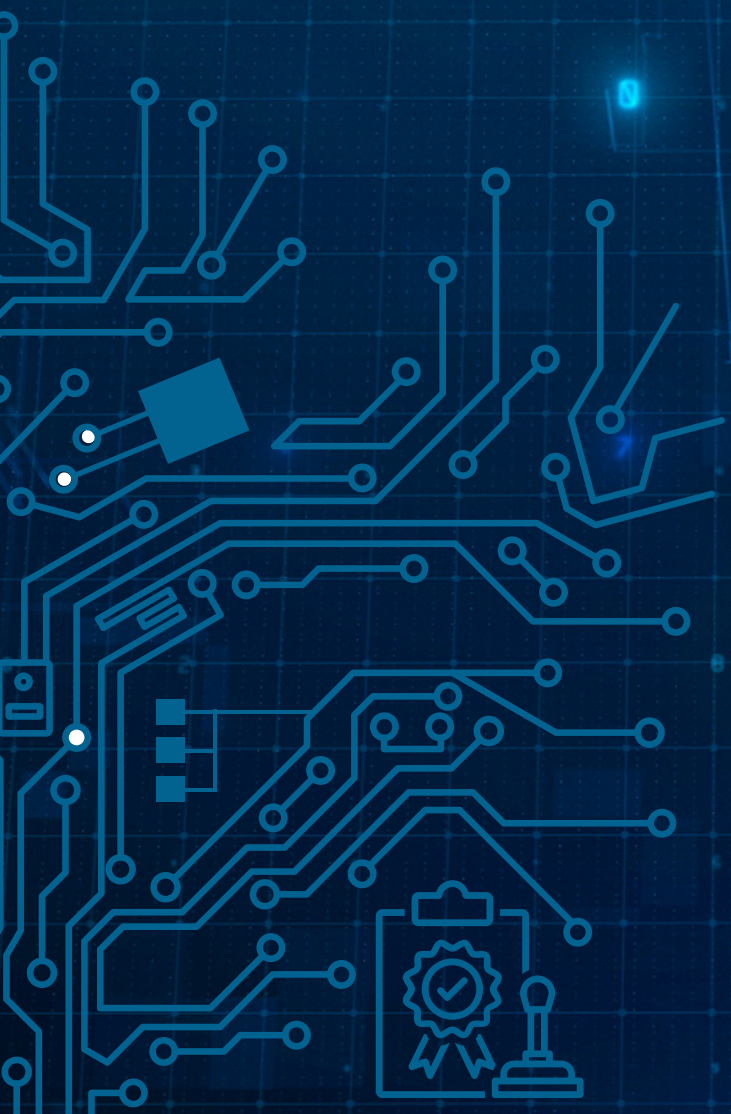
Runecast

SECURITY COMPLIANCE GUIDE

Achieving Audit-Readiness for Security Standards Compliance in Modern IT Environments



By Steve Salisbury

Product Marketing Specialist at Runecast Solutions Ltd.

Publication date: May 2023

Table of Contents

Overview

Modern IT environments are highly complex. Some companies run a fully on-premises or private cloud model using a mix of virtualization products. There is now an increasing trend to mix technologies using a hybrid cloud model such as virtualization on Amazon Web Services (AWS), Microsoft Azure, and GCP based solutions and models utilizing combinations of VMware, Hyper-V and Kubernetes.

Modern enterprises utilize more and more multi-cloud and distributed architecture, and the resulting increase in complexity is making everyday security increasingly difficult, requiring security teams to work through and with multiple vendors and toolsets, increasing both the cost and the risk of blind spots.

Security teams need to ensure that their Cloud Security Posture Management (CSPM) misconfiguration and compliance issues are fully visible, auditable, and that solutions are provided to remediate security flaws which may open environments to attacks, resulting in costly downtime, loss of customer faith and possible loss of continued business.

An increase in regulatory compliance requirements, market pressures on following security standards and best practices, and the continuous flow of changes and additions to existing standards put today's enterprise in a constant state of firefighting for the next audit. Without a platform that allows for automated, multi-cloud and cross-platform scanning of compliance standards, demonstrating continuous compliance turns into a near-impossible challenge.

Realistically, most organizations are using some combination of each technology, and tracking compliance with security standards can require significant effort. Keeping environments up-to-date with the latest standards and best practices is time-consuming and cost-prohibitive without help from automated processes.

This white paper discusses an outline of some of the more common security standards, their associated pain points, and ways for CISOs, CIOs, and their Security and Operations teams to comply with these standards to maintain secure private, hybrid, and public cloud environments.

Overall Pain Points

- A lack of visibility into the compliance state of the environment.
- The time required for manual checks and remediation.
- Configuration drift over time, and visibility into this.
- Bottlenecks/Resource constraints.
- The costs of reactive, rather than proactive remediation.
- Fines for non-compliance with industry security standards.
- Damage to organizational reputation, and subsequent loss of revenue.
- The need for external Consultants to deal with the aftermath of a breach.

Security auditing and compliance are a continuous challenge. Many of the industry security standards speak with enough attempt at universality to appear generic.

