experiences

Use the following framework to adopt an automated, digital governance solution that can scale with your enterprise.

Plan

Digital governance plays an important role in planning your data collection strategy, privacy compliance validation, and how you will monitor and maintain implementations. Assemble a team that will make it a priority in your organization.

Establish a Digital Governance Committee

A digital governance committee ensures accountability for governance strategy, documentation, testing, and success of digital initiatives. Include data champions from applicable departments (Marketing, Analytics, Privacy, Legal, IT, Engineering) and appoint a leader with organizational seniority and a strong technical background. The committee should meet regularly and take responsibility for:

- Establishing business requirements for deploying technology
- Assembling and enforcing a standardized technology and governance plan
- Setting up protocols to enable compliance with privacy regulations
- Addressing concerns that arise

Strategize

Take a look at each of your digital technology vendors, the different sections of your site, and critical user paths, then ask the following questions:

- Why is this technology/page/user path included on my site?
- What would happen if it failed?
- How would I define success/failure for this technology/page/user path?

Think of it in terms of:

Purpose	Why does this technology/page/user path exist?
Priority	How important is this to my site?
Prevent	How can I identify and protect against future failure?

The planning phase allows you to map your business questions (e.g. Which segment of our customers converts best under x conditions?) against the variables that collect relevant data. The same principle applies for tags that add features to your site: you need to have a plan for when, where, and how they should be implemented.

Build a Tagging & Technology Plan

This is the blueprint for all the details of your implementation, specifically technology vendors, tags, and variables. It describes where, when, and how technology should be deployed and functioning.

Solutions for Enterprise Digital Governance

ObservePoint's complete Digital Governance solution can help:

- Govern technology across teams with multiple user access
- Test implementations and alert digital governance owners
- Reverse engineer tagging plans if you've been living with an outdated one

Comply

Proactively protecting consumer data is good business, not only to avoid hefty fines, but also because a trustworthy reputation translates into loyalty from your customers. Compliance with GDPR, CCPA, LGPD, and other impending regulations should be a regular part of your operations to provide a transparent, welcoming digital experience that safeguards your customers and your company.

While there are larger privacy frameworks to assess and manage overall privacy risks for your company, your digital governance strategy should include protocols for governing consent, cookies, and other data collection on your digital properties.

Compliance & Consent Management Platforms

CMPs are vital to managing your visitor's consent profiles, but you'll need to verify that they are doing what you intend beyond the initial data discovery stage. Implement Audits, Journeys, and Rules in your governance processes to validate ongoing compliance (see next section for details).

Implement tests to regularly check:

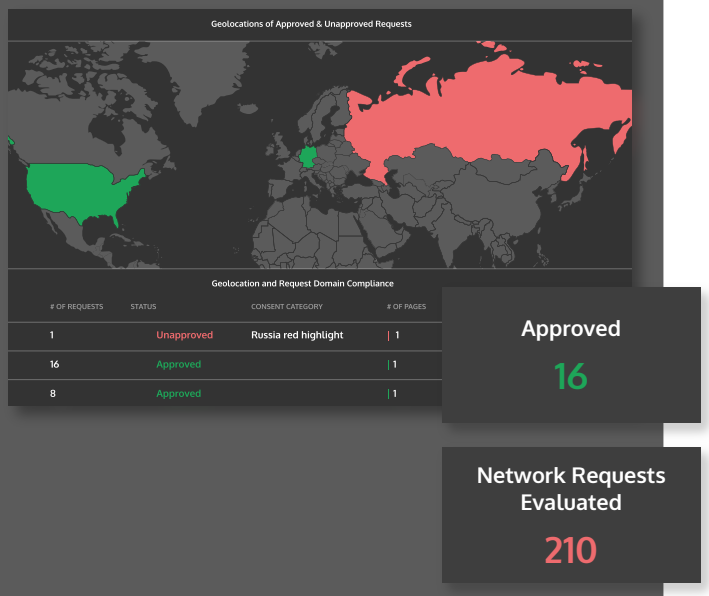
- ☑ The CMP is connected correctly to your Tag Management System
- ☑ Cookie banners and privacy policies are present on every page
- ☑ The CMP is dropping cookies after receiving consent
- ☑ Any tags a CMP can't see outside of your TMS are accounted for
- ☑ No unapproved tech has been deployed
- ☑ Data isn't being sent to unapproved locations

In addition, the Digital Governance Committee should have plans regarding how to address:

- Risky dark patterns of design
- Monitoring where data is being sent
- Mitigating risks of data leaks

Privacy Compliance Audits

You can't protect your customer's data without a complete understanding of the technology collecting data on your site or app. ObservePoint performs automated audits to identify all the tech collecting data on your site and tests CMP implementation to ensure compliance with digital standards and government regulations for customer data.



