

Whitepaper

SIMPLIFY, STRENGTHEN, AND STREAMLINE IN-HOUSE E-DISCOVERY

Scott Van Nice, E-Discovery Manager, Procter & Gamble

EXECUTIVE SUMMARY	3
ABOUT THE AUTHOR	4
ABOUT THE COMPANY	4
INTRODUCTION: DO MORE WITH LESS	4
FINE-TUNE IN-HOUSE E-DISCOVERY RESPONSIBILITIES	5
1. 30(b)(6) Witness	5
2. Technical Mastery	5
3. Vendor Management	5
4. Service delivery	6
5. Stewardship	6
IDENTIFY WHERE YOU PLAY... AND DON'T PLAY	6
FIND THE RIGHT SERVICE PROVIDER	7
Points to Consider when Selecting a Service Provider	8
STAY BALANCED WITH CASE MANAGEMENT, E-DISCOVERY BOARD AND MEASUREMENTS	9
Case Management	9
E-Discovery Governance Board	10
Measurements	11
What to Measure	12
Internal vs. External Scorecards	12
IMPLEMENT AN ESI POLICY	13
CONCLUSION	14



EXECUTIVE SUMMARY

As the roles and responsibilities associated with e-discovery teams swell with the tidal wave of new requirements such as social media, “bring your own device” (BYOD), big data, cloud computing, globalization and more, corporations are realizing that their litigation arsenal requires more than just new service partners, software or tools. For some companies, a holistic approach to e-discovery has helped them to simplify, strengthen, and streamline the process altogether.

The benefits of in-house e-discovery are becoming more obvious and compelling: efficiency, consistency, transparency, and cost savings, to name a few. On the other hand, there are risks and challenges. Creating and managing an e-discovery operation demands a collaborative corporate culture—one that engages all business groups that are impacted on the litigation battlefield.

This case study explores how Procter & Gamble (P&G), the world’s largest consumer goods company, tackled a hefty in-house e-discovery process with a lean team of two. It presents a bold plan that enabled P&G to revamp its e-discovery model resulting in reducing its e-discovery spend by 50 percent in the first eight months and reduced a four- to six-week case start-up time to just two days.

Written by an e-discovery veteran who built P&G’s in-house electronic discovery process eight years ago, this blueprint can serve as a tactical plan for a company that wants to create a new e-discovery process or calibrate an existing one. To be clear, there are two things this paper is not:

1. This isn’t an e-discovery “how to” paper, as there is a plethora of educational resources available to fit every unique need for professional training and certification on the legal and technological requirements for data investigations
2. This isn’t a white paper on why to bring e-discovery in-house, as the author saves time by assuming the audience has already waded through the pros and cons of in-house vs. outsourcing, and has landed on the consensus that in-house e-discovery is a good fit.

This paper addresses the organizational structure put in place by P&G to simplify, strengthen, and streamline its e-discovery process, including how to:

- Mobilize teams for rapid response
- Identify and fine-tune responsibilities
- Measure service delivery expectations
- Nurture cross-team collaboration
- Select and manage vendors

ABOUT THE AUTHOR

Scott Van Nice is the e-discovery manager at Procter & Gamble. He has been with P&G for 14 years and has managed an e-discovery forensics program for the past seven years. What is unusual about the in-house program for a Fortune 50 company is that it's composed of just two people, but has proven to be effective on a global scale with an average of 30 to 40 cases per year.

Scott has a Bachelor of Science degree in information technology from Rochester Institute of Technology. He has a Juris Doctorate from Salmon P. Chase College of Law at Northern Kentucky University and is licensed to practice law in Ohio. He is pursuing a master's degree in informatics from Northern Kentucky University and is certified by Guidance Software as a forensic investigator with EnCEP® and EnCE® certifications.