It can be overwhelming to translate the countless controls and requirements of the security standards to your environment settings, with the purpose of both becoming and staying compliant.

As these standards are dynamic, far-reaching, and cut across industries, it requires that System Admins remain up-to-speed on all of them as changes occur. As you can imagine, this can seem a daunting task.

Time-consuming security audits

Staying on top of the latest security standards and best practices in the rapidly evolving world of IT is challenging and time-consuming for any IT department, regardless of how well-staffed it might be. These standards are written in a technology agnostic style, purposely defined in a broad way to encompass the highest number of possible situations.

It can be extremely difficult for IT Security teams to translate requirements such as HIPAA, NIST 800-53, and PCI DSS, into technical controls.

- Security and Operations teams often do not have the resources or skillset to build and manage security policies that meet these standards.
- A lack of visibility into environments leaves Security teams reactive at best toward audit compliance.

A Solution for Audit-Readiness

Few tools exist that can help to maintain audit-readiness. A solution that can correlate between the standards' policy requirements and more technology-specific checks that can be clearly understood by all IT personnel is required. Every industry, business, and organization is subject to security standards that can cost time, money, and business reputation in the case of compliance failure. The typical pain points listed above are called such for many reasons, among them, that even the most experienced System Admins understand that there are some aspects of their work that are not humanly possible.

An automation solution is needed, which can be used as a single point of reference, in the realm of security compliance. It is required to translate human-readable language from numerous industry sources into machine-readable language that works securely (both on-premises and offline). It must provide software-defined data centers (SDDCs) continuous audits for an ever-expanding list of the most relevant and complex security standards. The solution needs to be able to scan specific configurations and provide gap analysis reports for security hardening checks, as well as remediation steps for any issues it discovers. General requirements include:

- Improved Availability, Manageability, Performance, Recoverability, and Security (AMPRS).
- Best practices analysis for the solutions in use.
- Continuous auditing against standards like BSI IT-Grundschutz, CIS CSC, DISA STIG 6, HIPAA, NIST 800-53, and PCI DSS.
- Easily filtered and sorted issues, with recommendations for approach to remediation.
- Automated scans, which remove manual work and ensure optimal operation of your IT environments.
- Visibility into known security vulnerabilities: Log4Shell, Spectre, Meltdown, L1TF, MDS, and more.
- A summary of existing configuration issues and their trends over time.
- Historical data on issue discovery and fixes (ideal to pair with configuration management or IT helpdesk reporting, to track what impacted the environment), which helps to prove compliance over time.
- The capability to easily monitor the objects, showing those with issues.
- A visual representation of issues broken down to show impact across both infrastructure and design qualities.
- A summary of prevalent issues in logs, with specific summary status for each area of your infrastructure.
- Detailed, unified, and granular reporting capabilities for all issues in your environments.

The following sections describe the specific pain points and requirements associated with achieving automated security compliance against various security standards.

BSI IT-Grundschutz

The German IT Baseline Protection (IT-Grundschutz) standard was established by the German Federal Office for Information Security (BSI) as a sound and sustainable information security management system (ISMS). IT-Grundschutz covers technical, organizational, infrastructural, and personnel aspects in equal measure. With its broad foundation, IT-Grundschutz offers a systematic approach to information security that is compatible with ISO/IEC 27001.

Along with the BSI Standards, ITGrundschutz offers essential publications for all kinds of institutions who want to set up an ISMS:

- BSI Standard 200-1 defines the general requirements for an ISMS.
- BSI Standard 200-2 explains how an ISMS can be built based on one of three different approaches.
- BSI Standard 200-3 contains all risk-related tasks.
- BSI Standard 100-4 covers Business Continuity Management (BCM).

To make the successful implementation of IT-Grundschutz transparent to the outside world, companies or public authorities can be certified according to ISO 27001 on the basis of IT-Grundschutz. This certificate confirms that the IT security concept meets the requirements of ISO 27001. This is a consumer-protection regulation that provides recommendations on methods, processes, procedures, approaches, and measures relating to information security. BSI addresses issues fundamental to information security in public authorities and companies for which appropriate, practical, national, or international approaches have been established.

While BSI is a German federal standard, it is likely to be applicable to any organizations with a client base within Germany (regardless of where they are themselves based), especially those in the public and legal sectors.

Pain Points

To make a bid on projects within the public and legal sectors of Germany, a BSI baseline protection certificate is required.

The BSI baseline protection catalog is the benchmark for the National Action Plan 2017 for public authorities.

The different modules of the ITGrundschutz Compendium contain security recommendations on a wide variety of topics. Detailed advice and safeguards in the implementation guidelines for the ITGrundschutz modules are designed to make it easier for information security officers to apply information security in their day to-day work, though understanding and applying the guidelines is a time consuming and painstaking path to remediation.

Requirements for automated BSI compliance

- Summary of the existing BSI configuration issues and their trends.
- Continuous monitoring for violations against BSI standards 200-1, 200-2, 200- 3, and 200-4.
- Complex legal and technical terminology translated into a format understandable by System Admins, allowing communication on an even scale with security teams and auditors.
- Automated scanning and reporting for a BSI-compliant environment.
- Results showing configured or failed findings with issues detailed for both.
- Mapping of each finding to the relevant Building Block within the BSI standard.
- Findings listed by severity in order to allow prioritization of remediation.

