The 5 Stages of Compliance Audit Grief

NNT

SECURITY THROUGH SYSTEM INTEGRITY

NOW PART OF netwrix

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

PRECIS

Some of us will need therapy during and after an audit - that's not unusual - but can a Compliance Audit really bring about the same feelings as other forms of grief?

Furthermore, if this really is the case then, by extension, could we coach ourselves through the compliance audit process to become more effective at dealing with future audit situations?

The aim of this whitepaper is to provide new angles from which to view compliance and cyber security. If you are responsible for some aspect of an information security audit and you have anything other than a completely positive perspective towards compliance, don't worry, you are not alone. Furthermore, be assured that there is light at the end of the tunnel.

By examining the attitudes observed by customers during their audit cycle it is apparent that there is a strong correlation with the popular Kübler-Ross '5 Stages of Grief' model. Applying this understanding means we can all take learn how to make our own experience less painful and more productive.

Introducion: The psychology of a Compliance Audit

Any psychotherapist will tell you that there are a range of mind states adopted when dealing with grief of any kind. The popular Kübler-Ross model lays out a progression through Denial, Anger, Bargaining and Depression before finally reaching Acceptance, often referred to as DABDA.

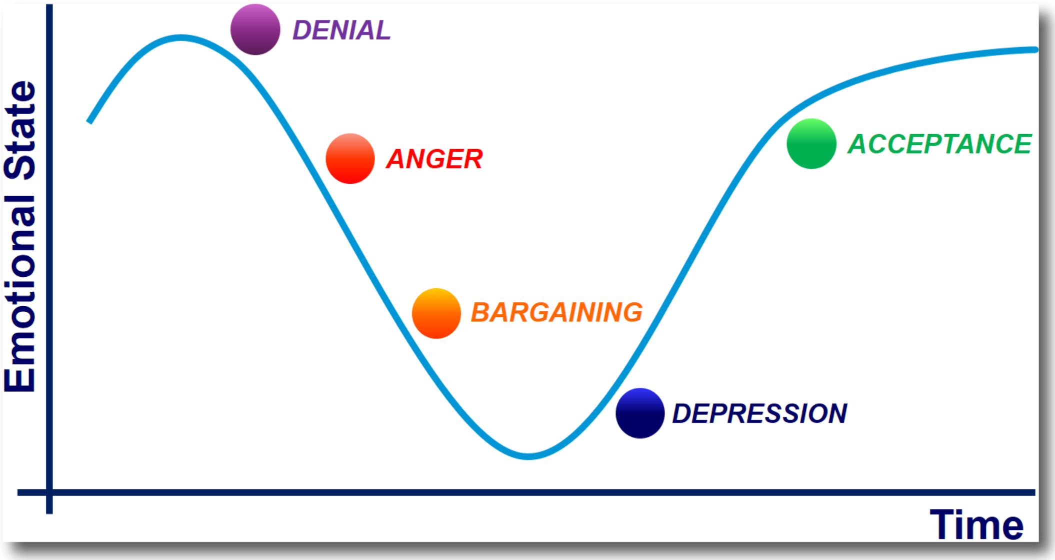


Figure 1: Kübler-Ross '5 Stages of Grief' curve Despite arguments to suggest there should be more stages and/or different emotional states used, the overall model still holds credibility today, almost 50 years after it was first proposed.

Studies have shown that there is little evidence to support the assertion that there is a fixed order in which emotional states are experienced, however, acceptance will always provide emotional stability.