He teaches at University of Cincinnati as an adjunct professor, where he teaches *Legal Issues for the Deaf and Hard of Hearing and Digital Investigations in a Cyber World*. Finally, Scott is profoundly deaf and P&G provides him a dedicated sign language interpreter, Hunter Bryant.

ABOUT THE COMPANY

P&G serves nearly five billion people around the world with its brands. The company has one of the strongest portfolios of trusted, quality, leadership brands, including Always®, Ambi Pur®, Ariel®, Bounty®, Charmin®, Crest®, Dawn®, Downy®, Duracell®, Fairy®, Febreze®, Gain®, Gillette®, Head & Shoulders®, Lenor®, Olay®, Oral-B®, Pampers®, Pantene®, SK-II®, Tide®, Vicks®, Wella®, and Whisper®. The P&G community includes operations in approximately 70 countries worldwide. Please visit <http://www.pg.com> for the latest news and in-depth information about P&G and its brand.

INTRODUCTION: DO MORE WITH LESS

It's easy to correlate an in-house e-discovery operation to that of the Green Berets—a strategic, multipurpose squad whose mission it is to organize, train, equip, and direct teams in national defense. Forced to do more with less, this elite group hones attributes like teamwork, intellectual curiosity, and communications, and stays focused and fit for rapid response in times of uncertainties.

P&G chose to bring e-discovery in-house eight years ago when it became apparent that, with the right tools, training, and procedures, we could also be better prepared for rapid response, provide more consistency, sharpen our transparency—in effect, do more with less and save money at the same time. Always a lean operation, e-discovery at P&G was a one-person operation up until 18 months ago. Today, it is a tenacious, two-person team with roles divided between e-discovery and computer forensics, although we are cross-trained and able to provide reinforcement in either area as needed. P&G has the peace of mind to know that when a triggering event occurs, our rapid response team mobilizes and within 24 to 48 hours, begins to preserve and collect data.

It wasn't always this efficient, as it used to take four to six weeks to get a case up and running. And, in a perfect world for a large corporation with a global footprint, one should be operating an in-house e-discovery team of more than 20 people. But if done right, a company can create consistency and transparency while increasing timeliness by using this simple strategy: designate a few people to do the heavy lifting, select a preferred vendor for tasks not typically handled in-house, create a governance board to provide cross-practice cooperation, and engage a short list of niche vendors to help manage unexpected incidents that aren't considered e-discovery but have potential to become litigious and/or pose a high risk.

P&G's e-discovery operation accomplishes tasks far beyond its numbers. Ideally, this prototype can help other small, in-house e-discovery teams do the same.

TACTICAL TIP: KEEP THE TEAM SMALL

1	Designate a few people to do the heavy lifting
2	Create a culture of cooperation among relevant business units
3	Form a relationship with a preferred vendor for tasks not typically done in-house
4	Engage a short list of niche vendors to help manage the unexpected

FINE-TUNE IN-HOUSE E-DISCOVERY RESPONSIBILITIES

P&G has been successful with in-house e-discovery because the company recognized early on that this work was not simply an IT task, nor was it purely legal. The e-discovery team has always been considered relevant as opposed to marginalized, tactical as opposed to repetitive, and not just another "information security group."

The five strategic and multipurpose responsibilities for e-discovery practitioners at P&G are outlined here:

1. 30(b)(6) Witness

First and most importantly, the e-discovery professional is a company's 30(b)(6) witness. He or she should be able to testify how the company identifies data; what steps were taken to collect, preserve, and maintain the authenticity of the data; as well as maintain a chain of custody that's provided to counsel for review. This is the person who protects the company, serves as the company's true subject-matter expert, and makes what could be hard to understand become easy to understand by judges, counsel, or interested parties.

2. Technical Mastery

Secondly, an e-discovery manager is expected to have technical mastery. This doesn't mean he or she must know the intricacies of every operating system or tool, but should at least have a good understanding of how a computer works, how a handheld works and how the forensic products are used, as well as have his or her fingers on the pulse of the industry. The e-discovery manager must be ready to explain, in detail, how the technology was implemented and what steps were taken in the discovery.