CIS CSC

The Center for Internet Security (CIS) is a non-profit organization focussed on improving public and private sector cybersecurity readiness and response. The CIS Critical Security Controls (CSC) are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. A principal benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results.

The CIS Benchmarks, also known as CIS Security Standards, comprise 140+ configuration guidelines for various technology groups to safeguard systems against today's evolving cyber threats. The process of checking for compliance within your AWS and VMware environments can be arduous and costly, and any kind of manual checks are subject to human error.

Pain Points

Organizations and admins can manually check for CIS Security Benchmarks with a lot of DIY effort, but it is difficult, timeconsuming and prone to human error. Additionally, organizations need to show historical quarterly CIS compliance over the course of the year in order to be considered compliant for a given year.

Requirements for automated CIS compliance

- Automated CIS Benchmark checks.
- Coverage of both on-premises and cloud- based services.
- On-premises analysis – with no data sent off-site.
- Sort issues by officially approved CIS levels of severity.
- Detailed history of findings for historical automated scans.

CISA

The Cybersecurity and Infrastructure Security Agency (CISA) is an agency of the United States Department of Homeland Security (DHS), responsible for strengthening cybersecurity and infrastructure protection across all levels of US critical infrastructure sectors. These areas include Academic Institutions, Federal Department and Agencies, Industry and Private Sector, Non-Profit Sector, and State, Local, Tribal, and Territorial Governments.

The National Security Agency (NSA) and CISA work together to provide a catalog of resources designed to enable the security, resiliency, and reliability of America's cybersecurity and communications infrastructure. The CISA Services Catalog is all of CISA, all in one place. A resource that provides users with access to information on services across all of CISA's mission areas.

Pain Points

CISA provides a list of Knows Exploited Vulnerabilities (KEVs) which government and military institutions are required to be protected against by specific dates. Manually checking and reporting on these issues is time consuming and mistakes can be made due to human error. Additionally, organizations need to show historical quarterly CISA compliance in order to be considered compliant for a given year. Noncompliance can result in large fines and constant audits, disrupting business continuity and reducing confidence in services provided.

Requirements for automated CISA compliance

- Automated CISA Benchmark checks.
- Coverage of both on-premises and cloud-based services.
- On-premises analysis – with no data sent off-site. Compliance against KEVs.
- Sort issues by officially approved CISA levels of severity.
- Detailed history of findings for historical automated scans.
- Full reporting capabilities to prove CISA compliance.

Cyber Essentials

If you work in the UK public sector or your business operates in conjunction with such, you're likely to be aware of the Cyber Essentials security standard. Cyber Essentials was set up by the UK Government in conjunction with the Information Assurance for Small & Medium Enterprises (IASME) and the Information Security Forum (ISF) and was launched on the 5th of June 2014.

As of October 1st 2014, the UK Government has mandated that all suppliers bidding for contracts involving the handling of certain sensitive and personal information be Cyber Essentials Certified.

Cyber Essentials guides on a number of fundamentals of information security, with a focus on securing the largest attack vector – services exposed to the internet. It covers the following areas.

- Boundary firewalls and internet gateways.
- Secure configuration.
- User access control.
- Malware protection.
- Patch management.

Cyber Essentials has a significantly smaller scope than many other standards, which makes it more easily attainable by smaller organizations' IT departments. By requiring this certification to bid on UK Government contracts, this kind of approach helps organizations ensure that they have technologies, policies, and procedures that ensure greater security of UK citizens' data throughout the supply chain.

Pain Points

While Cyber Essentials is developed and administered in the United Kingdom, it is by no means in use only there. Any global organization bidding for work for the UK government is likely going to be required to have certification.

There are two tiers of Cyber Essentials certification: the base level (called Cyber Essentials) requires that a business complete a self-assessment and submit a payment to the IASME certifying board. The higher Cyber Essentials Plus certification mandates the same protections and controls be in place.

Still, it involves an assessor carrying out a technical audit of systems, end-user devices, internet gateways and services exposed to unauthenticated users over the internet. The costs involved in the Cyber Essentials Plus audit vary depending on the size and complexity of the organization's network.

Requirements for automated Cyber Essentials compliance

- Summary of existing Cyber Essentials configuration issues and their trends.
- Regular automated scans of the vSphere environment(s) against Cyber Essentials, with trends easy to identify.
- Coverage of each of the Technical Control Theme domains: Firewalls, Malware Protection, Patch
- Management, Secure Configuration and User Access Control.
- Detailed explanations of each finding, including details as to how these can be manually audited and any issues reported can be remediated.
- The capability to automate reporting, including prompts for periodic manual confirmation where an automated check cannot be performed. These include things like confirming that there is a valid support contract to cover the software within the environment, for example.

