



40 Minutes to Actionable Strategies that will Improve Customer Experience

DrupalCamp Atlanta | September 12-14, 2019



Ray Saltini

Director, Training & Enablement



Ever feel like you're jumping from one problem to the next putting out fires but never get the bandwidth to implement longer term solutions?

This 30-minute session focuses on the importance of establishing baseline assessments and measuring progress through **regular formal audits** of your content, architecture, workflow and infrastructure to seize opportunities that will strengthen visitor journeys and increase conversions.

This session is geared to both new and experienced web professionals struggling to find ways to get beyond their daily grind and make lasting improvements in systems and decision making that benefit site managers and end users alike.

Hi, we're FFW.

We combine data insights, design, and development to create engaging experiences that make brands captivating and every visit valuable.

We're not just vendors. We're trusted partners. Since 2000, we've been advisors, partners, and close collaborators to over 500 clients and counting.

375+

FULL TIME
EMPLOYEES

15

YEARS
EXPERIENCE

1000+

SOLUTIONS
DELIVERED

250

TECHNOLOGY
SPECIALISTS

500+

CLIENTS
SERVED

25

OFFICES
WORLDWIDE



Customer Experience Strategies

According to Gartner, customer experience will be the main battleground for competing companies over the next two years. And when researchers analyzed the experience and revenue data from \$1 billion+ companies for **a recent study published in the Harvard Business Review**, they found that:

In transaction-based businesses, customers who had the best experiences spent 140% more than customers who had the worst experiences.

In subscription-based businesses, customers who had the best experiences had a 74% chance of being a subscriber one year later, yet customers who had the worst experiences only had a 43% chance of remaining a subscriber a year later.

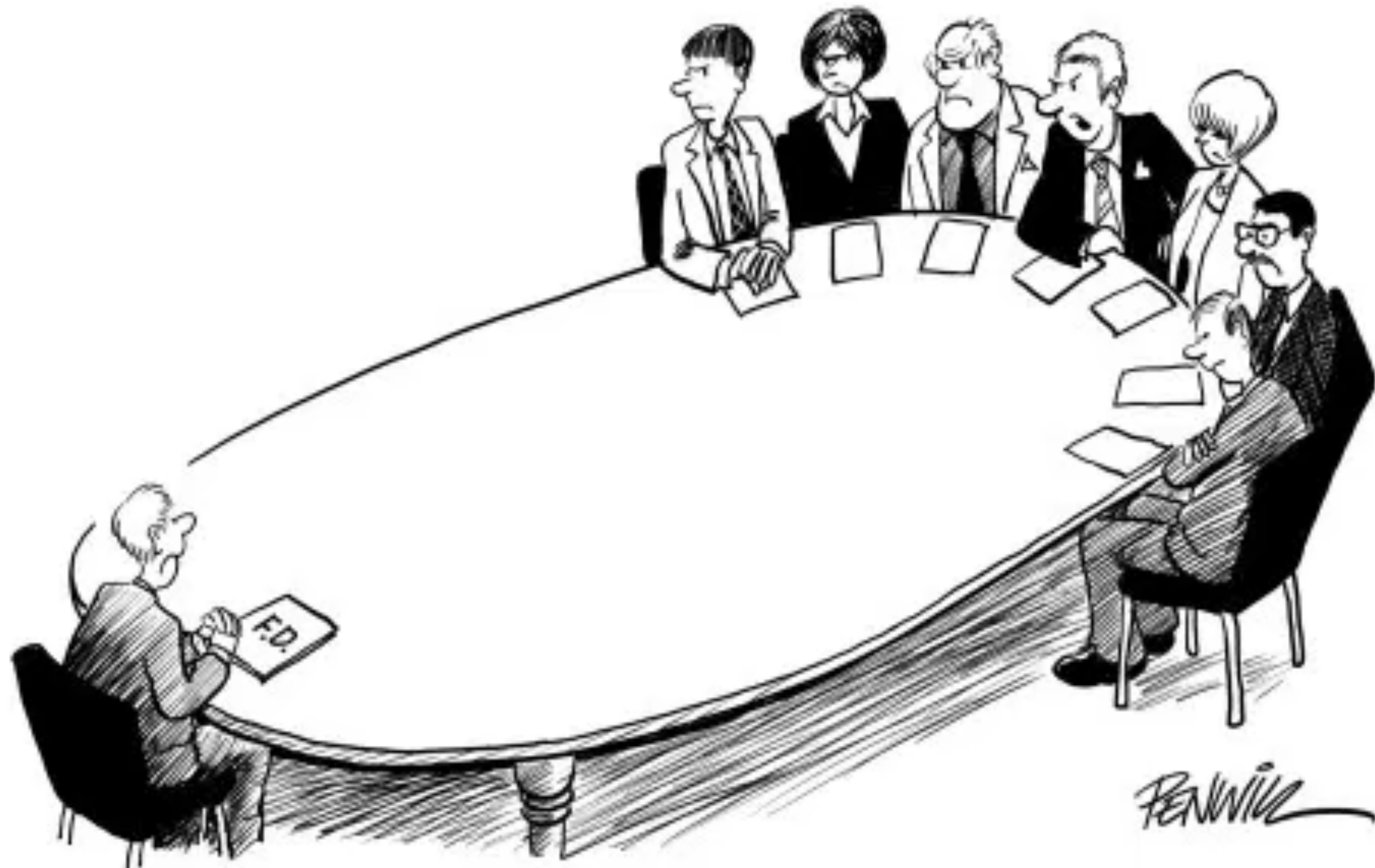
Content

UX

Accessibility

Security






"WE DON'T WANT YOU TO VIEW THIS AUDIT COMMITTEE
AS BEING IN ANY WAY CONFRONTATIONAL"



“Let thee embrace me, sour adversity, for wise men say it is the wisest course”

Standard Definition of a Audit

au·dit

/ˈôdət/ 

noun

1. an official inspection of an individual's or organization's accounts, typically by an independent body.