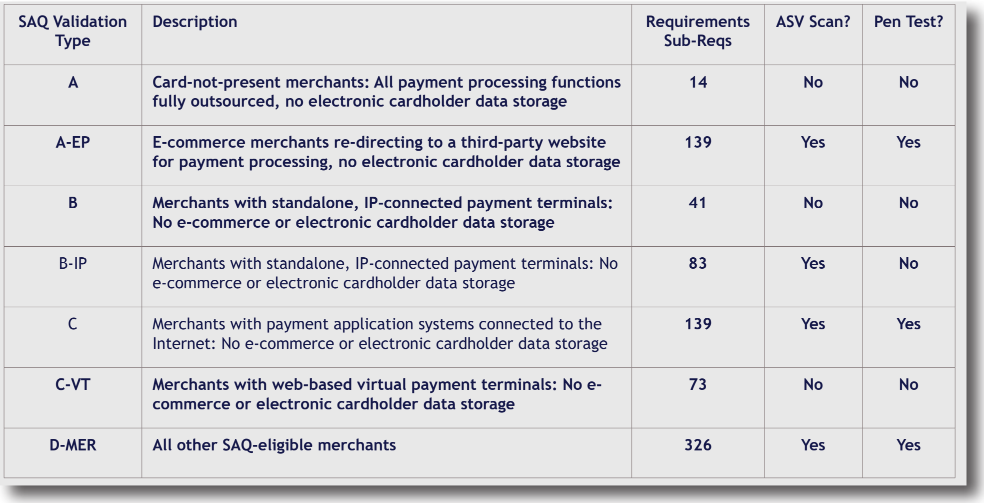
Nothing changes when dealing with the grief – angst, distress, torment or just aggravation - caused by having to manage a GRC compliance audit. The good news? You will get through it. Some of us will need therapy during and after an audit - that's not unusual - but the received wisdom is that all the other conditions of anger, denial, depression and bargaining will never truly provide a lasting solution. In fact, the sooner you can get to acceptance, the sooner you can move on. Closure can be yours.

But can a Compliance Audit really be considered as a form of grief? If you are involved in an audit, do you recognize any of these behaviors in yourself or colleagues? If it really is the case then, by extension, could we coach ourselves through the process to become more effective at dealing with future audit situations?

Denial: The Wine Retailer

The first stage of compliance audit grief involves denial. We once met with a wine retailer, with stores and both on-line and call center sales channels – classic PCI territory and needing them to observe the full SAQ D requirements.

(Note: SAQ D stands for Self-Assesment Questionnaire, a PCI Security Standards Council inititiave to allow smaller merchants to self-audit. Various categories exist for the SAQ so that those Merchants with lower risk e.g. no cardholder not present transactions, are permitted to observe fewer PCI DSS requirements than a higher-risk Merchant. An SAQ D is the most comprehensive SAQ.)



SAQ Validation Type	Description	Requirements Sub-Reqs	ASV Scan?	Pen Test?
A	Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage	14	No	No
A-EP	E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage	139	Yes	Yes
B	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage	41	No	No
B-IP	Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage	83	Yes	No
C	Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage	139	Yes	Yes
C-VT	Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage	73	No	No
D-MER	All other SAQ-eligible merchants	326	Yes	Yes

Figure 2: PCI SSC SAQ Matrix - the higher the risk, the more requirements must be met

However, in this instance the organization was reluctant to adopy any PCI measures.

We spent an hour confirming previous discussions they had covered with their QSA with respect to how many devices were in-scope. We confirmed that they they had some opportunities to de-scope, but that they also had considerable risk areas that PCI requirements are squarely aimed at protecting. We then went on to discuss how we could help with chunks of PCI requirements, all points they accepted and agreed would address their security weakspots.

They then asked what the current levels of fines were for not implementing PCI measures – we know of merchants fined $15K per quarter for persistent non-compliance but it’s actually a very grey area because the dynamic is usually between the merchant and their Acquiring Bank.

The bank wants the payment transaction business and they want the merchant to be compliant, but the two objectives aren’t always of equal priority. The bank makes their own assessment of risk and applies stick and carrot to encouraging compliance through transaction fee rates and fines if agreed compliance milestones are missed, for example, remediation of scan results and implementation of FIM and logging.Their conclusion? *‘So, until we get told to do this we don’t need to do anything’*

In fact the 2015 Verizon report on PCI Compliance reported that 80% of merchants overall do not meet PCI DSS requirements. More of a concern was that a separate study by the Merchant Acquirers Committee showed that more than 30% of Level 1 Merchants are not compliant. On this basis one might take a stance that ‘Nobody else is doing it – why should we?’.

Classic denial but is this really such a short-sighted approach to take? If your bank agrees to let you get away without implemneting PCI DSS measures isn’t that the end of the story?

> *“80% of all merchants and 30% of Level 1 merchants do not meet PCI DSS requirements”*
>
> *‘If nobody else is doing it, why should we?’*
>
> *2015 Verizon report on PCI Compliance and 2015 study by Merchant Acquirers Committee*

verizon
Verizon 2015
PCI COMPLIANCE REPORT
Insight for helping businesses manage risk through payment security.
67%

Figure 3: Draw your own conclusions: Verizon’s 2015 PCI Compliance Report showed that only 20% of organizations are validated as compliant when assessed for their Interim Report on Compliance - that means 80% are not compliant under ‘Business as Usual’ conditions

Anger: The War Room

Most organizations with compliance responsibilities will resent the expense and disruption.