DISA STIG

The United States Department of Defense (DoD) designed these standards to ensure consistent and secure configurations across all environments. DISA STIG guidelines are often used as a baseline in other sectors or segments to ensure compliance with the standards and access to the DoD networks. All organizations must meet the DISA STIG security standards before accessing and operating on DoD networks. They are defined as:

DISA Defense Information Systems Agency (provides IT and communications support to defense and federal agencies, government, and coalition partners).

Security Technical Implementation Guides (a set of rules "created and maintained based on the cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security. These guides, when implemented, enhance security for software, hardware, physical and logical architectures to further reduce vulnerabilities").

Three Levels of Security Checks

DISA STIG speaks in terms of the CIA triad from an information security perspective. Confidentiality, Integrity, and Availability are all crucial when it comes to a system. If any of these three fail, the security can be considered compromised. Vulnerabilities are classified in terms of severity.

Low Severity: Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Integrity, or Availability.

Medium Severity: Any vulnerability, the exploitation of which has the potential to result in loss of Confidentiality, Integrity, or Availability.

High Severity: Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Integrity, or Availability.

Pain Points

Non-compliance means that systems lose access and authorization to operate on DoD networks. The policy complexity varies considerably, from checking infrastructure configuration settings to confirming manual user verifications (e.g. that verified ESXi installation media was used).

Requirements for automated DISA compliance

Summary of existing DISA configuration issues and their trends.

- Regular automated scans of the environment(s) against DISA STIG.
- Coverage of all major components of the environment, including interdependency mapping.
- Detailed explanations of each finding, including details as to how these can be manually audited and any issues reported can be remediated.
- Mapping of any findings to the specific Vulnerability
- ID detailed in DISA STIG.
- Each finding should include Impact, Importance, and Risk Rating to allow for prioritization of
- remediation effort.

DORA

The Digital Operational Resilience Act (DORA), Regulation (EU) 2022/2554, is a European Union regulation aimed at standardizing and enhancing digital operational resilience across the financial sector. It is designed to ensure that all regulated financial entities can anticipate, adapt to, withstand, recover from, and learn from operational disruptions. These disruptions could include everything from cyberattacks to natural disasters.

The regulation focuses on several key areas:

- Risk Management: It mandates financial institutions to identify, classify, and manage all risks related to their digital operations.
- Testing: Financial institutions are required to conduct regular tests, potentially including stress tests, to assess how well they can withstand various types of disruptions.
- Incident Reporting: DORA requires a formal procedure for reporting operational incidents, both internally and to regulatory authorities. This enables a more coordinated response to incidents affecting financial stability.
- Information Sharing: The Act promotes the exchange of information among financial institutions to help better understand and counter common threats.
- Oversight: Regulatory authorities are given enhanced powers to monitor compliance and to intervene as necessary to maintain the stability and integrity of the financial system.
- Third-Party Risk Management: calls for conducting thorough assessments and continuous monitoring of risks related to third-party service providers. IT practitioners must establish and enforce risk management protocols to align with DORA's standards.
- Technology Investment: entails aligning with up-to-date technology standards for risk detection, prevention, and mitigation. IT practitioners are responsible for evaluating, selecting, and implementing necessary technologies and tools that adhere to DORA's requirements.

Pain Points

Financial Cost

- Initial Investment: Comprehensive risk assessment, new software and hardware systems, and cybersecurity measures can be expensive to implement initially.
- Ongoing Costs: Continuous monitoring, regular audits, and mandatory reporting can result in recurring expenses.

Operational Challenges

- Complexity: The regulation often involves intricate requirements that may be hard to understand and implement effectively.
- Resource Allocation: Meeting the stringent standards might require reallocating resources from other pressing issues or departments.
- Legacy Systems: Older infrastructures may need to be updated or replaced, which can be a long and painful process.

Skill Gaps

- Expertise: Specialized knowledge in cybersecurity, risk management, and compliance is required, and organizations may not have this expertise in-house.
- Training: Existing staff may require additional training to understand and comply with the new requirements, which takes time and money.

Interoperability and Compatibility

- System Integration: The various tools and solutions needed to meet compliance requirements may not easily integrate with existing systems.
- Data Sharing: Sharing sensitive data across entities for risk assessment and resilience planning may raise security and privacy concerns.

Legal and Compliance Risks

- Non-Compliance Penalties: Failure to meet the regulations may result in severe financial and reputational damage.
- Ambiguity: Any lack of clarity in the regulation's language could lead to varied interpretations, potentially resulting in unintentional non-compliance.

Time Constraints

- Implementation Time: Rolling out all the required measures to be in full compliance often takes significant time, which may be challenging if the regulatory deadlines are tight.

Cultural Challenges

- Organizational Culture: Adapting to a more compliance-focused culture can be a challenge for some organizations.
- Employee Resistance: There may be internal resistance to new protocols, requiring a change management strategy.

Addressing these challenges often involves a multi-disciplinary approach, drawing from legal, technological, operational, and financial expertise. Many organizations also need to seek help from external consultants and compliance solutions providers adding additional cost.

