STORM GRC – Cloud SaaS Platform for Automated Cyber Risk & Compliance Management

Πρόκληση

Η **Διαχείριση Ασφάλειας** είναι μια συνεχής και συστηματική διαδικασία *προσδιορισμού*, *ανάλυσης*, *χειρισμού* και *παρακολούθησης* των επιχειρησιακών κινδύνων ενός οργανισμού. Στόχο έχει την προστασία των Πληροφοριακών Συστημάτων (ΠΣ) από εσωτερικούς και εξωτερικούς κινδύνους που θα μπορούσαν να επηρεάσουν αρνητικά την επίτευξη των επιχειρησιακών στόχων του οργανισμού και την ομαλή λειτουργία του.

Οι απαιτήσεις συμμόρφωσης συνεχώς αυξάνονται και προέρχονται πλέον όχι μόνο από νέους κανονισμούς και οδηγίες αλλά και από τους ίδιους τους πελάτες εξαιτίας της νέας πραγματικότητας στο η- επιχειρείν αλλά και την αλματώδη αύξηση του ανταγωνισμού.

Ανάλογα με τον κλάδο δραστηριοποίησης, οι οργανισμοί πρέπει να ανταποκριθούν σε πολυσύνθετες απαιτήσεις όπως:

- **Cloud providers & διεθνή πρότυπα:** ISO 27001, ISO 27018, ISO 27019, SOC 1 / SOC 2 / ISAE 3402, CSA.
- **Προστασία προσωπικών δεδομένων:** GDPR, CCPA, Canada Digital Charter κ.λπ.
- **Κρίσιμες υποδομές & εθνικοί κανονισμοί:** NIS 2, ΑΔΑΕ.
- **Χρηματοοικονομικός κλάδος:** DORA, PCI DSS.
- **Εξειδικευμένοι τομείς:** ναυτιλία (IMO, BIMCO, TMSA), βιομηχανία (ICS), ενέργεια κ.ά.

Η πολυπλοκότητα, η διαφορετικότητα και η συχνή επικαιροποίηση αυτών των απαιτήσεων καθιστούν δύσκολη τη διατήρηση ενιαίας εικόνας συμμόρφωσης και οδηγούν σε αυξημένο λειτουργικό κόστος, πολλαπλά εργαλεία, χαοτική τεκμηρίωση και έλλειψη ορατότητας σε πραγματικό χρόνο.

Αυτό δημιουργεί ένα θεμελιώδες ζήτημα: οι οργανισμοί χρειάζονται ένα **ενιαίο, αυτοματοποιημένο, cloud-based GRC περιβάλλον** που να διασφαλίζει συνεχή συμμόρφωση, επιχειρησιακή αποτελεσματικότητα και αντικειμενική διαχείριση κινδύνων.

Λύση

Το **STORM GRC** αποτελεί μία πλήρως αυτοματοποιημένη και παραμετροποιήσιμη cloud πλατφόρμα Governance, Risk & Compliance, σχεδιασμένη για οργανισμούς κάθε μεγέθους και πολυπλοκότητας. Ενοποιεί σε ένα περιβάλλον όλες τις κρίσιμες λειτουργίες ασφάλειας πληροφοριών, προστασίας δεδομένων, διαχείρισης κινδύνων και ελέγχου συμμόρφωσης.

Η πλατφόρμα ενσωματώνει διεθνή πρότυπα (ISO 27001 / 27002 / 22301, NIST CSF, SOC 2, GDPR, DORA, NIS 2) και εξειδικευμένο περιεχόμενο ανά κλάδο, επιτρέποντας στους χρήστες να:

- προσδιορίζουν, αξιολογούν και κατηγοριοποιούν περιοχές επικινδυνότητας,
- αναγνωρίζουν επιχειρησιακές επιπτώσεις από περιστατικά ασφάλειας,
- διενεργούν τυποποιημένη διαχείριση κινδύνων και να επιλέγουν κατάλληλα μέτρα προστασίας,
- αναπτύσσουν και επικαιροποιούν πολιτικές και διαδικασίες,
- υλοποιούν εσωτερικούς ελέγχους βάσει προτύπων και κανονισμών,
- εξασφαλίζουν συνεχή και τεκμηριωμένη συμμόρφωση.

Βασικές Λειτουργίες του STORM GRC

1. Risk & Compliance Management

- Αποτύπωση υπηρεσιών, διαδικασιών και αλληλεξαρτήσεων.
- Δημιουργία και ανανέωση Asset Models.
- DPIA, BIA, Threat & Vulnerability Assessments.
- Risk Treatment με βάση ISO 27002 και NIST CSF.
- Real-time risk mapping, heatmaps, residual risk monitoring.
- Αυτοματοποιημένο Risk Register & Risk Treatment Plan.

2. Security Governance & ISMS Operations

- Παραγωγή/αναθεώρηση πολιτικών & διαδικασιών (ISO 27001/27002).
- Δημιουργία BCP & DRP (ISO 22301).
- Τεχνικοί έλεγχοι αδυναμιών & ενσωμάτωση αποτελεσμάτων Pen Tests.
- Αναφορές περιστατικών & ticketing για remediation actions.
- Δημιουργία Statement of Applicability.
- Καταγραφή ευρημάτων εσωτερικών επιθεωρήσεων & ISMS Review Meetings.