Deploy

Once you have established plans for tags and privacy compliance, you can utilize governance solutions and processes to monitor your implementation deployments and ensure the reality of your website matches your organization's vision. To start, let's go over some of the key components of digital governance you'll want to employ throughout each stage of the governance framework.

Audits, Journeys, & Rules

The three major building blocks are:

1 | Audits

Scans of the code on your site that identifies data collection technologies and any tagging errors.

2 | Journeys

Scans that validate critical user paths to ensure they are functioning correctly.

3 | Rules

A set of principles you define in the Plan stage to measure tech and their components against expected values.

Automated Audits, Journeys, & Rules

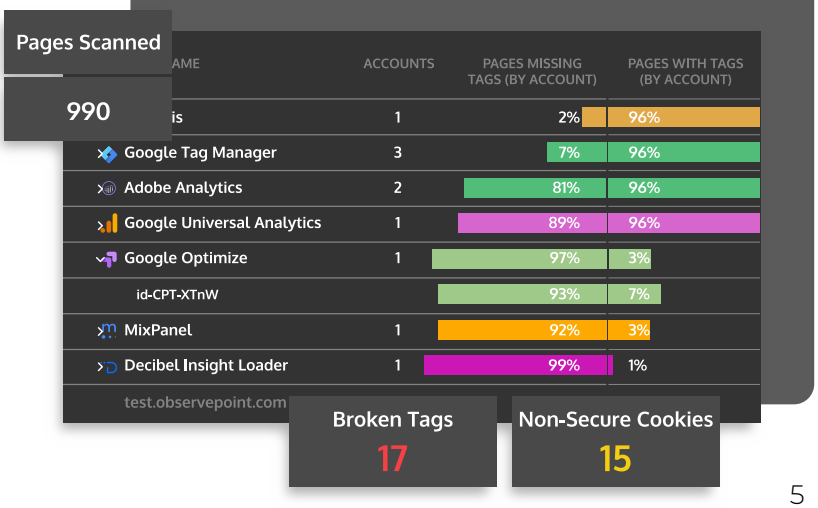
ObservePoint is a Digital Governance Solution that specializes in scalable, automated Audits, Journeys, and Rules.

Within ObservePoint:

Audits can be scheduled to regularly scan a predetermined set of pages to discover all technologies and any tagging errors, along with corresponding accounts, versions, values, and variables. They help you know what, where, and how tech is deployed. They can also check for unapproved technology and test that your CMP is fully functional.

Journeys are sequential micro-audits that simulate the interactions of a user with your website (paths to conversion, checkout, login, etc.), validating that event-triggered technology is functioning, and there are no interruptions in the user path.

Rules can be applied to any Audit or Journey, set to check for the presence of a technology, used to test the presence of Privacy Policies, and more. When a Rule fails, you'll receive a notification, so you can resolve the issue. Using filters and conditions on your Rules allows for specificity in testing. You can also save them to a library so they can be reused on demand.



Catch Errors Before They Happen

How does digital governance fit into a QA workflow? When a development team is equipped with a governance framework, they can scan implementations during development to make sure tags and data layer variables are populating according to the requirements included in the tagging/technology plan.

Where to Perform Audits vs Journeys?

Think of the first two Ps of Triple P: Purpose and Priority. Here are a few different questions to help you decide how to allocate digital governance resources:

- What are the most highly trafficked sections of my website?
- What sections of my site are most valuable to my business objectives?
- What sections of my site have a high volume of vendor tags?
- Which vendors are most integral to the functionality of my site? Where are they deployed?

Overall, you will want to have enough Audits to sample every section of your site. However, the order in which you implement these Audits or Journeys and the frequency in which they are performed will depend on the priorities and business objectives of the asset.

When to Perform Audits vs Journeys?

Ideally, you should QA your analytics implementations during development, after pushing the site live, and regularly thereafter in order to validate that everything stays in place and that the collected data is complete and clean. See the following three stages for more details on this.

QA

Digital governance solutions give quality assurance engineers procedures and tools to automate testing in staging environments.

QA: Your last line of defense before production

The job of the QA engineer is similar to the developer in that they are testing technology performance against tagging/technology plan requirements before pushing to a production environment.

The difference is that quality assurance is going to take that tag performance testing to a whole new level—running iterative tests under various conditions, checking the functionality of buttons and forms, and making sure the measurement of the event occurred as well.

