

# Security Transcends Compliance

*By Laura Whitt-Winyard  
ICIT Fellow and Global CISO, DLL Group*



Despite common misconceptions, ticking all the boxes on a regulatory compliance audit does not make your company secure. No company is 100% secure. Security transcends compliance, not the other way around. Regardless of whether it is FFIEC, GDPR, PCI-DSS, HIPAA, etc. regulations; standards such as NIST, ISO, COBIT, NERC; or the overwhelming slew of privacy regulations around the world, nearly all of these regulations are comprised of basic security hygiene and they are outdated at publication. Most often, these regulations are drafted, reviewed, and edited with an effective date and years have already passed. The world of security advances at a break-neck speed and the regulatory process cannot keep up. Regulations and legislation are meant as enforcement for those companies who are not doing proper security hygiene; they are the minimum, not the gold standard.

If your security hygiene is good, then visits from auditors will not be time consuming, dreadful, and laborious. Instead, audits will be positive experiences that help you identify overlooked areas that should be addressed. After all, you are only as secure as your weakest link. Auditors can act as a sanity check, confirming your company has a good security strategy. Additionally, an audit can be an opportunity to educate your auditor on innovative and new security capabilities and strategies. In an ideal world, an audit is a two-way street where both parties seek to educate each other.

An audit can also be a prime opportunity to increase your budget and praise your security organization. Every organization struggles to fund their security efforts because cybersecurity is often viewed as important, but not a priority. If your Board of Directors has this mindset, using the threat of regulatory fines can help you pass a new budget, perhaps funding a solution for that annoying legacy environment. However, fear mongering can perpetuate an attitude that believes nothing should be funded unless required by regulation, which is why it must be used sparingly. Everyone in cybersecurity knows it is a thankless job. Most teams work tirelessly, but often go unnoticed. The nature of the job ensures that when things are going well, cybersecurity teams are forgotten. It is only when something inevitably goes wrong that security teams gain the unwelcome spotlight. An audit is an excellent opportunity to praise the innovative and hardworking individuals that make up your security organization. These kudos are often warranted and help you retain highly skilled security professionals.

Security is an uphill battle, with companies needing to constantly innovate to stay one step ahead of the auditors and close the ranks on cybercriminals. Make no mistake, it is a battle and even a

war some might say, as is evident by so much military language incorporated into security terminology. For the laurel resting status-quo sect, it is even more so compounded by the fact that security is always and vastly morphing. For those education addicted, high energy, puzzle solving innovators, it is an exciting challenge bordering on a life-long mission of the highest order. For the former, a serious adjustment in thinking and attitude towards security is required. Ultimately, there are diverging paths that must be walked simultaneously. It is an effort in futility to attempt to clean up the gaps and only then focus on innovation. Any attempt in doing so will ensure a company is continually lagging behind. The only viable answer is to focus on the past, present and future simultaneously.

*"It is an effort in futility to attempt to clean up the gaps and only then focus on innovation."*

- Laura Whitt-Winyard

Concentrating on the past is daunting, conjuring nightmares of bad configurations, and legacy systems compounded by years of neglect. Where do you start to address these security gaps? The amount of work is overwhelming. The first step is to create a gap assessment based on whichever security framework or regulation you prefer. Try to pick one that is somewhat prescriptive as this makes it easier to interpret, leaving less room for error and debate. While performing the assessment, be as expeditious as possible. Do not let perfect get in the way of good because remediation plans

will inescapably need to be developed. During that process, new gaps will invariably present themselves which is why it is not efficient to be meticulous when getting started.

Next, identify the owner of each gap. For the majority, the owner should not be someone in the security department. For example, access reviews belong to business, configuration errors usually belong to DevOps or Infrastructure, and application penetration testing and remediation belongs to a development team. Once the owners have been identified, the security department should confirm the correct owner and ensure everyone's responsibilities are clear.

To increase adoption, create visibility among executive leadership and the gap owner's peers. The best way to do this is creating a conspicuous dashboard that is linked to a tracking tool. For each gap, create a task or ticket and assign it to the leadership of the department that owns the gap. As each gap is remediated or goes past due, your dashboard should automatically update. The intention is to create friendly competition between departments, shed light on areas that need help, and motivate people to fix their security issues.

By automating as much of the tracking as possible, the security organization should be free to focus on the present, validating remediation plans, reviewing exceptions, and identifying countermeasures to ensure gaps do not reoccur. Good countermeasures can be anything from servers hardened by default to requiring configuration changes to go through an approval board, preventing code from going into production without scanning for vulnerabilities, and disabling unused access.