verb

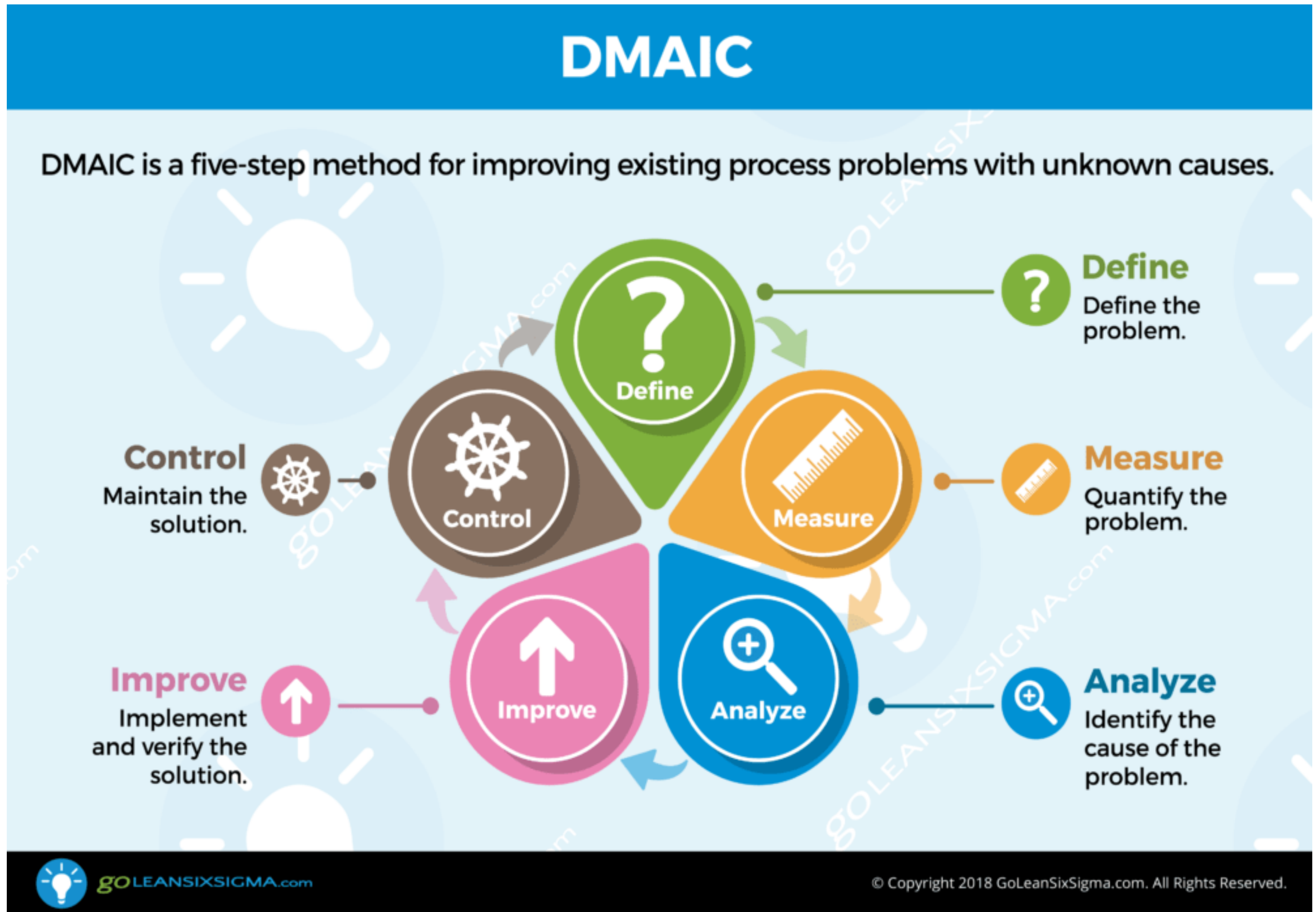
1. conduct an official financial examination of (an individual's or organization's accounts).
"companies must have their accounts audited"
synonyms: inspect, examine, survey, go through, scrutinize, check, probe, vet, investigate, inquire into, assess, verify, appraise, evaluate, review, analyze, study; [More](#)




Ancient Art of Six Sigma

Define – Your outcome goals, who your users are, and know their goals.

Measure – Metrics should align with your goals. Choose carefully.





**Audits are all
about that
base
line**

**I'm all about that
base
line**

Customer Experience Strategies

**Content Audit Strategies to
Improve Client Journeys and
Customer Experience**

The Content Audit

Content audits are the cornerstone of content strategy. They are a **qualitative** analysis of what you are communicating to your customers and an essential step in reaching your digital goals and strengthening customer experience.

What's a Journey?

The background is a movie poster for 'The Oddysey'. It features a large, dark, multi-eyed tentacle on the left side, reaching towards the center. In the upper left, a three-masted sailing ship is being held within the grasp of a smaller tentacle. The title 'THE ODDYSSEY' is written in a large, serif font across the center. The background is a warm, golden sunset over a dark sea.

THE ODDYSSEY

*Find the journey's end
in every step
of the road.*

Ralph Waldo Emerson

*Life is a journey,
not a destination.*

Steven Tyler and Richie Supa

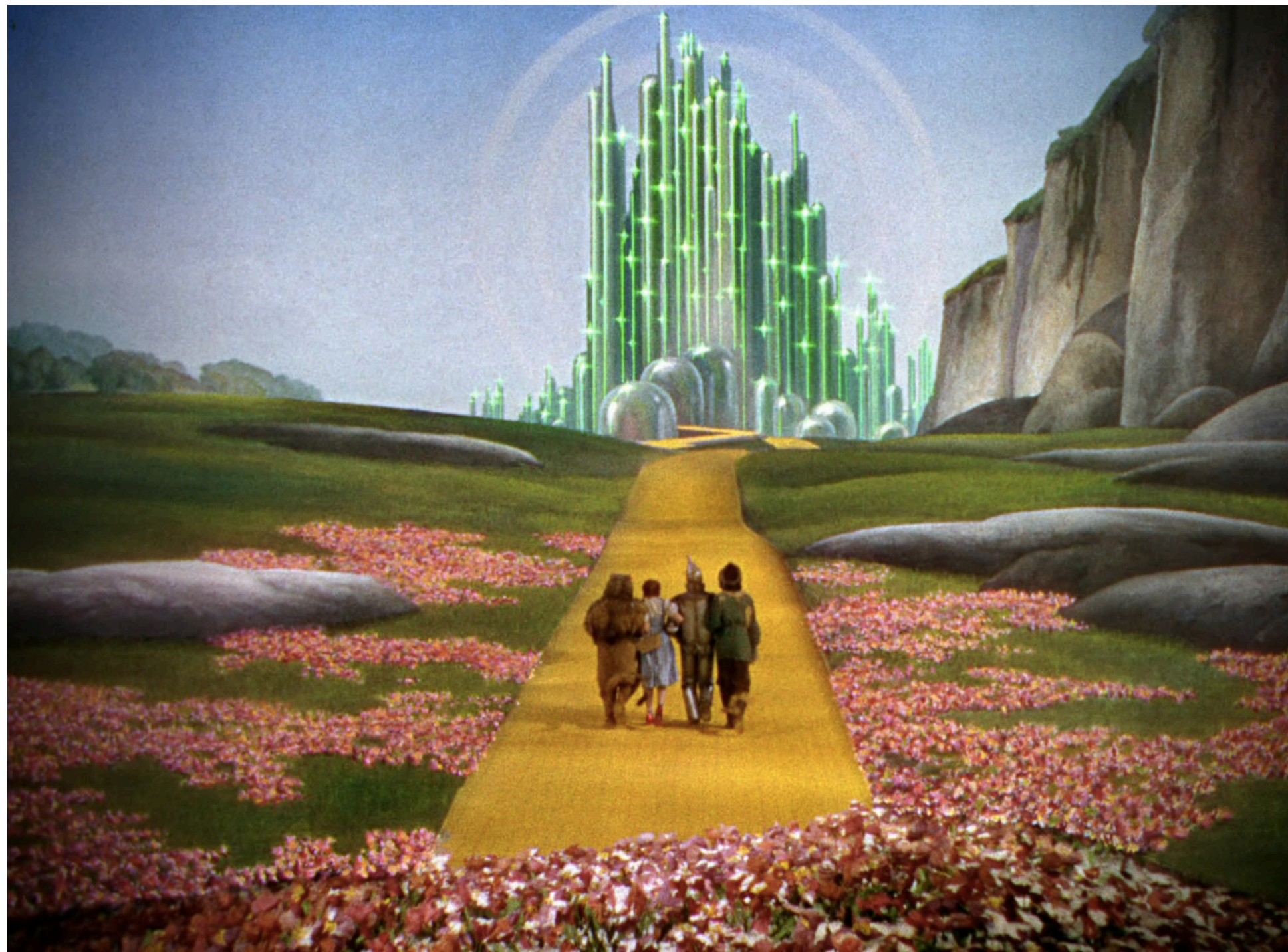
Why Should We Care?