3. Vendor Management

The reason why a two-person team works so well at P&G is because we tap into the expertise of vendors. We know who the right vendors are for specific cases. First, we have a preferred vendor for review, hosting, and production of our culled data and we have in-house and outside counsel work with that vendor and the vendor's review platform. This goes a long way in ensuring defensibility and repeatability over time as long as the right controls are in place. We have a list of tiered vendors, or niche vendors, that who can do their specific job quickly for situations that aren't classified as "e-discovery" in the formal sense but are, at the same time, high-risk and could become litigious. This is an important part of the recipe for success. Choose a few reputable vendors, give them a chance to earn your trust, and manage them well. They will work with you and for you to make your job easier.

Example - Technical Mastery: We recently faced the issue of how to best retrieve voicemail and text messages from a phone that was not in our physical possession. There are very few solutions that can do this efficiently. But, because we are connected within the industry and stay abreast of developments, we were able to find a niche tool to do the job. The solution, similar to iTunes in how the software captures the voicemails and text messages, was minimal. In testing it, we were able to demonstrate that it maintained the metadata and the authenticity of the data. Technical mastery, in this example, helped our e-discovery team be reactive and responsive at a moment's notice.



4. Service Delivery

Service delivery is a critical responsibility because the e-discovery team must be able to do the job required, with excellence, consistently. At the end of the day, zero sanctions is all about delivering the service well, and helping counsel to meet their deadlines and objectives to be unchallenged by opposing counsel.

5. Stewardship

And finally, the role of steward is foundational in all of the aforementioned e-discovery responsibilities. Synonyms of stewardship—guardianship, watchfulness, and vigilance—are at the heart of our job. E-discovery managers must take their role of protecting the company seriously.

We must be responsible stewards by identifying how to improve processes and operate smarter, faster, better, at all times.

TACTICAL TIP: FINE-TUNE E-DISCOVERY RESPONSIBILITIES	
1	FRCP 30(b)(6)
2	Technical mastery
3	Vendor management
4	Service delivery
5	Stewardship

IDENTIFY WHERE YOU PLAY... AND DON'T PLAY

A key to our success at P&G is that we have identified thresholds of what we will handle in-house and where we should still lean on trusted partners.

ELECTRONIC DISCOVERY REFERENCE MODEL

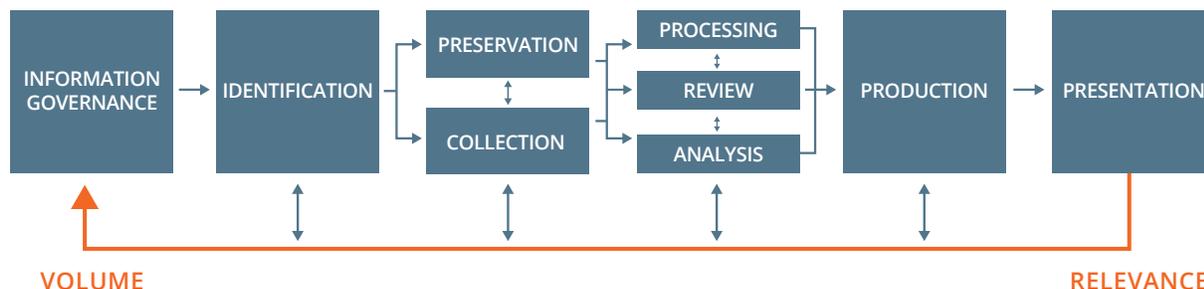


Figure 1: The Electronic Discovery Reference Model provides a framework for organizing e-discovery into more manageable stages and processes.

Example - Stewardship: When my colleague or I learn of a new P&G initiative that will be holding electronic data, we are proactive in reaching out to the responsible team. As the “guardians” of electronically stored information (ESI), it’s our job to advise them on the best ways to manage ESI, and why it’s important to have the right controls in place to identify, preserve, and collect data. We want them to understand what needs to be done so we aren’t caught off guard down the road.