The cost of getting compliant varies massively depending on the scope of your PCI estate (how many devices 'store' cardholder data) and how you can segregate and protect these devices. Remediation and segregation fees may run to $100K's, for example, implementing new firewalls, updating and hardening devices and even re-designing application operations.

Similarly the more complex an enterprise in PCI terms, the longer and more expensive an audit will be, but assuming the auditing team is on-site for a couple of weeks the overall fees can easily run to $50K plus.

Then there is the resource needed to manage the exercise – in a recent scenario a client of our needed to establish a War Room, populated with key team members to orchestrate the implementation of logging and FIM, gathering evidence/artefacts for the auditor, and remediating systems where needed. Hotel bills, flights and subsistence ran to $100K's.

> *"Segregation and remediation costs... Auditor fees...Who wouldn't resent the expense of PCI compliance?"*

Figure 4: The Burden of Compliance - PCI Merchant Levels and compliance validation requirements

All merchants will fall into one of four merchant levels based on Visa transaction volume over a 12-month period. The following guide indicates the volume of transactions and the appropriate validation requirements at each level.

Level*	Merchant criteria	Validation requirements
1	Merchants processing more than 6 million Visa transactions annually via all channels or global merchants identified as level 1 by any Visa region.**	Annual Report on Compliance (ROC) to follow an on-site audit by either a Qualified Security Assessor or qualified internal security resourceQuarterly network scan by Approved Scan Vendor (ASV)Attestation of Compliance form
2	Merchants processing 1 million to 6 million Visa transactions annually via all channels.	Annual Self-Assessment Questionnaire (SAQ) Quarterly network scan by ASV Attestation of Compliance form
3	Merchants processing 20,000 to one million Visa e-commerce transactions annually.	Use a service provider that has certified their PCI DSS compliance (certified providers are listed on Visa Europe's website: www.visaeurope.com) OR Have certified their own PCI DSS compliance to the acquirer (who must, on request, be able to validate that compliance to Visa Europe) (SAQ)
4	E-commerce merchants only Merchants processing fewer than 20,000 Visa e-commerce transactions annually.	Use a service provider that has certified their PCI DSS compliance (certified providers are listed on Visa Europe's website: www.visaeurope.com) OR Have certified their own PCI DSS compliance to the acquirer (who must, on request, be able to validate that compliance to Visa Europe) (SAQ)
	Non e-commerce merchants Merchants processing up to one million Visa transactions annually.	Annual SAQ Quarterly network scan by an ASV Attestation of Compliance form

* Compromised entities may be escalated at regional discretion

** Where merchants operate in more than one country or region, if they meet level one criteria in any Visa country or region, they are considered a global Level one merchant. An exception may apply to global merchants if there is no common infrastructure and if Visa data is not aggregated across borders. In such cases merchants are validated according to regional levels.

Who wouldn't resent the expense of PCI compliance, especially when much of the time is spent confirming that your existing security is sufficiently good, rather than necessarily implementing new measures.

Your therapist will tell you that if you are angry, this is actually a good sign - it shows you are making progress: you should be pleased!

Bargaining: You can fool some of the people...

We have a number of experiences whereby a customer wants to put everything on hold while they decide what their overall strategy should be. Should they outsource payment transactions completely or manage security of cardholder data themselves? Can they delay the audit? Can they quickly implement some kind of freeware?

> *“... cyber security skill-sets are still in short supply...Too many security vendors sell their clients what they ask for, not what they need”*

It’s a pretty common approach to adopt: *‘We don’t have the time to do this properly so let’s just make it through the audit **THEN** next time we will do things properly’*. Would the results from a couple of vulnerability scans show enough willingness to make the auditor go away? Sometimes it may work, but you’ve also made your problems ten times as bad if you then suffer a breach having taken shortcuts to bypasse key security best practices such as FIM and logging.

Take a step back and think about what the ultimate objective is? Is it only about ducking the current audit, in which case, what will be different next time? Long-term, you will need to implement data security measures and every day you continue to deliberate, customer data is at risk of being compromised. And its not just about cardholder data. For example, SOX compliance overlaps greatly with PCI requirements, so why not take a unified approach for all compliance needs?