Requirements for Automated DORA Compliance

- Summary of existing DORA configuration issues and their trends.
- Regular automated scans of the environment(s) against the DORA regulation.
- Coverage of all major components of the environment, including interdependency mapping.
- Detailed explanations of each finding, including details as to how these can be manually audited and any issues reported can be remediated, ensuring even the most junior admin can remediate issues.
- Each finding should include Impact, Importance, and Risk Rating to allow for prioritization of remediation effort.
- Compliance audits according to the DORA regulation.
- Historical reporting going back for at least a year.
- Ability to check on-premises and cloud resources.
- 24/7 visibility into your audit compliance posture.
- A solution that can run entirely on-premises, with no data leaving your control.

Essential Eight

The Essential Eight compliance is designed to protect Microsoft Windows based networks which are connected to the internet. It was not designed to cover cloud infrastructures, the ACSC provides alternative guidance for these technologies.

When implementing the Essential Eight, organizations should identify a level from the Essential Eight maturity model, using a risk-based approach, that suits their requirements for a security framework.

The maturity model has four levels and as stated by the ACSC, "Maturity Level Three will not stop adversaries that are willing and able to invest enough time, money and effort to compromise a target. As such, organizations still need to consider the remainder of the mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* and the *Information Security Manual*."

From:
https://www.cyber.gov.au/acsc/view-all-content/publications/essential- eight-maturity-model

Maturity levels are based on weaknesses which can be exploited by external threats.

Maturity level 0
Exploitation of weaknesses which could compromise the confidentiality or integrity of systems and data.

Maturity level 1
Exploitation of unpatched security vulnerabilities, or access to systems via stolen, reused, brute forced or guessed user credentials for the purpose of launching malicious applications.

Maturity level 2
Attackers use phishing and social engineering techniques to gain access through selective targeting of accounts with special privileges.

Maturity level 3
Attackers use cyber security posture weaknesses such as older software or inadequate logging and monitoring. Immediate use of exploits are employed as soon as they become public knowledge, multi-factor authentication is evaded by stealing authentication token values to impersonate a user, and privileged credentials or password hashes are used to hide their digital footprint allowing free reign on environments.

Mitigation strategies are detailed on the Essential Eight maturity model web page.

Pain Points

The Australian federal government is mandating compliance across all eight controls of the framework.

Many organizations struggle to implement the top four controls, let alone all eight to prevent and limit attack impact, and data availability to external and internal attacks.

Administrators struggle to translate the Essential Eight mitigation strategies into actionable remediation.

Requirements for automated Essential Eight compliance

- Application control.
- Patch applications.
- Configure Microsoft Office macro settings.
- User application hardening.
- Restrict administrative privileges.
- Patch operating systems.
- Multi-factor authentication.
- Regular backups.

GDPR

The General Data Protection Regulation (GDPR) became enforceable under European Union (EU) law on 25 May 2018, replacing the EU Data Protection Directive. As an EU regulation, it applies to the personal data of EU citizens. Therefore, it is a regulation that applies to any organization that processes or stores the personal information of EU citizens, regardless of where that organization is located.

This includes organizations outside the EU that offer goods or services to individuals in the EU or monitor the behavior of individuals in the EU.

Pain Points

GDPR implementation typically takes longer than anticipated, and penalty amounts for noncompliance are influenced by various factors, such as the severity of the incident, the number of compromised data sets, and the annual global financial turnover of the organization. Reported fines have ranged from multiple thousands, to multiple hundreds of millions of euros.

In the first two years after GDPR compliance enforcement went into effect, there were a total of 391 cases made public in which authorities raised fines against both private companies and public organizations. In just over two years following enforcement, GDPR violations caused by breaches of articles 25 and 32 alone totaled 97 of those cases. Fines for infringements of just those two articles together average at 7.07 million euros and totaled 395.3 million euros in fines paid. One of the primary GDPR security requirements to address is needing to communicate a reportable data breach to the relevant regulators within 72 hours of becoming aware of the event, and an organization's ability to communicate such in time can be incredibly challenging.

In responses to a GDPR implementation survey carried out by Ponemon Institute that involved 1,263 responding organizations:

- Almost half of reportable breaches during the first two years since implementation were caused by negligent insiders, followed by outsourcing data to a third party and cyber-attacks.
- About one-third of organizations that experienced breaches reported that they did not know what caused the breach.

While vendors do much to cover GDPR compliance issues, responsibility also rests on organizations to maintain compliance.

Despite attempts to segment services by region, it is possible for organizations to accidentally violate GDPR compliance due to some global services going across sovereign borders. As an example of this, the official AWS presentation on GDPR states that "Customers are responsible for their security and compliance in the cloud. AWS is responsible for the security of the cloud." In that same presentation, AWS recommends four key categories of GDPR Compliance Tools:

- Data Access Control.
- Monitoring of Access Activities.
- Data Encryption.
- Strong Compliance Framework.

As with any standards, it can happen that even if you're doing your best to manually achieve security compliance, it's not possible to keep track of all updates and changes in your environment – and to the standard – at the same time.