The Electronic Discovery Reference Model^l (EDRM) allowed us to set the stage for our service, how to structure it, and how best to explain it to others. This model is often shared with senior management to clarify with them exactly what we do and don't do and what we have to offer: On the left side of the model is where our internal e-discovery team plays. On the right side of the model is where we have asked a vendor to play.

It's important to identify one or two service providers as your primary protection, like a crash helmet that becomes part of your daily armor. We have one for forensic identification, preservation, collection, and culling, and another who takes care of hosting, processing, and production. We keep niche partners to call into play for unique situations that require unique solutions.

Before we brought e-discovery in-house, we had to rely on multiple outside vendors. There was no consistency, policy or standard cost structure, and start-up time varied. It was not an ideal environment and not how P&G likes to operate. Standardizing our vendor partnerships has streamlined our operation.

TACTICAL TIP: SHARE THE STEPS IN THE EDRM MODEL

1	Identify where you play
2	Identify where your vendors play
3	Choose one or two vendors to serve as your primary "shield"
4	Keep niche players on call for unique situations
5	Streamline and standardize

FIND THE RIGHT SERVICE PROVIDER

How do you know which service provider to use for in-house e-discovery when there are so many solutions available? To find the best tools for P&G, we started with the EDRM diagram to identify where we play. Based on our team size, case load, corporate infrastructure, and other various factors, we decided to bring collection and preservation (the "left side" of EDRM) in-house, so focused our request for proposal (RFP) requirements there. For e-discovery and digital forensic activities, we use EnCase[®] Discovery v5ⁱⁱ and EnCase Enterprise v7ⁱⁱⁱ from Guidance Software.

The following figure displays statistics on our P&G e-discovery projects over the last six years. Prior to putting these numbers together, I assumed our cases were fairly large. This exercise was eye-opening, as it revealed that the majority of our cases are fairly small. EnCase is a good fit because we use it for key custodians; we collect a narrow set of potentially relevant data between five and seven gigabytes (GB) per custodian, and it enables us to quickly triage and filter the data. On the rare occasion we have a large number of custodians and data for discovery, EnCase has also proven to be scalable to meet our needs.

P&G E-DISCOVERY STATISTICS			
Year	Case Load	Custodians	Approx. GB*
2009	4	159	1,113 (1.1TB)
2010	21	170	1,190 (1.2TB)
2011	29	223	1,561 (1.5 TB)
2012	21	194	1,358 (1.4TB)
2013	6	120	1,595 (1.6TB)
2014	16	225	1,133 (1.1TB)

*Assume 7GB each custodian

- 69% of cases are fewer than 5 custodians
- 14% of cases are between 6 and 15 custodians
- 8% of cases are between 16 and 30 custodians
- <4% of cases are between 30 and 50 custodians
- <4% of cases are over 50 custodians
- 90% of e-discovery cases end within a year

Figure 2: P&G e-discovery statistics over a six-year period



When choosing an e-discovery product or tool, I envision the shield held by Captain America, the classic comic book superhero. The red, white, and blue shield is durable, reliable, powerful, and most important; it's an offensive weapon as much as it is a defensive one that can perform incomprehensible tricks. Fortunately for P&G, we found this capability in a few vendors, like Guidance Software, and depend on their products and services to achieve an efficient, repeatable, and defensible e-discovery process.

Before you jump into a request for proposal (RFP), understand the unique needs of your company. Remember how fast the industry is moving. Not too long ago, our digital investigations focused on a computer and email. Next, share drives were added. Now, as technology continually changes, we have new challenges involving social media, blogs, websites, servers, voicemail, handhelds, and so on. Become comfortable with how and where you need to preserve data, then find the shield that fits best.