The Commoditization of Almost Everything

Without great content, without great narrative, great code and functionality are just commodities



What makes a journey memorable and worth repeating?



We can see ourselves at
the **center** of the narrative.

*“There’s no place
like home”*

What makes a journey memorable and worth repeating?



The story has **value** for us.
It resonates.

*“Life is like a box a
chocolate, you never know
what your going to get.”*



No one remembers experiences that don't offer value or
put the client at the center of the story.

Bogus

What Do Too Many Client Journeys Look Like?





How would you like it to feel?



The New Client Centered Paradigm Journey

- **Visitors and Clients need to see themselves in the center of every story.**
- **They need to see value in your content for themselves.**

The New Client Centered Paradigm Journey

- Help visitors find what they are looking for quickly
- Don't make them wade through extraneous content
- Tell a story, put them in the middle
- Give them value, meaningful content, along the way
- Be consistent
- Focus on your core expertise



What Does a Great, Client Journey Improving, Content Audit Look Like?

- It starts with understanding your target personas.
- Begin with them in the first column!
- Align your content audit with high level user stories
- Audits images too.
- Identify good assets
- Call out the lack of assets
- Create an objective rubric of ideal content and a rating system
- Outlines editorial workflows for different types of content
- Calls out differentiators – what is special to you?
- Ask your visitors! (gasp!)



Get There From Here

- Stakeholders – Have you involved your key stakeholders?
- Architecture – Does your architecture fit your content?
- Cataloging – Are you cataloging what's not there?

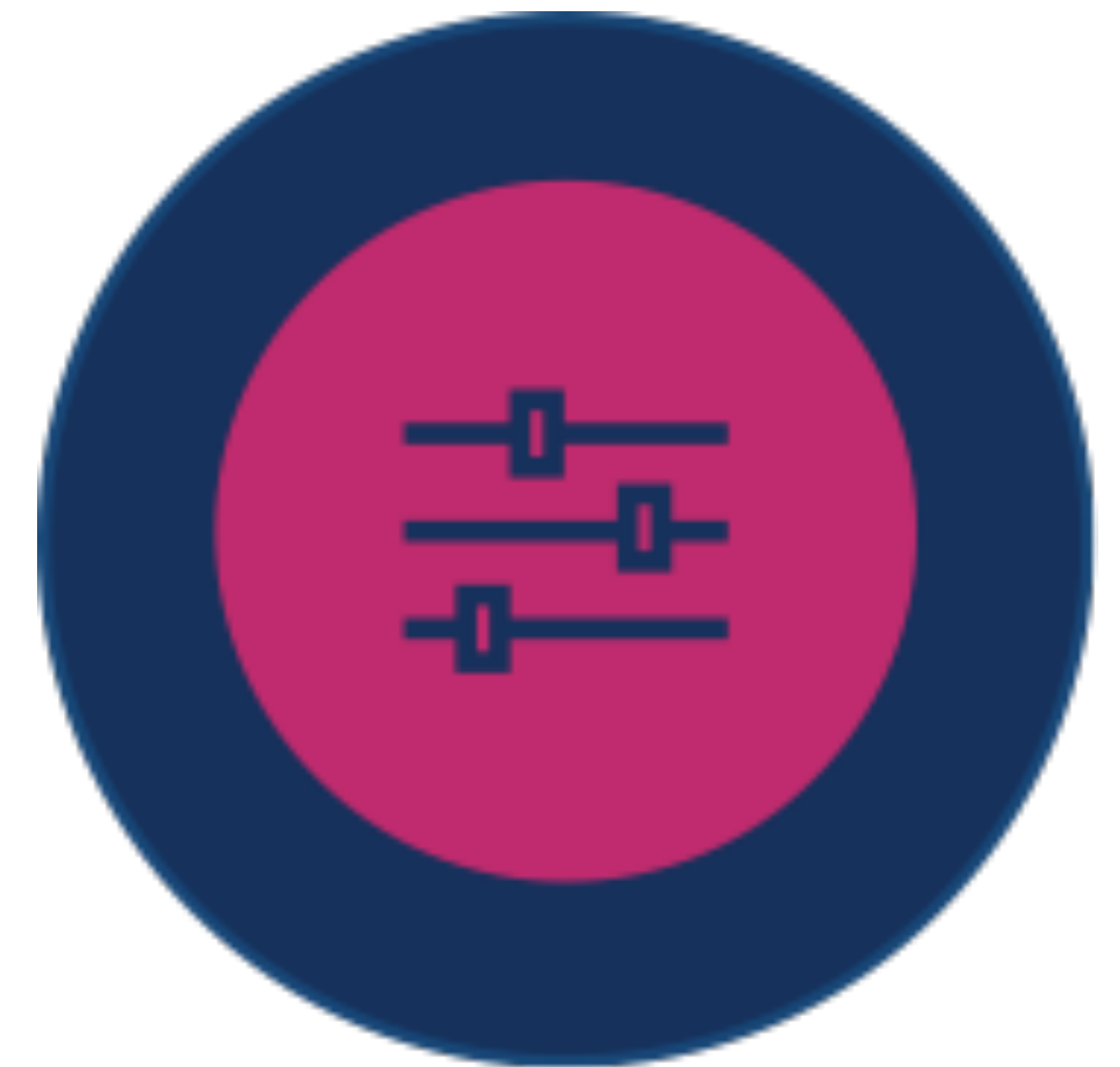


Artifacts for Practical Application

If your Content Audit does not provide essential artifacts for:

- Really great Search
- Really relevant Personalization

Then you're doing something wrong.



Search

- Native search available in your application
- It should actually work
- Exposed filters to help visitors drill down
- Faceted search that aligns with your content tagging and navigation
- Will actually find all the things
- Smart – auto populates
- Fast – consistently quick results
- Capable of learning – tracks session data to progressively enhancement results




Personalization

- An important part of putting your visitors in the center of your story – not the only part.
- A good content audit will serve as the basis for a robust personalization program that offers up customized display of your information in real time.
- Use the audit to identify opportunities for the personalization of your content.



A baby wearing a green hoodie is crawling through a yellow, circular tunnel. The baby is looking towards the camera with a slight smile. The tunnel is brightly lit, creating a warm, yellow glow.

You can use your audits to help you start generating memorable experiences that will improve customer experience.



**Its all about
starting with that
base
line**

Customer Experience Strategies

**UX Audit Strategies to Improve Customer
Experience SEO and Conversion**

The UX Audit

Of all the methods used to improve customer experience, SEO and conversion rates, Usability and User Experience Optimization may be the least understood and most difficult to manage.

Audit your site's UX to create web applications designed to increase visitor conversion and build SEO.

Understanding UX

- it's not just the UI
- UX is a combination of things

Designing the Product

UI



Designing the Experience

UX



Measuring the Usability

Usability



Hellmann's is eliminating **mayo lovers' frustrations** using a new-and-improved squeeze bottle that's designed to squeeze more out with less waste, less mess and more control. The innovative new bottle comes with three main improvements for a **better squeeze experience:**

- Precision tip: The angled tip enables more control and better precision so mayonnaise dispenses where you want it.
- Clean-lock cap: With a new customized cap that stays clean, there's no need to worry about messy surprises when opening and closing the bottle.
- Sleek new design: The improved bottle design offers ease of use with proprietary technology that helps squeeze more mayonnaise out than ever before.