Requirements for automated GDPR compliance

- Proactive checks against GDPR regulations in your environment, to ensure compliance without spending vital time on manual checks.
- Compliance audits according to GDPR regulations.
- Checks should map directly to the relevant articles of the regulation.
- Checks should map against the relevant category within the regulation: Data Access, Data Protection, Monitoring & Logging.
- Where automated checks cannot validate compliance, the user should be periodically prompted for a manual check and response.

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the Secretary of the U.S Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule.

Pain Points

HIPAA security checks add another layer of complexity when analyzing the virtual environment. The rules and regulations cover three key aspects of healthcare delivery: electronic data interchange (EDI), security, and privacy.

Health plans must accept and respond to all transactions in the EDI format. Security policies and procedures that protect the accuracy and integrity of information and limit access must be applied. Privacy must be enforced on how information is used and disclosed. Security and privacy regulations require administrative, physical, and technical safeguards – which can be complex for sysadmins to understand and remediate against.

Requirements for automated HIPAA compliance

- Summary of the existing HIPAA configuration issues and their trends.
- Continuous monitoring for old and new HIPAA privacy and security violations.
- Detailed list of all issues in VMware environments, including the number of affected objects and related VMware products.
- Detailed explanations of each check, with full technical details for remediation.
- Automated remediation for a HIPAA- compliant environment.
- Mapping of each finding to the Rule ID detailed within the HIPAA standard.
- Findings listed by severity in order to allow prioritization of remediation.

ISO/IEC 27001

Anyone working in IT will have undoubtedly encountered ISO/IEC 27001 by now. First published jointly in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), it has been updated several times since. The ISO/IEC 27001 is designed to be an international standard to assist organizations in knowing how best to manage information security.

Also known as ISO 27001 (without 'IEC'), the standards are internationally agreed upon by security experts. Such consensus-based standardization provides a more commonly understood framework for identifying security risks that can lead to information misuse or full data breaches. Thus, ISO helps manage the security of an organization's information assets, including (but not limited to) customer data, financial data, or intellectual property.

Pain Points

Complying with ISO 27001 standards requires the design and implementation of coherent and comprehensive information security controls to address any risks deemed unacceptable.

Additionally, it means adopting overarching security measures to ensure that those controls continue to meet the organization's requirements as they evolve over time.

Finally, it requires regular, systematic auditing of information security risks within the organization, accounting for threats/vulnerabilities and potential impacts.

On top of the ongoing issues that IT admins manage daily, ISO 27001 poses the following additional challenges to deal with:

- Certification is a multi-level process.
- Covers much more than just IT.
- Audits required more frequently in the beginning, then at least annually .
- Certification auditor decides which controls get tested/
- Organizations managing to comply in every way often lack a way to prove such There are 114 controls in 14 groups and 35 control categories; the 2005 standard had 133 controls in 11 groups.
  - A.5: Information security policies (2 controls).
  - A.6: Organization of information security (7 controls).
  - A.7: Human resource security - 6 controls that are applied before, during, or after employment.
  - A.8: Asset management (10 controls).
  - A.9: Access control (14 controls).
  - A.10: Cryptography (2 controls).
  - A.11: Physical and environmental security (15 controls).
  - A.12: Operations security (14 controls).
  - A.13: Communications security (7 controls).
  - A.14: System acquisition, development, and maintenance (13 controls).
  - A.15: Supplier relationships (5 controls).
  - A.16: Information security incident management (7 controls).
  - A.17: Information security aspects of business continuity management (4 controls).
  - A.18: Compliance; with internal requirements, such as policies, and with external requirements, such as laws (8 controls).

A common pain point (for any who may have somehow managed to keep up with compliance manually) has been a lack of confirmation or assurance that the standards have been and continue to be met.

Requirements for automated ISO 27001 compliance

- Comprehensive automated ISO/IEC 27001 compliance audits for VMware and AWS infrastructures.
- Historical reporting going back for at least a year.
- Ability to check VMware vSphere, VMware NSX and native AWS public cloud resources.
- Visibility of details related not only to impacted objects, but also both the wording from the standard and a technical translation.
- Clear instructions for how to manually audit the finding and remediate any non- compliances.
- 24/7 visibility into your audit compliance posture.
- Complete visibility into risks and non- compliances inherent in your environment, allowing you to identify gaps between where you are and a fully compliant state.
- A solution that runs entirely on-premises, with no data leaving your control.

KVKK

Kişisel Verileri Koruma Kanunu (KVKK) is the Turkish Personal Data Protection Law No. 6698, which regulates personal data protection and outlines legal obligations that entities and individuals dealing with personal data must comply with. KVKK is based on GDPRs predecessor and comes with its own individual set of requirements which do not all align with the latest GDPR regulations.

KVKK applies to entities and individuals who process data about Turkish citizens, whether Turkish or foreign entities. All data controllers are required to register on VERBIS where they must record all data processing activities they take part in. Failure to register with VERBIS can result in fines and/or the restriction of the controller's data processing activities.

Pain Points

KVKK provides guidelines which need to be adhered to. Understanding how these guidelines apply to technologies in the data center is a complex undertaking. By trying to manually achieve security compliance, it's not possible to keep track of all updates and changes in your environment, making it harder to achieve and stay on top of compliance.