Points to Consider when Selecting a Service Provider:

- **EDRM:** Where does your team play in the EDRM field? If you focus just on collection and preservation, you can narrow your search down to find a search and preservation tool.
- **Requests:** How many requests or threats do you get on an annual basis? This will determine the scope and offerings of the software you need
- **Clients:** Who are or will be your standard clients? For example, will you be working with the litigation group, or also with HR, information security, or cybersecurity? Different software products focus on different clients.
- **Collection:** Is collection usually done in person or remotely? If it's a small company, then you probably do it in person. But if you're a Fortune 500 company, you will often be asked to do collection remotely. If this is the case, the product or tool you buy must provide remote discovery options
- **Custodians:** What is your average number of custodians for each e-discovery case? If it varies from small cases to large, class action lawsuits, you'll need a solution that is scalable.
- **Qualifications:** What are the strengths and qualifications of the e-discovery team? Are they technologically savvy, attorneys, or paralegals? Some tools are very powerful and legally respected, but are not intuitive. Find the right product for your team's skill sets.
- **Verification:** Sometimes you need to employ an "unverified" solution for unique collection or verification needs. Be prepared to explain to the court how this niche product was repeatable, defensible, and peer-reviewed.

TACTICAL TIP: UNDERSTAND YOUR NEEDS BEFORE ISSUING A RFP

1	Where does your team play in the EDRM flow?
2	How many requests do you get per year?
3	Who are (or will be) your standard clients?
4	Is collection done in person or remotely?
5	What is the average number of custodians in each case?
6	What are the strengths and qualifications of your team?
7	Will you have a need for unverified products?

Example - Vendor Choice: Identifying a preferred vendor for all e-discovery cases helped us reduce our case start-up time by almost 95%, from a usual four weeks down to just one or two days. And within eight months of revamping our in-house e-discovery process, we realized significant savings that would otherwise have been spent on hiring consultants, outsourcing investigations, or using multiple vendors.

STAY BALANCED WITH CASE MANAGEMENT, E-DISCOVERY BOARD, AND MEASUREMENTS

Once it's clear where the e-discovery team and the chosen vendors play in the Electronic Discovery Reference Model, it's time to delineate internal team responsibilities and align cross-functional teams for tactical and efficient electronic discovery project management.

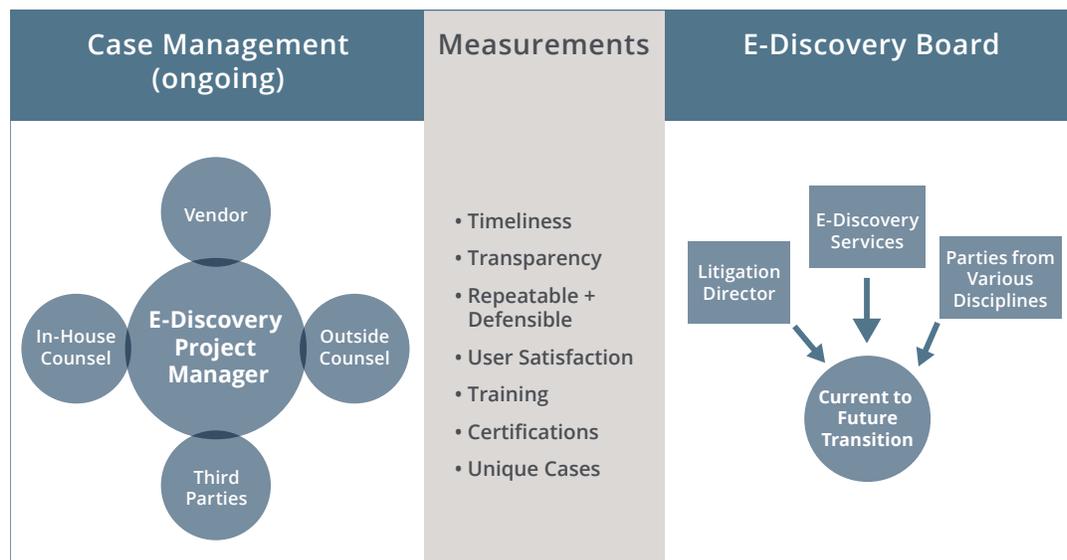


Figure 3: This P&G approach highlights the cross-functional relationships required for effective e-discovery