3. Compliance Dashboard

- Καταγραφή των πρακτικών των συναντήσεων ανασκόπησης του Συστήματος Διαχείρισης Ασφάλειας (ISMS Review Meetings Minutes).
- Ανάθεση διορθωτικών ενεργειών στους κατάλληλους χρήστες προς υλοποίηση μέσω του Ticketing Module.
- Παρακολούθηση της πορείας όλων των διορθωτικών ενεργειών
- Δημιουργία compliance reports βάσει συγκεκριμένων απαιτήσεων (ISO 27001, ISO 27017, ISO 27018, NIST CSF, GDPR, DORA, NIS 2, ΑΔΑΕ , SOC 2).
- Αξιολόγηση ασφάλειας συνεργατών / προμηθευτών (Third Party Risk Assessments) βάσει συγκεκριμένων απαιτήσεων (ISO 27001, ISO 27017, ISO 27018, NIST CSF, GDPR, DORA, NIS 2, ΑΔΑΕ , SOC 2).

4. Reporting & Regulatory Alignment

Αυτοματοποιημένη παραγωγή compliance reports για:
ISO 27001, ISO 27017, ISO 27018, NIST CSF, GDPR, DORA, NIS 2, ΑΔΑΕ, SOC 2.

5. Third-Party Risk Management

- Αξιολόγηση προμηθευτών βάσει προτύπων και κανονισμών.
- Ανάθεση ερωτηματολογίων και βαρύτητα αξιολόγησης
- Τεχνικός έλεγχος του public exposure του προμηθευτή (π.χ. εμπλοκή σε προηγούμενα breaches, κλπ)
- Παρακολούθηση διορθωτικών ενεργειών.

6. Security Awareness & Industry-Specific Content

- Wiki, Forum, online training, αξιολόγηση εκπαίδευσης.
- Προκαθορισμένες απειλές, ευπάθειες & μέτρα προστασίας ανά asset type.
- Εξειδικευμένα μοντέλα για ICS, maritime, χρηματοοικονομικό κλάδο κ.λπ.

Μετρήσιμα Αποτελέσματα (KPIs)

Η εφαρμογή του STORM GRC έχει αποφέρει σημαντικά επιχειρησιακά οφέλη σε μεγάλους και μικρομεσαίους οργανισμούς:

- **έως 60% μείωση** του χρόνου προετοιμασίας για audits & inspections (ISO 27001, NIS 2, DORA),

- **40–50% μείωση** του απαιτούμενου FTE για evidence collection, documentation & reporting,
- **έως 50% ταχύτερη** ολοκλήρωση risk assessments και παραγωγής risk treatment plans,
- **έως 80% μείωση** του χρόνου παραγωγής compliance reports μέσω αυτοματοποίησης,
- **30% αύξηση** της ωριμότητας συμμόρφωσης κατά τον πρώτο χρόνο χρήσης,
- σημαντική **μείωση operational remediation time** μέσω ticketing & workflow mechanisms,
- **ενιαία ορατότητα** σε πραγματικό χρόνο για όλους τους επιχειρησιακούς κινδύνους.

Τα παραπάνω αποδεικνύουν τον ουσιαστικό αντίκτυπο της πλατφόρμας, τόσο σε επίπεδο ασφάλειας όσο και σε μείωση κόστους και βελτίωση παραγωγικότητας.

Η υιοθέτηση του STORM GRC προσφέρει στους οργανισμούς:

- πλήρη αποτύπωση κρίσιμων υπηρεσιών, αγαθών και αλληλεξαρτήσεων,
- ακριβέστερη αξιολόγηση της τρωτότητας συστημάτων & υποδομών,
- αντικειμενική και ενοποιημένη διαχείριση κινδύνων,
- δυνατότητα πολλαπλής συμμόρφωσης με ένα μόνο assessment (π.χ. GDPR, DORA , NIS 2),
- σαφή καθορισμό και παρακολούθηση των μέτρων ασφάλειας ανά πρότυπο/κανονισμό,
- διαρκή καταγραφή, παρακολούθηση και τεκμηρίωση διορθωτικών ενεργειών,
- ενιαίο σημείο αναφοράς για compliance & cybersecurity governance,
- μείωση χρόνου προετοιμασίας αναφορών και επιθεωρήσεων,
- συστηματική παρακολούθηση KPIs και επιχειρησιακών στόχων,
- ενίσχυση της κουλτούρας ασφάλειας σε όλο το οργανωτικό οικοσύστημα.

Το STORM GRC μετατρέπει την πολυπλοκότητα του GRC σε μια αυτοματοποιημένη, αποδοτική και κλιμακώσιμη διαδικασία, επιτρέποντας στους οργανισμούς να ευθυγραμμίζονται με τις regulatory expectations και να ενισχύουν την επιχειρησιακή τους ανθεκτικότητα.