By Packaging Digest Staff in Food Packaging on March 24, 2015

Bad UX Makes Users Feel Trapped

...and never want to come back



User Experiences are Evolutionary

UX:

- Is not static
- Is influenced by external factors and trends
- Gets old





The experience economy



Commodity
1-2 ¢/cup



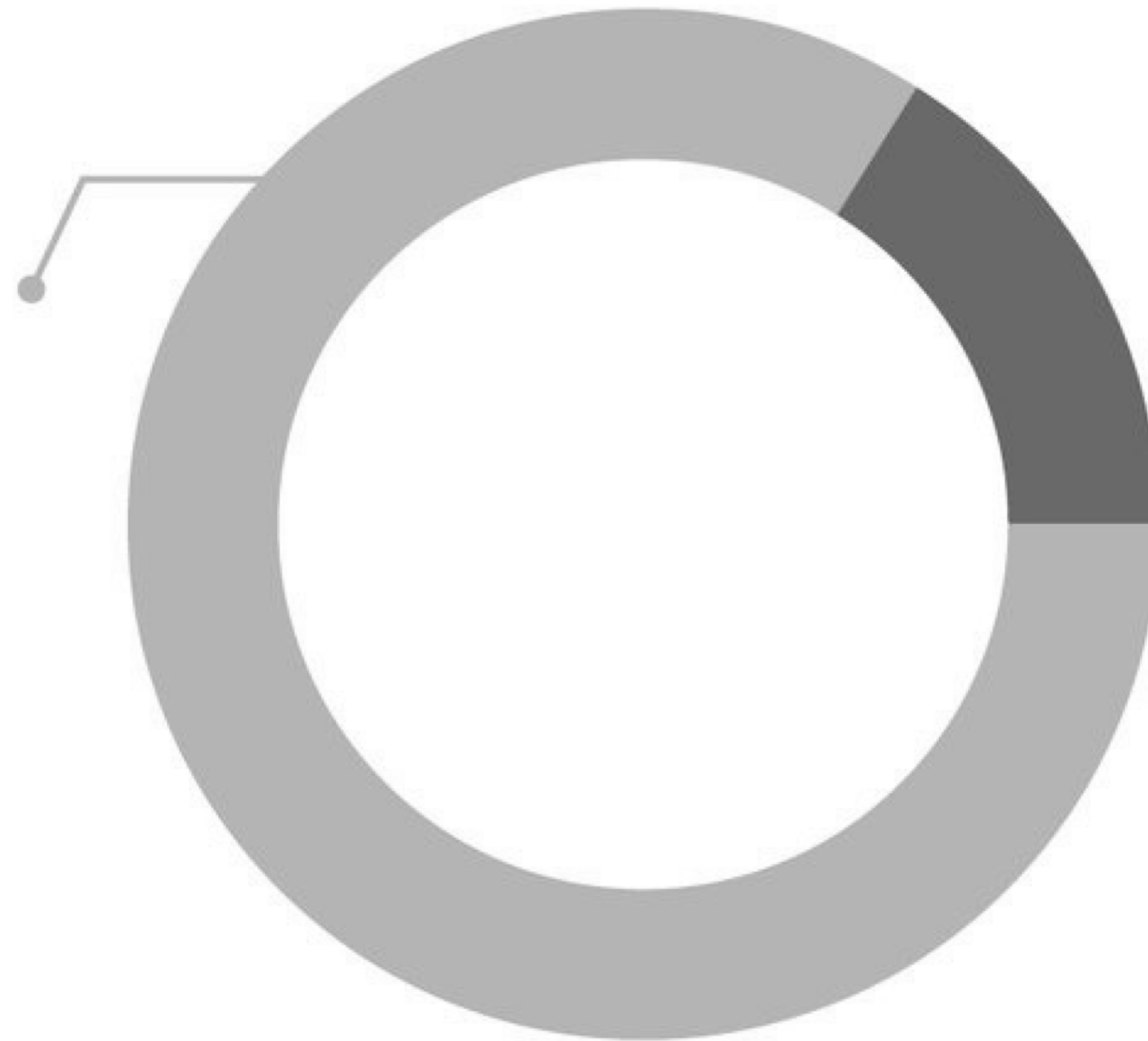
Goods
5-25¢/cup



Experience
2-5 \$/cup

In 1975 intangible assets accounted for 16% of corporate value.

**Today it is
87%**



<http://www.everedgeglobal.com/>

UX Audit Strategies

If it's intangible, how do you measure it?

Measure:

the **solution**

processes and **authentic outcomes**

by tracking **performance indicators** that are **objective**
and **independently verifiable**

by collecting **normative** and **outlier** stories of
subjective experiences according to your **target**
personas



“UX is the intangible design of a strategy that brings us to a **solution.**”

Bruno Mendes

Front End Developer, UI/UX Designer

What to measure?

Examine what is necessary for your organization.

Quantitative Data – metrics that align with your goals: analytics, heatmaps, social media tracking, server-side stats

Qualitative Data – demographics, feedback, search terms, spent ad info

Accessibility Testing Performance

UI and UX Obvious Pain Points, Newly Discovered Pain Points

Information Architecture – findability, discoverability, reading levels, CTA and menu labeling,

Branding Consistency

Performance

Also...

- Your audit report should include an overview with descriptions of definitions, objectives and artifacts, sometimes a competitor analysis
- And of course it should include a carefully constructed set of Recommendations

When? Early and Often

Before, During and After...**a project**

- After Discovery
- Before UI Design
- ...before...
- *Sketching*
- *Wireframing*
- *Interactive Wireframing*
- *Prototyping*

Before, During and After...**a problem**

- **Conduct a mini UX audit with an appropriate structure for both problems and solutions**

Orgs with a UX Team...

- **...audit on an ongoing basis**

Are you auditing what's not there?

You should be.

Missing features get added in, when will you assess their usability?



Collect Actionable Data

Customer Analytics

- Revenue
- Satisfaction
- Profitability
- Lifetime Value
- Loyalty
- Brand Awareness
- Top Tasks
- Conversion Rate
- Completion Rate
- Churn Rate

Don't Miss Your User Signals

Search engines are ranking processes and outcomes like User Signals.

User signals are user patterns that search engines like Google use to rank your site.

What signals are you being sent by your users? Are you measuring your performance?

Search Sequence: Focus on the inside of your web site. Are you creating and reviewing site search logs?

Content Quality: If a page on your site comes up in a Google search and the user bounces right back to the search results, they know it and take it as a signal that your content quality is not to their liking. That hurts your ranking.