At P&G, we've divided e-discovery oversight into two buckets, case management (shown above on the left) and the e-discovery governance board (shown on the right). However, there's a third and complementary process—measurements—that is so intrinsic to both areas that we placed it in the middle of the process, as shown here.

Case Management

Case management encompasses the ongoing information governance and investigation activities that fall under the purview of the e-discovery project management team. Sometimes we work with inside counsel, outside counsel, or other third parties to accomplish all of the steps within the EDRM model. At the end of the day, however, the e-discovery manager owns the case and determines the execution in accordance with each specific project and game plan:

- How is the data going to be identified, collected and preserved?
- Do we cull the data with in-house, or do we need to hand the data over to a vendor?
- How is the production going to be handled?
- What will the privilege logs look like?

The e-discovery product manager is the 30(b)(6) witness, so needs to be at the center of everything. Even after the electronic discovery has been relinquished to another party for hosting or production, for example, it's important that e-discovery case managers are copied on all correspondence. That party needs to have exposure from start to finish in all conversations about the case if he or she is to be a reliable witness.

TACTICAL TIP: E-DISCOVERY PROJECT MANAGER OWNS THE CASE

1	E-discovery manager determines the steps and tools for e-discovery
2	E-discovery manager retains case exposure from start to finish



E-Discovery Governance Board

The E-Discovery Governance Board is a cross-function advisory group that provides governance, insight, and reinforcement, keeping us focused on our mission, and ensuring that the right level of support is available to the e-discovery team when and if needed. It also complements our job as a watchtower for trends in litigation management and electronic discovery—ensuring there are no surprises—because a reactive approach to potential lawsuits can paralyze a company.

At P&G, the e-discovery governance board includes representatives from groups such as litigation, intellectual property, media, advertising, and marketing. Each brings unique expertise and discernment to the e-discovery table. They also act as valuable vessels for driving communications outward. When we have updates or changes within our workflow, they take our message back to their respective groups or colleagues and spread the word. Through this interaction, the board members become valued shareholders in e-discovery.

TACTICAL TIP: E-DISCOVERY BOARD KEEPS THE TEAM FOCUSED

1	Includes delegates from a variety of business groups
2	Serves as a watchtower for industry and legal trends
3	Acts as a communications vessel within the company

Example - Governance Board: The industry is seeing an increase in litigation requests driven by social media. With the insight and vision from our governance board, we identified this issue early on. We addressed the exposures that social media brings in a variety of disciplines, not just litigation, but also antitrust, digital media, and compliance. Through cross-pollination of ideas, the board enabled us to efficiently tackle a new initiative in less time and with less liability than it would have taken otherwise.



Measurements

Annual measurements are used to confirm our e-discovery preparedness. A scorecard feeds the measurements that keep the e-discovery process balanced between case management and the governance board. I consider this to be one of the most important tactics that helps our team exceed performance expectations. It's a clever coup for anyone ready to take their company's e-discovery process to the next level and revamp it from one of mediocrity and missteps to one of maturation and mastery.

The scorecard serves as our dashboard view into case management and the governance board to continually monitor opportunities, gaps, and effectiveness. And since a core value at P&G is to drive oneself by internal measures, the e-discovery scorecard does just this.