Similarly, if your organization handles Health Insurance data then you will also be subject to HIPAA/HITECH. As such, if you are then breached and responsible for the loss of any personal identifable information, you should expect to be hit with punitive fines from the DHHS Office for Civil Rights (OCR), running to millions of dollars.

Then you have more general Data Protection legislation, for example, the State of California Data Security Breach Reporting laws and the recent announcement from the New York State Department of Financial Services for Cybersecurity Requirements. Expect to see organizations presiding over breaches facing settlement costs similar to those being paid to the OCR for health insurance data losses.

Mark at NNT rounded off the answer “First point to make is that if you don’t know what you have today and somebody adds a new device to your network tomorrow, you wont spot it – network sniffer or rogue access point for example.Your knowledge needs to go beyond the platform, further than the software and versions installed, right through to the actual settings at a security policy-level where config vulnerability mitigation is enabled. Changes here could weaken hardened defences leaving you prone to attack – you need visibility at this level”

ISO
CALIFORNIA REPUBLIC
FedRAMP
PCI Security Standards Council
NIST National Institute of Standards and Technology U.S. Department of Commerce
NERC North American Electric Reliability Corporation
European Commission

Figure 5: Compliance Time-Bomb *The trend is undeniable - as realization increases of the potential impact a cyber attack could have on our national and industry-sector infrastructure, so too the drive for greater regulation will grow.*

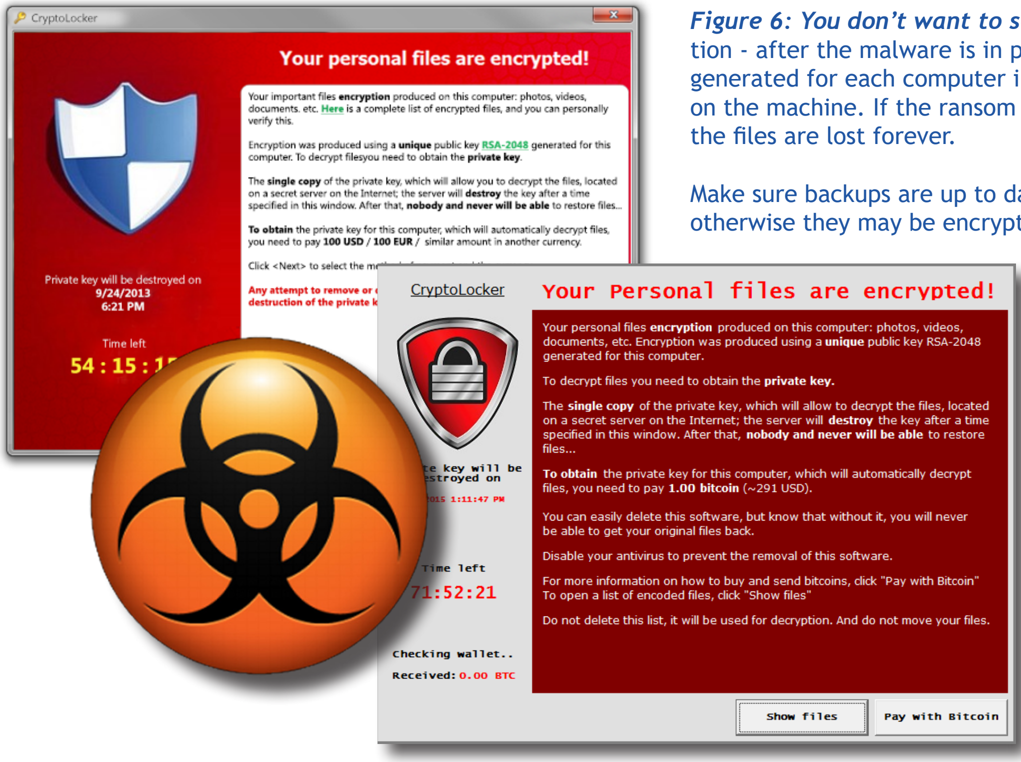
Following the California State Data Breach legislation, both the EU GDPR and the NY State Financial Services Cybersecurity Requirements have been introduced.

Demonstrating Compliance with Cyber Security requirements fo Data Portection to become universal for all organizations.

And not to be outdone, in Europe there is now the GDPR (General Data Protection Regulation). Significantly, “the Regulation also applies to organizations outside the European Union if they process personal data of EU residents” with fines up to Euro 20M or 4% of the total worldwide annual turnover, whichever is the greater number. So now you need to protect cardholder data, and financial reporting data and supporting systems, plus health insurance data ***AND*** any other customer data.