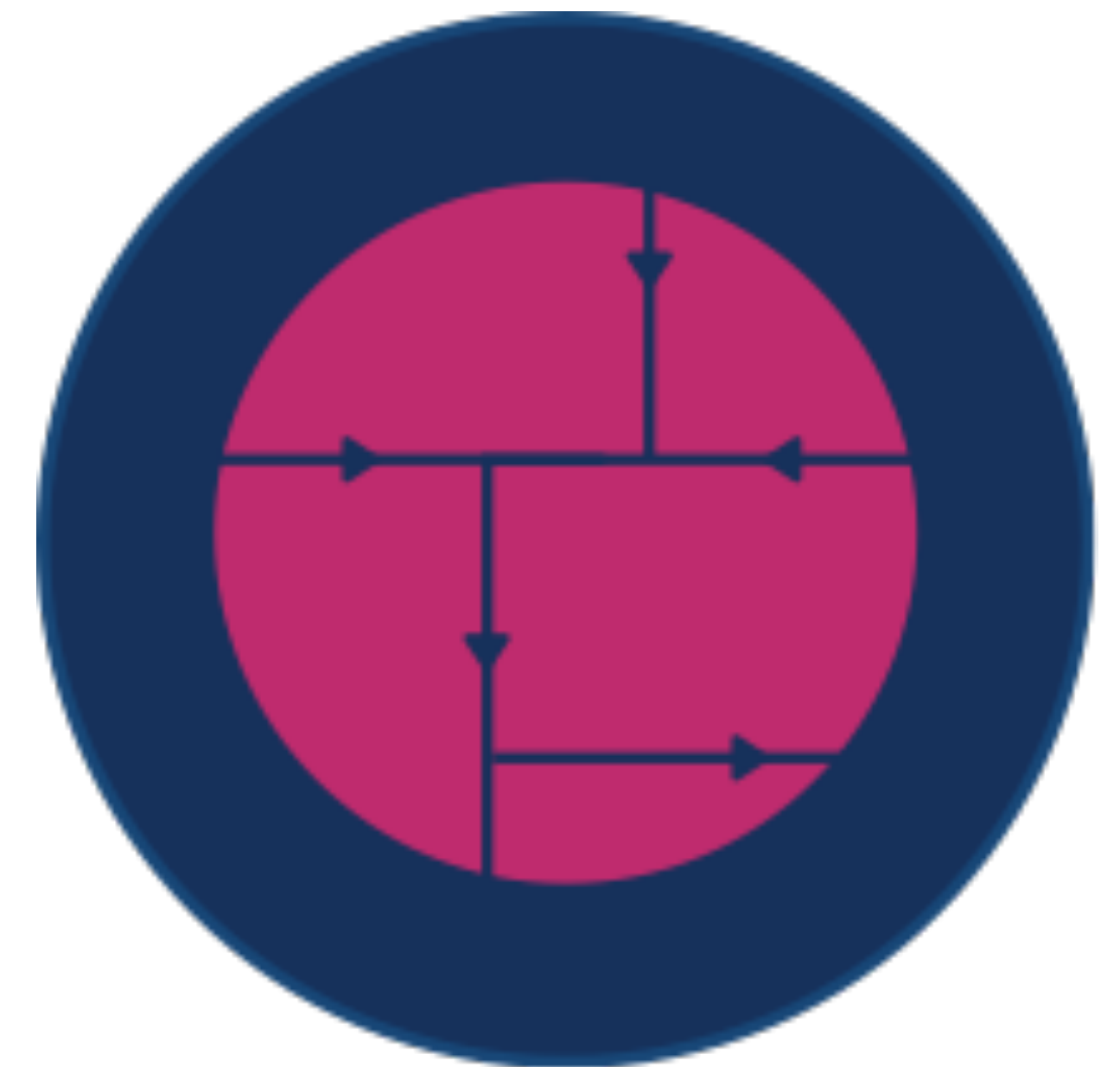
Structure: Users aren't linear and won't always land on your home page. Can they find what they searched for on your page? Is it buried or hidden? Are they able to easily find and navigate to other useful information from an inside page?

Sentiment: Are you well liked? It makes a difference. Social likes, thumbs up, shares, follows are all tracked, both negative feedback and positive.

Are you measuring what's elsewhere?

Sometimes, what you can't see is just as important as what you can.

- If your goal is increased SEO and conversion a UX audit should assess titles, meta-descriptions, header tags and alt-tags. Your recommendations should include a plan for optimizing items which are usually not seen but should still be found by search engines.
- Do you have awesome content like press releases buried in PDF's that can't be searched? Making your pdf content searchable or converting it to text can make a huge difference.
- Off site things like integrations, videos, social sharing, links from other sites and online magazines or feeds can also make a big difference and can be overlooked in your UX audit if you are not careful.



Take Homes
Resources
Tools and Training

Take Homes - Essential Strategy Checklist

Confirm the tactics and methods your UX team will use to ensure these strategies are prioritized.

- ✓ Great UX begins with putting users in the center of the experience. How will your UX audit keep users at it's center?
- ✓ You don't create a great user experience without a thorough understanding of your existing users and the users you want to attract. What steps will you take in your UX audit to get to know their personas?
- ✓ Validate your assumptions. What steps will your UX audit take to ensure they are accurate?
- ✓ Real users are not one dimensional and will have many needs. How will your UX audit surface and track the multi dimensional needs of your personas?
- ✓ Be prepared to engage with your visitors over time. Will your UX audit help you build a relationship?
- ✓ Markets and user needs change. What parts of your UX audit will help you be consistent and adaptive throughout a sales cycle or other lifespan.
- ✓ Optimal UX is the effective implementation of a design of an awesome solution that exceeds the expectations of all your users on an ongoing basis. Have you structured your UX audit to provide you with the recommendations you need to take your next steps?

Take Homes - Essential Strategy Checklist

...continued

- ✓ Stakeholders need to be involved in your UX audit. Have you left anyone out?
- ✓ Don't be tripped up by the basics. Have you taken steps to help everyone on your team understand the process?
- ✓ Timing is everything. Will all your UX testing and recommendations be complete before you begin designing your solution?
- ✓ Usability testing of features that are not in production is hard. Do you have a plan to make sure new features are audited properly?
- ✓ Data is only useful if it is actionable. Are you structuring your data collection to to make sure you will have a clear set of next steps to outline in your recommendations?
- ✓ New SEO algorithms for user signals are always being developed. Have you checked Google's latest?
- ✓ Not all your user interactions will be hosted on your site. Do you have a plan to manage UX for your integrations?
- ✓ UX needs can outpace organizational capacity and current technology. Is your organization prepared to prioritize and/or begin to make changes?

Take Homes - Artifacts Checklist

Build artifact templates that connect and prioritize your audit strategies. Can you see your strategies being operationalized from the artifacts produced during you UX audit?

- ✓ Capture user requirements for audiences, consider your sales cycle, visitor tasks and metrics. **Will your UX Audit define these accurately and precisely?**
- ✓ Track user journeys over time to plot points during their journey. **Will you be using a longitudinal user journey?**

Take Homes - Resources

Whitepapers

The Marketer's Guide to Atomic Design

<https://ffwagency.com/resources>

Don't Miss the Mark: Responsive Design & Content

<https://ffwagency.com/resources>

Blogs and More

For weekly posts on the latest in digital strategy, how-to and training, visit us at ffwagency.com/digital-strategies-blog



Take Homes - Some Tools

There's a lot of overlap between different tools. The best tool set is the one that fits your organization's needs and capacity. Do you need a tool set that will integrate with other tools and processes? Make that part of your selection criteria. Slack? Jira? Basecamp? Invision? Sketch? (FYI - We're not including the multitude of design and prototyping tools.)