Automated solutions that provide AI driven services must ensure accountability for all stakeholders, in terms of compliance with the personal data protection law, starting from the design of products and services throughout their entire life cycle. Finding a platform that conforms to this can be challenging when looking for a solution to implement in the data center.

The Personal Data Protection Law No. 6698, imposes serious administrative fines, of up to 1,800,000 Turkish lira, on institutions and business owners, who break this law and in some cases, prison sentences, between one and four years, can be imposed.

Companies including Microsoft, Facebook and Marriott International have all been fined for not taking necessary technical and organizational measures to ensure data security within scope of the Article 12(1) of the Law and for not notifying the breach to the Board within the shortest time in line with the Article 12(5) of the Law.

Requirements for automated KVKK compliance

- Automated KVKK guideline checks.
- Coverage of both on-premises and cloud-based services.
- On-premises analysis – with no data sent off-site. Detailed history of findings for historical automated scans.
- Full reporting capabilities to prove KVKK compliance.

NIST

The National Institute of Standards and Technology (NIST) published the NIST special publication (SP) 800-53, which offers security and privacy controls for federal information systems and organizations. According to the Office of Management and Budget (OMB), the NIST standards and policies are mandatory for all non-national security systems run by federal agencies in the US.

Pain Points

To protect both data and information systems, federal agencies have to meet the requirements of the Federal Information Security Management Act (FISMA). By means of its SP 800-53, NIST offers the security controls to help those federal agencies comply with FISMA, in addition to common best practices and other standards such as FIPS 200.

Validating your entire virtual environment based on all currently published NIST controls can be a painstakingly long and ongoing endeavor. Without continuous monitoring and fast-guided remediation in accordance with all applicable NIST controls, risks can stay undetected or unmitigated until discovered by an audit.

As a result, workloads increase rapidly in the run-up to an audit, and other tasks can get delayed. To take back control and avoid any “panic-driven” pre-audit scenarios, it is crucial to make audit preparations a part of your daily routine. To avoid slowing down any of your daily operations as a result of such continuous effort, it is necessary to drastically reduce costs and time spent by automating any repetitive steps in your security lifecycle.

Requirements for automated NIST compliance

- Summary of the existing NIST configuration issues and their trends.
- Details of the NIST 800-53 controls to be remediated.
- Coverage of both on-premises and cloud- based services.
- Guided remediation to show exactly how to remove detected vulnerabilities.
- Document accountability and traceability of changes.
- Detailed NIST compliance history.
- Extensive reporting, with findings listed by severity in order to allow prioritization of remediation.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an IT security standard for organizations that are involved in handling credit cards and their associated data. While administered by the Payment Card Industry Security Standards Council, the PCI Standard is mandated by the card brands, with the aim to tighten controls around cardholder data and reduce credit card fraud.

Pain Points

For many IT departments – especially in the financial sector, greatly subject to PCI DSS regulations – security auditing and compliance are a continuous challenge due to the complexity of requirements. PCI DSS comprises 12 compliance requirements for building and maintaining a secure network. Compliance validation occurs at regular intervals, performed by a certified assessor.

These 12 requirements are further broken down into additional groups known as control objectives, which cover a broad range of security processes for business continuity and consumer protection.

Requirements for automated PCI DSS compliance

- Identification of non-compliances and vulnerabilities.
- Capability to customize checks where business risk posture requires higher standards than the baseline requirements.
- Coverage of both on-premises and cloud- based services.
- Continuous monitoring for PCI-DSS violations.
- Address Control ID and Milestone aspects of the standard.
- Provides historical analysis, with full reporting capabilities.
- Provide automation for remediation against PCI DSS controls.
- Coverage of vulnerability management and risk assessment.
- Support for the most up-to-date revision of the standard (3.2.1, released May, 2018).
- View specific and full content from the relevant control and context from the relevant requirement area for all non- compliance checks.
- Prioritize remediation actions according to PCI DSS security milestones.
- Provide a fully-justified view on how a specific automated check relates to a specific control in the standard, and (where applicable) where it relates to certain sub-sections of the control.
- Detailed technical descriptions that map the PCI standard to specific environments, including details for manual auditing and remediation.

TISAX

TISAX (Trusted Information Security Assessment Exchange) is a framework for information security evaluation in the automotive industry. It was developed by the German Association of the Automotive Industry (VDA) and is designed to standardize information security assessment across the automotive supply chain.

TISAX assessments are performed by accredited third-party assessors who evaluate a company's information security management system (ISMS) against the TISAX requirements. The results of the assessment are then shared through the TISAX Assessment and Exchange Platform, which allows companies to exchange assessment results with their partners in a standardized and secure manner.

By implementing TISAX, companies in the automotive industry can demonstrate their commitment to information security and build trust with their partners. It also helps to ensure that the entire supply chain is secure, reducing the risk of cyber attacks and data breaches.

Pain Points

Companies in the automotive supply chain are required to comply with TISAX if they want to work with leading automotive manufacturers.