Depression: Nowhere to run, nowhere to hide

Taking all that into account ***SHOULD*** be enough to persuade anyone, but what about if you then factor in the global trends in malware and in particular Ransomware? Surely this must be enough to persuade any lingering procrastinators that cyber security is mandatory for a reason? The requirement to demonstrate compliance with security best practices is because the threat is real and imminent. Get secure for the right reasons, not just to get rid of an auditor?



CryptoLocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents. etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key RSA-2048 generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR** / similar amount in another currency.

Click <Next> to select the m

Any attempt to remove or
destruction of the private k

Private key will be destroyed on
9/24/2013
6:21 PM

Time left
54 : 15 : 1

CryptoLocker

Your Personal files are encrypted!

Your personal files **encryption** produced on this computer: photos, videos, documents, etc. Encryption was produced using a **unique** public key RSA-2048 generated for this computer.

To decrypt files you need to obtain the **private key.**

The **single copy** of the private key, which will allow to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **1.00 bitcoin** (~291 USD).

You can easily delete this software, but know that without it, you will never be able to get your original files back.

Disable your antivirus to prevent the removal of this software.

For more information on how to buy and send bitcoins, click "Pay with Bitcoin"
To open a list of encoded files, click "Show files"

Do not delete this list, it will be used for decryption. And do not move your files.

te key will be
estroyed on
015 1:11:47 PM

Time left
71:52:21

Checking wallet..
Received: 0.00 BTC

Figure 6: You don't want to see this Classic Ransomware operation - after the malware is in place, a unique encryption key is generated for each computer infected and is used to encrypt data on the machine. If the ransom is not paid within the allotted time the files are lost forever.

Make sure backups are up to date and isolated from the computer, otherwise they may be encrypted too.

The rate at which new ransomware samples are being introduced has grown by 600% this year according to ProofPoint - especially worying as any Zero Day malware is always the most deadly, being as it is compeletly invisible to signature-based Anti-Virus defense systems.

FBI advice is now that ransoms should not be paid *"Paying a ransom doesn't guarantee an organization that it will get its data back—we've seen cases where organizations never got a decryption key after having paid the ransom.*

Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And finally, by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals."

At this stage, feelings of hopelessness will be a natural reaction because having been through the denial, anger and bargaining stages, time has been wasted trying to avoid and ignore the inevitable conclusion.

In all likelihood you'll be thing 'We've blown it'. There will be nothing to show for all the time and effort spent protesting that it isn't fair, that you cant afford the investment, that it isn't necessary anyway.

Only now is the conclusion that Cyber Security is actually an essential, priority imperative that will not only protect your organization's ability to conduct its business, but will safeguard your customer data too.

Not only that, but by rejecting rather embracing the need for security defense measures, you risk punitive fines and incalculable damage to your brand's reputation. How did you ever think you could afford ***NOT*** to implement security best practices?

Acceptance: Finally – At last, it is time to get on with it!

But to use a favorite cliché of all therapists, it is always darkest before the dawn, and now the denial, anger and bargaining have all passed without any respite from the audit, it is time to face facts. Only at this stage can you begin to make progress. The great news is that technology has changed so much that not only is the cost and time to implement a fraction of what it used to be, the on-going management is also much simpler than in the past.

New technological innovations like Intelligent Change Control will mute Change Noise by literally learning what regular system activity looks like within your estate, thereby performing much of the previously time-consuming review of events necessary to spot breach activity.