Analytics Some analytics vendors offer powerful suites that can track data, conduct surveys, make recordings, create heatmaps, do A/B testing and are very mobile friendly. Vendors: Kissmetrics, Google Analytics, Woopra, Heap, Clicktale

Heatmaps Heatmaps are valuable tools used to track a user's activity on your pages. Use it to monitor things like cursor activity - movement, clicks and scanning activity. Vendors: HotJar, Crazy Egg, Chalkmark, Looktracker

Testing Make sure you choose tools that will focus on mobile interactions. Vendors: Usabilla, Mixpanel, Userlytics, Lookback, Apsee, Optimizely, Access Analytics, BOIA WCAG 2.0 AA Report

BI, Organization, Visualization Sometimes you need extra help, a little or alot. Vendors: Airtable, SmartSheet, Domo, Tableau

UX is a Journey Too

*Find the journey's end in
every step of the road.*

Ralph Waldo Emerson


*Life is a journey, not a
destination.*

Steven Tyler and Richie Supa



You can use an audit
to help you improve
UX and customer
experience.





**Its all about
starting with that
base
line**

Customer Experience Strategies

**Accessibility Audit Strategies to Ensure
Continuous Compliance and Strengthen
Customer Experience**

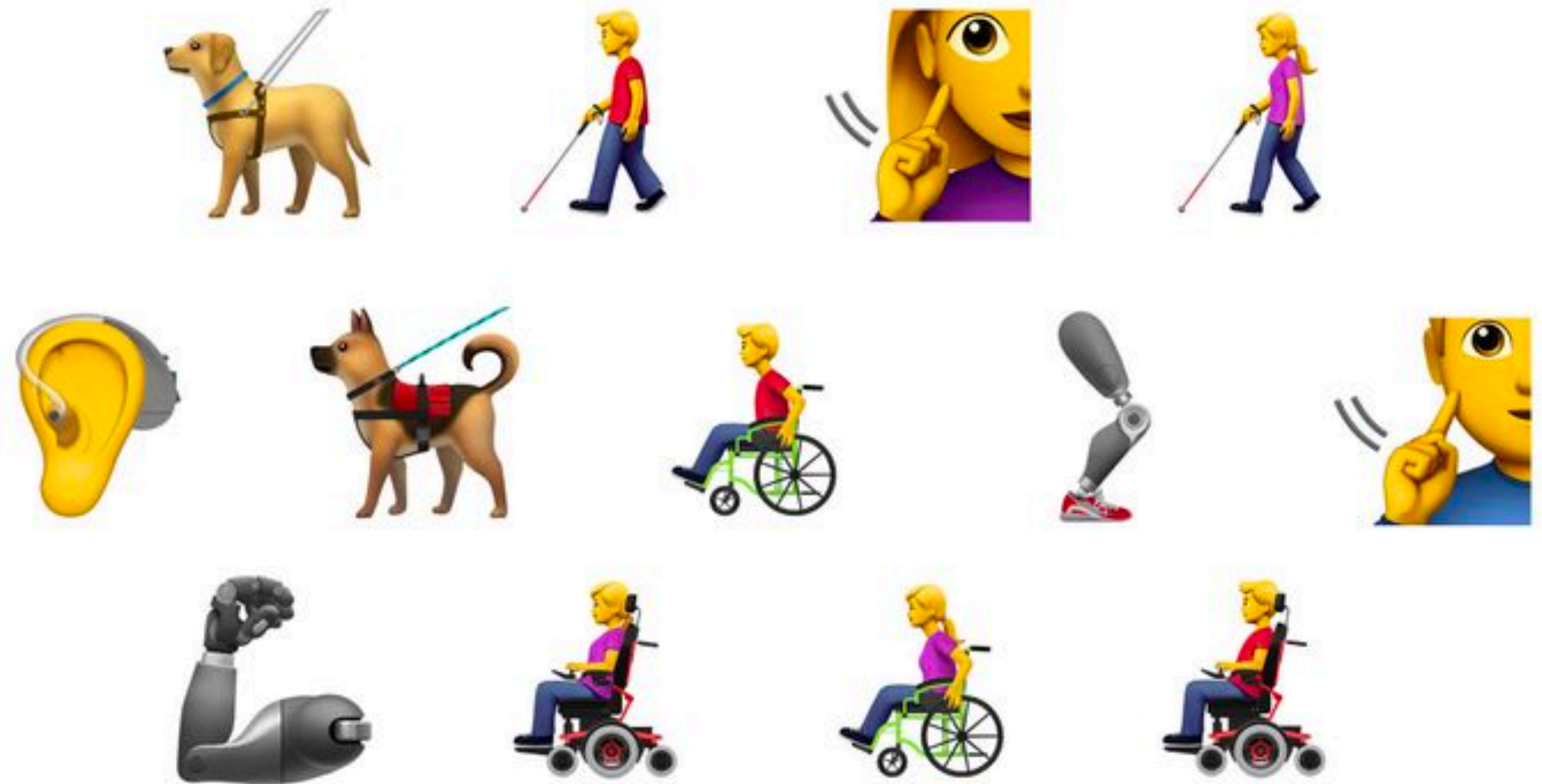
The Accessibility Audit

Accessibility planning and compliance is an important and often-neglected aspect of digital strategy and customer experience. Failing to comply with accessibility standards is a serious problem for users and property owners from all segments.

Audit your accessibility levels, prepare for increased performance and create systems that will help **ensure continued accessibility and promote digital inclusion.**

Welcome

Apple worked with the American Council of the Blind, the Cerebral Palsy Foundation and the National Association of the Deaf to develop the disability-specific emoji.



Web Accessibility

- Visual
- Motor/Mobility
- Auditory
- Seizures
- Cognitive/Intellectual

At a Glance

- **It is estimated that as many as 10 million Americans are blind or visually impaired.**
- **Studies show that over the next 30 years aging baby boomers will double the current number of blind or visually impaired Americans.**
- **Approximately 15% of American adults (37.5 million) aged 18 and over report some trouble hearing.**

Best Practices for Accessible Content

When creating digital content, make sure to consider the following:

- Do not rely on **color** as a navigational tool or as the sole way to differentiate items
- Images should include **Alt text** in the markup/code; complex images should have more extensive descriptions near the image (perhaps as a caption or descriptive summaries built right into a neighboring paragraph)
- **Functionality** should be accessible through mouse and keyboard and be tagged to work with voice-control systems
- Provide **transcripts** for podcasts
- If you have a video on your site, you must provide visual access to the audio information through **in-sync captioning**
- Sites should have a **skip navigation** feature
- Consider **508 testing** to assure your site is in compliance

Measurement Tools and Resources

Take Homes – Useful Links and other Tools

There's a lot of overlap between different tools. The best tool set is the one that fits your organization's needs and capacity. Do you need a tool set that will integrate with other tools and processes? Make that part of your selection criteria.