The TISAX assessment process is complex and time-consuming. It requires companies to undergo a thorough security assessment and to demonstrate compliance with a broad range of security standards and requirements. The cost of complying with TISAX can be significant, especially for small and medium-sized enterprises (SMEs). The cost includes hiring external auditors, implementing security controls, and maintaining compliance.

Many companies may lack the necessary resources and expertise to carry out the TISAX assessment and implement the required security controls. This can lead to delays in the assessment process and increase the risk of non-compliance and TISAX compliance is not a one-time event. Companies need to continuously monitor their security posture and improve their security controls to maintain compliance. This requires ongoing investment and commitment to information security.

Requirements for automated TISAX compliance

- Identification of non-compliances and vulnerabilities.
- Coverage of both on-premises and cloud-based services.
- Continuous monitoring for TISAX violations.
- Provides historical analysis, with full reporting capabilities.
- Provide automation for remediation against TISAX controls.
- Coverage of vulnerability management and risk assessment.
- View specific and full content from the relevant control and context from the relevant requirement area for all non- compliance checks.
- Prioritize remediation actions according to TISAX security controls.
- Provide a fully-justified view on how a specific automated check relates to a specific control in the standard, and (where applicable) where it relates to certain sub-sections of the control.
- Detailed technical descriptions that map the TISAX standard to specific environments, including details for manual auditing and remediation.

VMware Security Configuration Guide

Security hardening guides provide prescriptive guidance for customers on how to deploy and operate VMware products in a secure manner.

Some organizations are not obliged to stay compliant against all of the specific security compliance standards. At the same time, they still need to build an internal security policy where the vendor's security guidelines are used as a starting point.

Pain Points

Not all System Admins are VMware security experts, and keeping up to date on security vulnerabilities is both time-consuming and costly. Scouring the entire VMware Security Configuration Guide to find where issues lie, removes System Admins from the ability to be proactive in other areas of their work.

Rectifying potential issues before they impact upon your production environment is also time-consuming, and reactive remediation after issues have occurred can lead to data breaches and downtime. Time spent discovering issues needs to be dramatically reduced by an automated solution that can provide instant answers, to allow System Admins to spend their time proactively remediating and staying ahead of the curve on security issues.

Requirements for automated VMware security

- Automated checks against the VMware Security Configuration Guide.
- Granular filtering functionality to customize analysis and reporting based on your organization's Security Policies.
- Security gaps need to be explained and immediate answers provided for auditing and remediation.
- Automation of remediation is required in order to minimize time to compliance.
- Historical views of the security compliance posture
- should be provided against specific security compliance baselines, with full reporting capabilities.
- Findings listed by severity in order to allow prioritization of remediation.

Summary: Achieving Compliance

Staying compliant with security standards and keeping up with the latest changes and updates is extremely time-consuming. Standards documentation can be challenging to understand for Security and Operations teams, as it is often written from a technology-agnostic perspective. Time spent reactively searching for answers is time that could be better spent proactively delivering business value.

It is paramount for security compliance to be approached in a proactive manner, ensuring that System Admins get ahead of the curve rather than remain locked in a firefighting paradigm. Securing environments against the most recent gaps and vulnerabilities ensures data security and provides continuity of service and brand assurance that customers can depend on.

Security and Operations teams require a solution that mitigates the necessity to spend hours checking through security hardening guides and compliance documents. Countless business hours can be saved by preventing these issues rather than fixing them after the event.

Predictive and actionable intelligence for System Admins must provide a detailed onestop look at the past, present, and future of environments – removing the need for admins to troubleshoot by providing 100% transparency on risks and security noncompliance.

The future of security is a solution which provides proactive analysis, immediate remediation answers, clear language, granular reporting, and depth of understanding.

The solution should mitigate lost time and associated costs incurred from troubleshooting complex issues in a limited and reactive capacity. By switching to a more proactive model, you can discover potential risks and provide admins with remediation solutions before any issues can develop into a major outage or security breach.

As both Security and Operations teams are pushed to mitigate risks to business, automation should be used to free up time for innovative work that creates even greater business value. With a solution that brings all of the answers to their fingertips, even an inexperienced technician can be enabled as if a seasoned expert.

Using a platform like Runecast enables Data Centers to become more secure, business time and money to be saved, and brand expectation to be upheld – ensuring continuity of service and customer trust.

It is also the only solution on the market (at the time of this publication) that addresses all of the automated security compliance requirements detailed above.

About Runecast

Runecast Solutions Ltd. is a leading global provider of a patented, AI-powered proactive vulnerability management and cloud-native application protection platform (CNAPP) for security, compliance, risk mitigation, and more efficient IT Operations Management (ITOM). Forward-focused enterprises like Avast, the German Aerospace Center (DLR), and Merck/MSD rely on Runecast for proactive vulnerability and configuration management, security and compliance assessment, operational efficiency, and mission-critical stability. Headquartered in London, U.K., Runecast is a Gartner Cool Vendor, is recommended by CISA, and has won Computing awards for Enterprise Threat Detection, Cloud Security Product of the Year, and Best Place to Work in Digital. See more at www.runecast.com.