E-DISCOVERY SCORECARD	STATUS
Technology	
1. How fast are we able to...	Yellow
2. How much did we save when...	Green
Capabilities	
3. How well did we meet...	Green
4. How efficient is the...	Red
5. How well are we doing with...	Yellow
Partnerships	
6. Do our vendors respond to...	Red
7. Can our partner help with...	Green
Education	
8. Are we up to date on...	Green

Figure 4: E-discovery scorecard example

This P&G scorecard is shared annually with management and P&G's chief legal officer. Using four rubrics (technology, capabilities, network partnerships, and education), we rate the core processes of our case management team and new trends identified by the governance board. Colors are assigned to measure how well we are hitting our goals and targets: yellow is a sign for improvement; red is cause for immediate action; green is a statement of stability. We align with executive directives and decide on next steps.

Example - Scorecard Results: Two years ago, our scorecard identified inefficiencies caused by using multiple vendors. The vendors were working in silos, some had outdated software, and we faced clunky issues between legal admin and setting up legal holds. Once this opportunity was identified and triaged, we were able to streamline vendors and tighten the legal hold process in a way that didn't hurt our defensibility (and in many respects, enhanced our defensibility *with* total cost of ownership!).



What to Measure

Here is a list of some of the internal scorecard measurements we currently use, or have used in the past:

- How quickly can we get the review in the system?
- How quickly can we have data ready for counsel to review?
- How quickly do we have our tools in place?
- How quickly do we have a project manager assigned?
- How well are we doing with user satisfaction?
- Are the methods transparent?
- Are the processes repeatable and defensible?
- Is the team trained?
- Are CLEs and required certifications up to date?
- Are we able to handle one-off cases?

Internal vs. External Scorecards

We put a lot of emphasis on our internally developed scorecard because our unique operation warrants unique measurements. We also use an external scorecard so we can compare ourselves against external metrics to keep ourselves honest and aligned with industry best practices. The e-discovery Maturity Self-Assessment Test (eMSAT-1)^{iv} is comprehensive and worth the time it takes to get through the multiple worksheets. It helps to rate how our P&G digital investigation service compares with industry expectations so we can have a more complete story with a holistic view of our service.

Tactical Tip: Scorecards Determine State of E-Discovery Preparedness

1	Internal review: Look back with your scorecards
2	External review: Dive deep to compare against industry best practices
3	Find the big opportunities as well as the big gaps
4	Get alignment with management and legal
5	Commit to reassessment in the next fiscal year

IMPLEMENT AN ESI POLICY

A recent AIIM Industry Watch^v reported that 61 percent of companies surveyed do not have an information governance policy and of those who do, 85 percent do not enforce it. This is a surprising statistic when you consider the clarity of the laws outlined in the Federal Rules of Civil Procedure (FRCP) and tighter controls by state court rules on data retention and preservation.

At P&G, there's no wiggle room when it comes to implementing an e-discovery policy. It's a given. It protects us in court when counsel asks for our ESI policy. It reduces frustration for new employees learning new procedures. It expedites marketing when a new product is launched and needs to have the right set of controls in place. At the end of the day, the ESI policy facilitates potential litigation.

Here's a snapshot of a portion of the current policy in place at P&G:

ELECTRONICALLY STORED INFORMATION POLICY	
<p>P&G identifies, preserves and collects electronically stored information relevant to U.S. litigation in which P&G is involved. Compliance with this policy is expected by all P&G employees located in the U.S. P&G has the necessary systems and procedures to comply with this policy.</p>	
<p>Electronically stored information is anything stored on a computing device and may include email, web pages, word processing files and video files. Electronically stored information that is part of P&G's business operations may be subject to subpoena by courts in the U.S. as part of a lawsuit in which P&G is involved. Failure to preserve electronically stored information appropriately could subject P&G or individuals at the company to severe court sanctions. P&G is committed to taking all reasonable and necessary steps to retain electronically stored information appropriately. P&G has an E-Discovery Support Team that provides Information Technology support, training, and consulting service to help P&G and its U.S. employees comply with its obligations (namehere@pg.com).</p>	
<p>P&G has implemented procedures and supporting software systems to help comply with this policy. The key elements of the procedure consist of: (1) Issuing a Legal Hold of electronic stored information for relevant employees; (2) Interviewing employees subject to the Legal Hold so that relevant electronically stored information can be identified; (3) Collecting the relevant electronically stored information and any other relevant non-electronic documents; and (4) Releasing the Legal Hold upon conclusion of the relevant litigation.</p>	