General Resources:

- Siteimprove.com
- w3.org/TR/UNDERSTANDING-WCAG20/
- Section508.gov
- WebAim.org
- Section 508 of the Rehabilitation Act full text
- Access for People with Disabilities
- HHS Digital Communications Division's Section 508 Resources
- <http://www.d.umn.edu/itss/training/online/webdesign/accessibility.html>
- <https://webaim.org/resources/>
- <https://www.levelaccess.com/>
- <https://usablenet.com/>
- Universal Design for Web Applications by Wendy Chisholm & Matt May

Take Homes – Useful Links and other Tools

General Testers:

- Siteimprove.com
- <http://bit.ly/firefox-toolbar>
- <http://wave.webaim.org/>
- <https://developer.paciellogroup.com/resources/aviewer/>

Color Testers:

- <https://developer.paciellogroup.com/resources/contrastanalyser/>
- <https://www.joedolson.com/tools/color-contrast-tester.php>
- <https://www.joedolson.com/tools/color-contrast.php?type=hex&color=%23FFFFFF&color2=%23333333&alpha=>

Screen Reader Tools:

- <http://www.nvda-project.org/>
- <http://bit.ly/jaws-reader>

Take Homes – Useful Links and other Tools

Code and Markup Validators:

- <http://validator.w3.org/>
- <http://jigsaw.w3.org/css-validator/>
- <http://bit.ly/vBKMyy>
- <http://bit.ly/w02s3J>

Other:

- <https://www.apple.com/accessibility/mac/>

Content Creation Practices and Workflows

Content
Creation
Practices
and
Workflows

Atomic Design



Content Creation Practices and Workflows

Atomic design is a phrase used to describe the practice of building a framework for making design decisions. Atomic design is a philosophy that breaks sites down to their smallest components, standardizes each piece, and then builds back up with increasingly larger, reusable-components.

Content Creation Practices and Workflows

What is the Unity Framework?

The purpose of this project is to provide a set of flexible and reusable UI components designed to work across browsers, devices and screen sizes. This project is meant to be platform agnostic, meaning it should work equally well across different CMS platforms as well as on static sites.

The project is maintained by DoIT Communications staff, primarily for use on projects we manage, but we see value in sharing our work and collaborating with the University at large as such we will make regular releases and keep the source code available through our GitHub.

We use a variety of open source technologies and methodologies to help keep us inline with industry and design trends. These technologies include: SASS, GULP, Pattern Lab, Web Fonts and several opensource CSS and JS Libraries including Bootstrap, AnimateCSS, and Breakpoint.

Motivations

Stony Brook University's web presence is enormous and is only growing larger. Branding, styling and accessibility compliance across our web properties is inconsistent (at best). And we are seeing an increase in the number of mobile computing devices.

Many departments, teams and individuals (faculty, staff and students) have a need for a web presence, often times the work of maintaining the web server, creating the sites design, developing the information architecture and maintaining its content falls on one person, with varying ability in this area and who is often overwhelmed by the amount of work required to properly maintain a large site.

Our current web dev support model is inefficient. Our teams cannot easily take

Goals

This project pledges that to the best of our ability, sites using this theme and following the guidelines provided will:

- Provide a great experience to desktop, widescreen and mobile users
- Fully Support Modern Browsers (IE10, Chrome, FF, Safari)
- Be built upon modern UX and Design Tools
- Follow University Branding Guidelines
- Be Section 508 Compliant
- Degrade Nicely on legacy browsers
- Be backend independent

<https://unity.it.stonybrook.edu/>

<https://www.linkedin.com/in/sbubaron/>

Visit
ffwagency.com/learning
to download our eBook.


The Marketer's Guide to

ATOMIC DESIGN

a faster way to build and manage your digital brand



**Audits are essential to accessibility
compliance, digital inclusion and
customer experience.**



**Its all about
starting with that
base
line**

Customer Experience Strategies

**Security Audit Strategies to Protect Your
Data and Improve Customer Experience**

The Security Audit

With high profile security breaches frequently in the news, what steps can organizations take to ensure their data is as safe as it can be and mitigate problems when breaches do happen?

There is no better way to of creating and positive customer experience than in being able to convey to your visitors that they are save.

Audit your security policies, procedures and systems with a mind toward practical everyday practices that help **manage vulnerabilities and harden applications.**

A computer security audit is a manual or systematic measurable technical assessment of a system or application. Manual assessments include interviewing staff, performing security vulnerability scans, reviewing application and operating system access controls, and analyzing physical access to the systems.

wikipedia

The Security Breach...

...is just the beginning of your problems.



“A security breach is any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. A security breach occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical IT perimeter.”

“A security breach is one of the earliest stages of a security attack by a malicious intruder, such as a hacker, cracker or nefarious application. ”

CIA

The IT Security Triad Model

Confidentiality is the term used to prevent the disclosure of information to unauthorized individuals or systems (Y. and oon Kim, 2007)

Integrity refers to the protection of information from unauthorized modification or destruction. Ensuring integrity is ensuring that information and information systems are accurate, complete and uncorrupted (Y. and hoon Kim, 2007)

Availability refers to the protection of information and information systems from unauthorized disruption. Ensuring availability is ensuring timely and reliable access to and use of information and information systems(Y. and hoon Kim, 2007)



Policies Matter

Security policies are the foundation and the bottom line of information security in an organization.

A well written and implemented policy contains sufficient information on what must be done to protect information and people in the organization (SAAN, 2015).

Security policies also establish computer usage guidelines for staff in the course of their job duties (SAAN, 2015).

Information Security policy defines the framework for how to use information and information systems.

But...

The 90 / 10 Rule

10% of security safeguards are technical.

90% of security safeguards rely on the user to adhere to good computing practices.

*University of California Santa Cruz

People Matter Even More

The lock on the door is the 10%.

You remembering to lock the lock, checking to see if the door is closed, ensuring others do not prop the door open, keeping control of the keys, etc. is the 90%. You need both parts for effective security.

*University of California Santa Cruz

At a Glance

Global Data Breaches in 2017

- **419 companies in 13 country or regional samples**
- **\$3.62 million is the average total cost of data breach**
- **27.7% is the likelihood of a recurring material data breach over the next two years**

* Benchmark research sponsored by IBM Security Independently conducted by Ponemon Institute LLC June 2017