Throughout this process, keep in mind that delaying gap remediation may be permitted with a valid business reason, approval of senior leadership, and a plan to reexamine the gap within an agreed upon timeframe. As a side note, excuses such as budget, time, or resources are all stall tactics. When extensions for the same gap are repeatedly requested, expedite the gap up the corporate ladder and request senior leadership to clearly, traceably document that they accept the risk caused by the gap. One of three things will happen:

1. The barriers will be removed because leadership will be unwilling to risk having their name associated with the consequences of the gap going unfixed.
2. Leadership will stall by ignoring messages, fabricating an inability to comprehend the request, or passing the buck on. In which case, elevation to the Board of Directors is required.
3. Leadership may also accept the risk, resulting in the gap being marked for follow up in a set amount of time, usually six months. Once the agreed-upon interval has passed, leadership should be asked to once again confirm the risk is still acceptable.

While setting up a system to automate gap remediation and implementing countermeasures, your cybersecurity team cannot forget the future of security. It is a scary world out there in terms of security. Think about Wikileaks, Sony Attack, WannaCry, Stuxnet, Cyber-offensives for political reasons, the deluge of data leaked/breached, etc. Within the last two years, two states, Colorado and Louisiana, declared a state of emergency due to ransomware attacks on government systems. This trend will continue to escalate, and it will get worse. There is no getting ahead of the bad guys. There is no getting ahead of security threats. There is no more flying under the radar because you are “not a target.” More and more, it is a crime of opportunity because the information needed to attack companies is readily available and exposed for all the bad actors to see on the likes of Shodan, Freenet, Onionland, etc. However, there is a real possibility of closing in, reducing the mean time to detection and meantime to remediate and a little thing called Bump Drafting (more on that later).

It is crucial to understand that the perimeter is fading if not already gone in most cases. Boundaries are increasingly vague encroaching on limitless. Humans are able to work/connect anywhere, anytime on virtually any device. It has never been more important than it is now to be proactive about security. Many publications have been devoted to concepts like “Security by Design”, “Zero Trust” and “Data-centric Security”. These are just a few ways to begin a proactive security path that automatically builds security into everything from software to account creation and hardware. Being future-focused reduces the gaps discovered during assessments, reduces re-work, frees up time for your cybersecurity team, and decreases the attack surface for bad actors. It is time to extinguish the trust but verify mentality. Internal versus external requests are irrelevant: neither should be trusted. Ultimately, it is all non-sense if the type of data and location of data is unknown. The point is, research, connect with peers, learn as much as you can about the principles of proactive security and help your business adapt and grow.

As we look to the future, one of the best analogies comes from racing. It is called Bump Drafting. Drafting is an aerodynamics technique where vehicles or other moving objects like bicycles align reducing the drag effect. If the gap is narrowed enough, a bump draft can nudge the object in front usually forcing it to slow down in response to the bump or lose control. In this analogy, the lead object is the hacker and those aligned behind are the security community. The goal is to narrow the gap by using techniques like quantum computing, which is accelerating faster than anticipated, artificial intelligence, machine learning, probabilistic methods, blockchain, anomalous detection with autonomous response, and user and entity behavior analytics (UEBA) combined with just-in-time training. Remember the education addicted, high energy, puzzle solving innovators? The security community needs more of these types of individuals. The need is great for accelerating security advancements and developing new concepts.

*"If the gap is narrowed enough, a bump draft can nudge the object in front usually forcing it to slow down in response to the bump or lose control. In this analogy, the lead object is the hacker and those aligned behind are the security community."*

*Laura Whitt-Winyard*

Security is a mindset that requires constant learning through reading, research, listening to podcasts, watching videos, attending conferences, networking with peers, and trying new ideas, breaking things, fixing things, etc., to the point of flirting with ad nauseam. Your mission, should you choose to accept it... well, you know the rest. If you can succeed in making cybersecurity an integral part of your organization's ethos, you need never fear another audit. You will be ahead of the curve, able to proudly display what your security team has been building to keep your company safe.

## About the Author

Laura Whitt-Winyard, CISM, CISA, CRISC, RSA-ACA is Global Chief Information Security Officer for DLL Group spanning more than 30 countries and is an Institute for Critical Infrastructure Technology (ICIT) Fellow. She has 19 years of information security experience and has been an active member of the security community. Laura joined DLL Group from Billtrust, where she served as Director of Security. Previously, she held information security leadership roles at Comcast and Bloomberg, L.P. Laura was included in the book: Women Know Cyber: 100 Fascinating Females Fighting Cyber Crime. She and her teams have been nominated for and the recipients of many awards spanning multiple years such as ISE® North America & Northeast Project Nominee & Finalist, ISE® North America & Northeast Executive of the Year nominee, CSO 50/40 Awards winner, RSA Archer Innovation Awards & Excellence Awards.

Twitter: @L\_WhittWinyard

LinkedIn: <https://www.linkedin.com/in/laurawhittwinyard/>

## About ICIT

[The Institute for Critical Infrastructure Technology \(ICIT\)](#) is a 501c(3) cybersecurity Think Tank with a mission to cultivate a cybersecurity renaissance that will improve the resiliency of our Nation's 16 critical infrastructure sectors, defend our democratic institutions, and empower generations of cybersecurity leaders.