Figure 5: P&G's ESI Policy

The good news is that the policy can be generic, straightforward, and best of all, brief. It's a tool to educate employees, consultants, and others in the organization about the corporate ESI procedures. And when employees are involved early, they become the first line of defense, helping to strengthen and simplify the e-discovery process from the ground up.

TACTICAL TIP: KEEP THE E-DISCOVERY POLICY SIMPLE	
1	What is electronic data?
2	Why does the company need a policy?
3	What are possible consequences of failure to comply?
4	Who to contact with questions?



CONCLUSION

IDC's The Digital Universe^{vi} study published in 2014 states that the total amount of data created and copied in 2013 was 4.4 zettabytes (equal to 4.4 trillion gigabytes or 4.4 billion 1TB disk drives) and will grow by a factor of 10 by 2020. Even if you can't wrap your brain around those numbers, it tells me one thing loud and clear: the data discovery battle has just begun.

We're in the era where employees bring their own device to work, and soon will walking the halls with Google Glass wearable technology, or some comparable equivalent, on their heads. The term "Internet of Things" is no longer a neat and catchy buzzword: it's a reality. I cannot lean back, take a breath, and say, "I've got this e-discovery service just the way I want it," otherwise, I'll find myself back at square one. Exponential explosions in data, shifts in technology, and revised legal landscapes will require all of us to be more vigilant, resourceful, and willing to reinvent the process as needed.

In summary, my colleague and I have a lean digital investigation team, so we take it seriously when reading about the indomitable downpour of data looming ahead. We're standing armed and ready, however, to be good stewards of P&G in the responsibilities we took on, because:

- We know where we play in the EDRM model and are very clear with our service—what we do and what we don't do.
- We have a good relationship with several vendors. We have a preferred vendor, but also have niche players for unique situations that require a unique solution.
- We have the e-discovery governance board for collaboration, coaching, and integrating new initiatives.
- We have an ESI policy in action and work with the application or system owner to ensure the right e-discovery controls are in place.
- We assess ourselves every year and compare our scorecards from the previous year. We commit to higher performance and align with management and legal.

Wishing the best as you strive to strengthen, simplify and streamline your own e-discovery process.

CITATIONS

ⁱ <http://www.edrm.net/resources/edrm-stages-explained>

ⁱⁱ <https://www.guidancesoftware.com/products/Pages/encase-e-discovery/overview.aspx?cmpid=nav>

ⁱⁱⁱ <https://www.guidancesoftware.com/products/Pages/encase-enterprise/overview.aspx?cmpid=nav>

^{iv} <http://www.edrm.net/resources/emsat1>

^v <http://www.aiim.org/Research-and-Publications/Research/Industry-Watch/InfoGov-2013>

^{vi} <http://www.emc.com/leadership/digital-universe/2014iview/index.htm>



ABOUT GUIDANCE

Guidance exists to turn chaos and the unknown into order and the known-so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. The makers of EnCase®, the gold standard in forensic security, Guidance provides a mission-critical foundation of market-leading applications that offer deep 360-degree visibility across all endpoints, devices and networks, allowing proactive identification and remediation of threats. From retail to financial institutions, our field-tested and court-proven solutions are deployed on an estimated 33 million endpoints at more than 70 of the Fortune 100 and hundreds of agencies worldwide, from beginning to endpoint.

Guidance Software®, EnCase®, EnForce™ and Tableau™ are trademarks owned by Guidance Software and may not be used without prior written permission. All other trademarks and copyrights are the property of their respective owners.