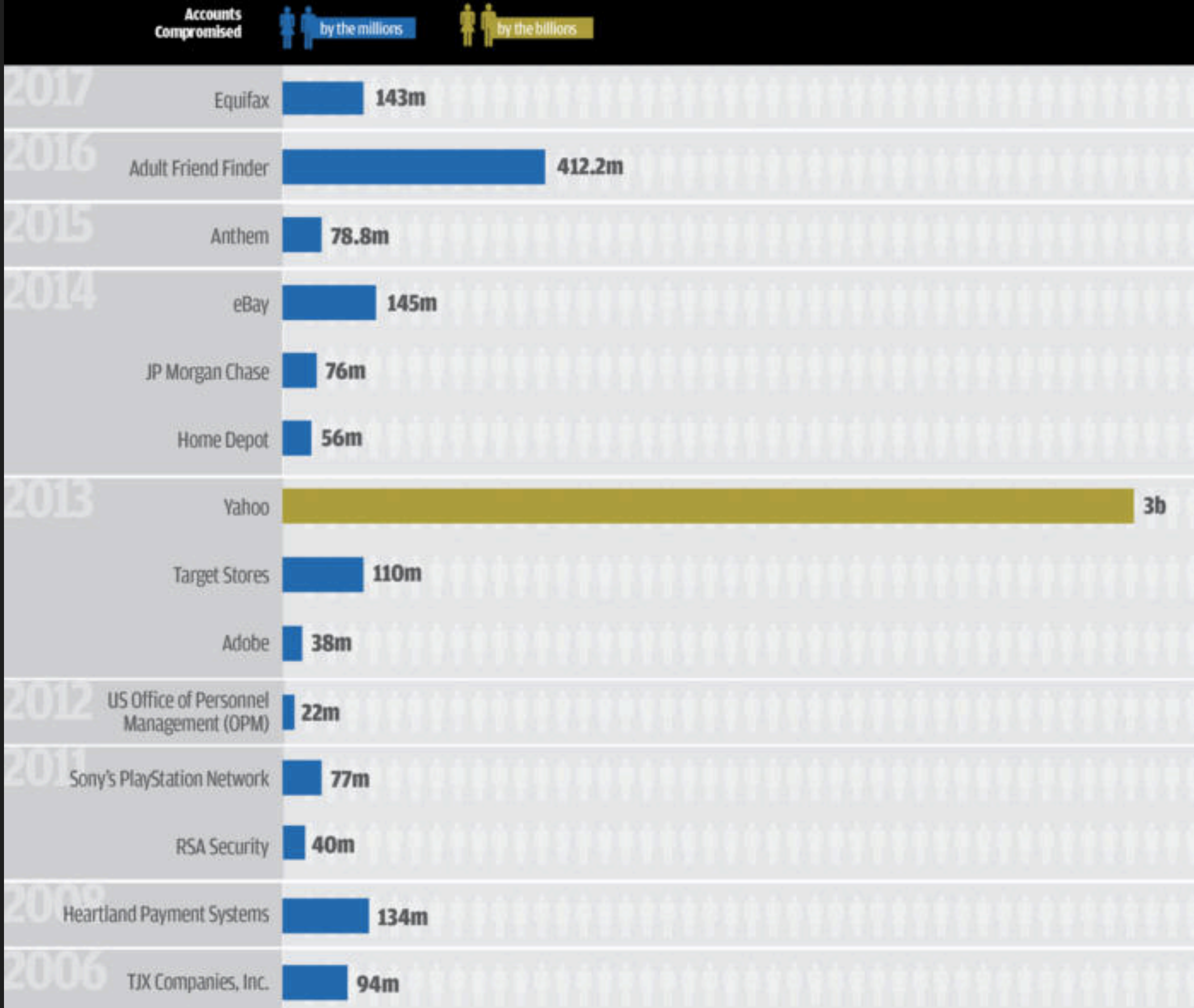


At a Glance

**Big Data Means
Potential Big Data Loses
And Even More
Potential Big Data Loses**

**Because so much more data is
constantly being mined and analyzed
and stored.**

Biggest DATA BREACHES of the 21st Century



Vulnerabilities

- **Websites**
- **Web applications**
- **Mobile Applications**
- **APIs**
- **Additional Channels**
 - **Mobile applications**
 - **Kiosks**
 - **Digital Signage**
- **Third Party Applications**
- **Internet of Things**
- **Identity Theft**

Master of your Realms

Code Realm - The thing that runs. Coding standards. Code updates.

Storage Realm - Data, Meta Data, Content, Configuration Data - What, Where and How? GoDaddy? Plain text?

Transit Realm - Does your data have secure passage? Is it passed through someone else's network?

Outer Realms - 3rd party servers/software - who's responsible, who updates?

Remember, It's all about the Base(line)

You can't effectively measure security unless you are measuring it against an established baseline.

Because security threats evolve on a daily basis you have to have a system to continuously measure progress.

Once you've established a baseline – pick it apart to make sure the assumptions and findings are correct. Hire a different auditor or seek a different opinion.*

Know What You Want

What's the job description for your audit firm? It's fine to accept guidance from your auditor but you are responsible and therefore you are in charge. Do your homework and make sure you clearly explain what you are seeking. Work collaboratively but make sure you get what you need from your audit.*

Jack or Jill in IT can't do your audit.

Internal IT staff has too much to do. They just do. Between updates and configuration requests and monitoring and other tickets they've more than likely got a full load. You will certainly need them to participate in the audit. Asking them to take on more responsibility will undermine your daily operations as well as your audit. Don't do it.

Hire an auditing team with the right security credentials but don't rely on certifications to ensure results. Make sure they have real world experience and a track record of helping organizations like yours.*

Do a real Audit.

A real audit is a full security assessment review that includes penetration testing and a review of policies and procedures and their implementation. So called Black Box Audit services are a far cry from a careful collaborative process with experience auditors. In many cases they provide a false sense of security. Real hackers don't care about damaging your system. A black box vendor routine will never be as penetrating as a real attack and will instead deliver very general results that are less actionable.*

Set Ground Rules

Because your audit will naturally deal with the most sensitive aspects of your information it is essential you set clear ground rules for communication and engagement.

How will you transfer sensitive credentials?

Specify restrictions on what testing will be performed when. There is no point to having a system grind to a halt or fail because it is being tested during peak load time.

Auditor should conform to your policies for handling proprietary information.

Alert your ISP or hosts that you are undergoing an audit. You may even need to give your auditors an indemnification statement.*

Give them what they need.

Speed things up by giving your auditors what they need to do their job.

- **Copies of Policies and Procedures**
- **Lists of OSeS and other application software**
- **Network and application topology**
- **External security, caching or CDN devices or services***

Get a Good Report Even if it's Bad

Specify in advance the format for your Audit Report and the level of detail you expect to see. Generic lists that could be for any organization will not be helpful. The report should reflect your organizations actual vulnerabilities as specifically as possible. Such as:

- Threat source**
- Exploitation probability**
- Impact of exposure**
- Actions to fix the problem**
- Legal liability**
- Risk of service interruption**

OWASP Top 10's

<https://www.owasp.org>

Avoid These At All Costs

A1:2017- Injection

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

A2:2017-Broken Authentication

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

A3:2017- Sensitive Data Exposure

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

A4:2017-XML External Entities (XXE)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

A5:2017-Broken Access Control

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

Avoid These At All Costs

A6:2017-Security Misconfiguration

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.

A7:2017-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

A8:2017-Insecure Deserialization

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

A9:2017-Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

A10:2017-Insufficient Logging & Monitoring

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

Do These All the Time

- 1. Verify for Security Early and Often**
- 2. Parameterize Queries**
- 3. Encode Data**
- 4. Validate All Inputs**
- 5. Implement Identity and Authentication Controls**
- 6. Implement Appropriate Access Controls**
- 7. Protect Data**
- 8. Implement Logging and Intrusion Detection**
- 9. Leverage Security Frameworks and Libraries**
- 10. Error and Exception Handling**

Remember, Don't Fear the Audit



"WE DON'T WANT YOU TO VIEW THIS AUDIT COMMITTEE AS BEING IN ANY WAY CONFRONTATIONAL"



**KEEP
CALM
AND
EMBRACE
THE SUCK**

A woman with long blonde hair and a floral headband featuring white and peach roses looks directly at the camera with a wide-eyed, surprised expression. She is wearing a pink and white striped top with a light blue bow at the collar. Her hands are raised, showing blue and yellow nail polish and a large ring. The background is a solid pink wall, and other people in party attire are partially visible around her.

I'm so glad we've had this time together.

Give us a call

USA:

+1 (732) 792 6566

Denmark:

+45 66 11 00 00

United Kingdom:

+44 (0)1304 806908

Germany:

+49 (0)30 293 81 370

France:

+33 (0)3 90 20 03 02

Thank you!

"I really liked how we were able to customize the course to our needs.."

Chris Payne - formerly Senior Director, Technology, "The Golf Channel"

Please send us your feedback and suggestions at
<https://bit.ly/30WxrZ2>



(732) 792 6566 | ffwagency.com/learning | training@ffwagency.com