Digital governance solutions help automate their iterative tests so they can ensure tags are working under various conditions. This keeps website release cycles agile while also minimizing broken code and experiences.

Validate

Once an update is pushed live, developers can once again run an Audit or Journey on the site to make sure there were no unintended problems breaking data collection or privacy compliance technologies.

Some tags get stage fright right when you're pushing a site live. And sometimes, because humans are not perfect, errors sneak by testers. Because your site is constantly changing (and being touched by people from various departments and teams), ongoing data validation through audits and journeys is critical.

When to Test

The most important time to validate your data is at key development milestones. For example, using the model below, you should run a full-site audit to test that technologies are collecting the correct data in the development and staging environments before pushing live to production. By doing so, you can locate errors before they have the opportunity to publicly impact customer experiences and revenue opportunities.

The Development, Staging, Production Model

1 | **Development Environment** is the initial experimentation environment where you can build the minimum viable product of a website or app.

2 | **Staging Environment** is where properties are prepared to be seen by the public.

3 | **Production Environment** is the live version of your site or app and is completely accessible to the public.

Testing In Pre-production

ObservePoint's pre-production testing abilities combined with interactive team profiles allow for QA, Engineering, IT, and Marketing to collaborate on testing priorities.

Monitor

From there, you should continue to perform regular, ongoing Audits and Journeys.

Because newsflash: websites break all the time.

You might have tags falling off when someone overwrites code, personal data getting inadvertently exposed, or a piggybacking tag hitching a ride on an ad-serving tag. Testing at a regular cadence is important to ensure that your analytics implementation is error-free and secure.

Determining Testing Frequency

Knowing how frequently you'll need to run Audits and Journeys is an issue of Priority—ask yourself:

- **If this technology failed on this page or section of pages, how long could we go without it before it would be missed?**
- **How customizable is this technology? How often is it updated or changed?**

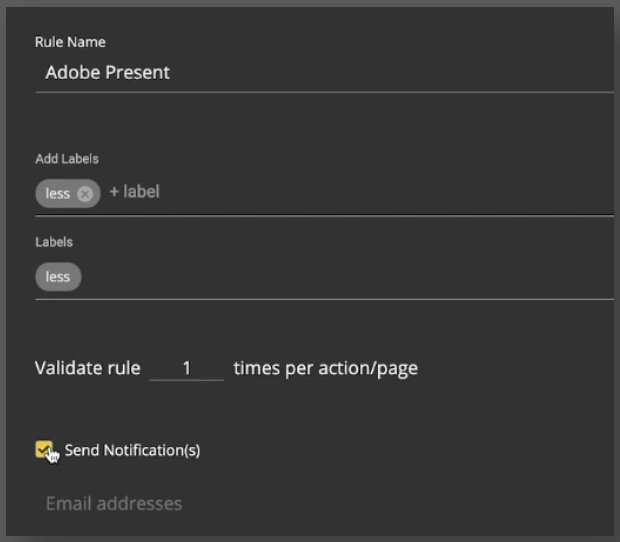
This should give you an idea of how frequently you should audit your web and mobile assets.

If your business would immediately suffer from the lost data, then these areas of your site or app should be audited daily. If not, a less frequent auditing cadence could be sufficient.

For example, you may have pages on your site that are almost never visited and rarely updated, or that provide only cursory value to your organization. Pages that fall under this category might only need to be audited monthly or quarterly, while other sections of your website that are frequently changed and/or regularly visited might need to be audited daily.

Automated Notifications

Remember with ObservePoint, Audits and Journeys can and should be set up with Rules to check against your implementation, sending you alerts whenever a Rule fails. That is where the real utility of daily auditing comes in: automated alerts. Automated alerts make it so you don't have to be in the audits daily—just when alerted to a problem.



Consistently Prioritize Testing

Finally, it is critical that the digital governance committee prioritizes ongoing testing. Responsibility for testing and validation ultimately lies with this group, so committee meetings should consistently address issues including the frequency with which audits and journeys are run and who is responsible for scheduling/initiating these tests.

Implementing the Digital Governance Framework

Digital technologies provide significant value to your company—when implemented correctly.

These technologies rely on tags and cookies, which in turn rely on proper implementation. By using an automated solution to govern tags at all phases of the framework, you can achieve greater data accuracy and actionability in your organization.

ObservePoint's digital governance solution is built on industry best practices to help enterprises like yours be more proactive about governing your digital assets and data.

The results:

- Confidence in your data and decisions
- CMP verification and privacy compliance
- Validated ROI for your technology spend

SEE HOW IT WORKS