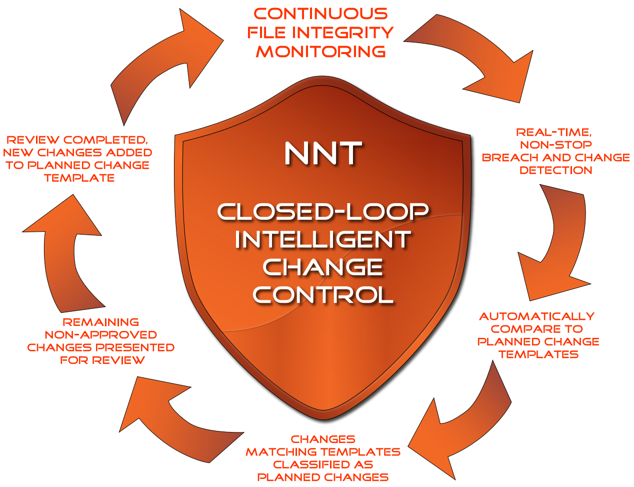
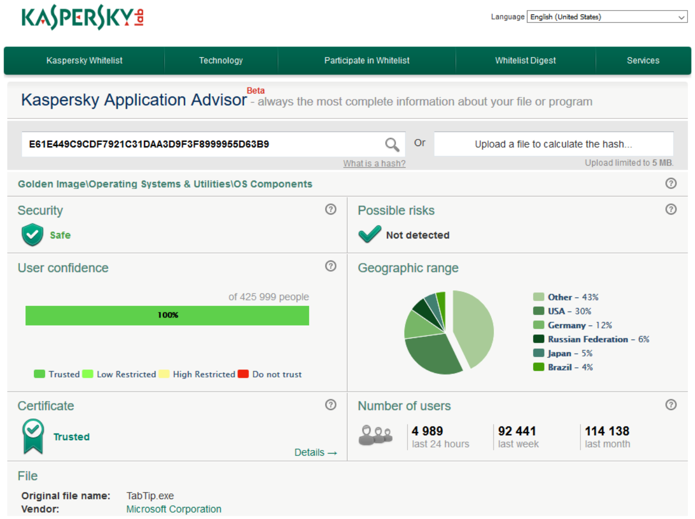

CONTINUOUS FILE INTEGRITY MONITORING
REAL-TIME, NON-STOP BREACH AND CHANGE DETECTION
AUTOMATICALLY COMPARE TO PLANNED CHANGE TEMPLATES
CHANGES MATCHING TEMPLATES CLASSIFIED AS PLANNED CHANGES
REMAINING NON-APPROVED CHANGES PRESENTED FOR REVIEW
REVIEW COMPLETED, NEW CHANGES ADDED TO PLANNED CHANGE TEMPLATE
NNT
CLOSED-LOOP INTELLIGENT CHANGE CONTROL

***Figure 7: Closed-Loop Intelligent Change Control** gives Information Security Teams an unfair advantage over hackers, malware and inside-man threats.By automatically assessing changes, all expected/pre-approved changes can be isolated leaving just unplanned changes - which may be breach activity - exposed, to then be properly investigated.*

Better still, all unplanned changes found to be legitimate can optionally be added to the list of pre-approved changes, improving the systems' intelligence further.



Kaspersky Application Advisor Beta - always the most complete information about your file or program

E61E449C9CDF7921C31DAA3D9F3F8999955D63B9 Or Upload a file to calculate the hash...

Upload limited to 5 MB.

Golden Image\Operating Systems & Utilities\OS Components

Security: Safe

Possible risks: Not detected

User confidence: 100% of 425 999 people

🟩 Trusted 🟩 Low Restricted 🟨 High Restricted 🟥 Do not trust

Geographic range

Other	43%
USA	30%
Germany	12%
Russian Federation	6%
Japan	5%
Brazil	4%

Certificate: Trusted

Number of users

4 989	92 441	114 138
last 24 hours	last week	last month

File

Original file name: TabTip.exe
Vendor: Microsoft Corporation

Figure 8: Threat Intelligence/File Reputation
Various file whitelist repositories are available, providing a continuously updated, authoritative reference for 'known-safe' file versions

The latest advances take this to another level, leveraging automated analysis of events using cloud-based threat intelligence repositories. This way you get the benefit of file whitelisting intelligence to confirm changes are non-malicious even if they weren't necessarily expected as part of a Planned Change.

Summary

We can learn from the 5 Stages of Grief model and apply the same thinking to Compliance Audit Grief.

Automation is the key difference for compliance today – make use of it – because the threat from cyber attack is getting greater by the day, as are the external demands to prove the adoption of Security Best Practices. Its no longer just a case of making the audit and auditor go away. As with any other from of grief, acceptance is the only way to go.

About NNT

New Net Technologies (NNT) is the leading provider of Secure Ops, which leverages security through System Integrity along with Intelligent Closed Loop Change Control, focused on helping organizations reduce their security risk, increase service availability and achieve continuous compliance. NNT delivers its Secure Ops suite by combining: System Configuration Hardening, Closed Loop Change Control, Vulnerability Management and Event Log Management. These core security disciplines are defined by the SANS Institute as the essential Critical Security Controls for any cyber security initiative.