Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Πληροφοριακά και Επικοινωνιακά Συστήματα*

Μεταπτυχιακή Διατριβή

Η εφαρμογή και χρησιμοποίηση Security SDLD σε συνδυασμό τον Ευρωπαϊκό κανονισμό (ΕΕ) 2016/679 δίνοντας έτσι επιχειρηματική αξία (business value) σε έναν οργανισμό.

Αντώνιος Μανώλης

Επιβλέπων Καθηγητής
Δρ. Νικόλαος Σκλάβος

Δεκέμβριος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών *Πληροφοριακά και Επικοινωνιακά Συστήματα*

Μεταπτυχιακή Διατριβή

Η εφαρμογή και χρησιμοποίηση Security SDLD σε συνδυασμό τον Ευρωπαϊκό κανονισμό (ΕΕ) 2016/679 δίνοντας έτσι επιχειρηματική αξία (business value) σε έναν οργανισμό.

Αντώνιος Μανώλης

Επιβλέπων Καθηγητής
Δρ. Νικόλαος Σκλάβος

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου
σπουδών στα Πληροφοριακά Συστήματα
από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου.

Δεκέμβριος 2019

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Σκοπός της μεταπτυχιακής διατριβής είναι να διερευνηθούν οι δυνατότητες δημιουργίας και ανάπτυξης ενός δυναμικού εργαλείου το οποίο θα βασίζεται στο μοντέλο SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού) του οργανισμού OWASP και στο νέο Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation), 2016/679. Έχοντας από τις 25 Μαΐου 2018 πλέον τεθεί σε υποχρεωτική εφαρμογή για τα κράτη-μέλη της Ευρωπαϊκής Ένωσης ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation), και οπού σύμφωνα με τον παρόν κανονισμό όποιος οργανισμός επεξεργάζεται διαχειρίζεται και διανέμει προσωπικά δεδομένα, θα πρέπει αυτό να λαμβάνει χώρα υπό συγκεκριμένους όρους και προϋποθέσεις καθώς η όποια μη συμμόρφωση θα τιμωρείται πλέον με πρόστιμο.

Οι στόχοι της μεταπτυχιακής διατριβής περιλαμβάνουν την διερεύνηση και τον προσδιορισμό αυτών των δυο προτύπων, τόσο του μοντέλου SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού) όσο και του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation), και κυρίως τον τρόπο με τον οποίο τα χαρακτηριστικά και οι απαιτήσεις τους καλύπτουν τον κύκλο ζωής ανάπτυξης ενός λογισμικού.
Μετά από εισαγωγή δεδομένων στο εργαλείο, θα ελέγχεται κατά πόσον το τελικό αποτέλεσμα είναι εναρμονισμένο με τα δυο παραπάνω πρότυπα.

Ως εκ τούτου, μελετάται και παρουσιάζεται η σχετική με το θέμα υπάρχον βιβλιογραφία πολλών και επιμέρους θεμάτων. Έχει μελετηθεί ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation), η έννοια της ιδιωτικότητας και του απορρήτου των δεδομένων, το μοντέλο SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού), η έννοια της Ανάπτυξης του Συστήματος Ασφαλείας σε ένα κύκλο ζωής ανάπτυξης λογισμικού, ο ίδιος κύκλος ζωής ανάπτυξης λογισμικού με απώτερο σκοπό να καθοριστούν οι τελικές προδιάγραφες του υπό ανάπτυξη εργαλείου καθώς και τα απαιτούμενα κριτήρια για την ανάπτυξη του εργαλείου. Στα επιμέρους θέματα έχει εξεταστεί στην παρούσα βιβλιογραφία ότι στην προοπτική ενός οργανισμού, η ασφάλεια είναι μια επένδυση που εκτιμάται ως εξοικονόμηση κόστους λόγω μειωμένων ζημιών από τις εκάστοτε παραβιάσεις ασφαλείας [1].

Αφού αναλύθηκε η υπάρχουσα βιβλιογραφία, προσδιορίζονται και αναλύονται οι τεχνικές που θεωρούνται κατάλληλες για την δημιουργία του πρακτικού αποτελέσματος και τέλος παρουσιάζεται η διαδικασία υλοποίησης και το τελικό πρακτικό αποτέλεσμα.

Επιπρόσθετα, καθώς η τεχνολογία προχωράει και νέα πρότυπα δημιουργούνται και άλλα εξελίσσονται, έχει εξεταστεί και η σχετική βιβλιογραφία από την σκοπιά των ασύρματων δικτύων 4ης γενιάς [2] και του διαδικτύου των πραγμάτων (Internet of things) [3], καθώς το εργαλείο που θα αναπτύξουμε θα μπορούσε υπό προϋποθέσεις να εφαρμοστεί σε αυτές τις δύο τεχνολογίες και πρότυπα.

Summary

The purpose of the master thesis is to investigate the possibilities of creating and developing a checking tool based on the OWASP model SAMM (Software Assurance Maturity Model) of the OWASP organization and the new Regulation 2016/679 (GDPR) 2016/679 of the European Parliament and of the Council of the European Union for its member states of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data circulation of such data.

Having adopted the new General Data Protection Regulation (GDPR) as of 25 May 2018, which, in accordance with this Regulation, is currently being implemented by Member States of the European Union, it manages and distributes personal data, this should be done under certain terms and conditions as the non-compliance will now be penalized with a fine.

After importing data into the tool, it will be checked whether the final result is in accordance with the two above mentioned standards. The objectives of the work include the exploration and identification of these two standards and the way their features and requirements cover the life cycle of a software.

Therefore, the relevant literature on several and individual topics is being studied and presented such as, the General Data Protection Regulation, the concept of privacy and data confidentiality, the SAMM (Software Assurance Maturity Model) model, the concept of Developing the Security System in a software development cycle and also the software development life cycle (SDLC) have been studied, trying to define the final specifications of the tool being developed as well as the required criteria for developing the tool. According to the literature review that has been performed on the subtopics, security is an investment serving to reduce expenses due to financial damage caused by security breaches.

A thorough investigation has also been carried out on potentially available tools that combine the SAMM model and the new General Data Protection Regulation (GDPR).

After analyzing the existing literature, the techniques considered appropriate for the practical effect are identified and analyzed. Finally, the implementation process and the final practical result are presented.

In addition, as technology evolves and new standards are introduced and established. The relevant literature has been studied for both 4th generation wireless networks and Internet of Things., as the tool that we are developing can be applied to the aforementioned technologies and standards.

Ευχαριστίες

«...Το δε ζητούμενον αλωτόν, εκφεύγειν δε ταμελούμενον..»

Αυτό που ζητούμε το πετυχαίνουμε, εκείνο που ξεφεύγει είναι ό,τι παρατάμε.

Σοφοκλής, 496-406 π.Χ., Αρχαίος τραγικός (Οιδίπους)

«...Το να κάνεις ό,τι καλύτερο μπορείς, σημαίνει να μη σταματάς ποτέ να προσπαθείς...»

Βενιαμίν Φραγκλίνος, 1706-1790, Αμερικανός πολιτικός & συγγραφέας

Η παρούσα διδακτορική διατριβή αποτελεί το επιστέγασμα μιας μεγάλης προσωπικής προσπάθειας μέσα από δυσκολίες και θυσίες.

Χωρίς την παρακίνηση, την στήριξη και την υποστήριξη, την ανεκτικότητα και την κατανόηση αρκετών ανθρώπων δεν θα ήταν δυνατή η υλοποίηση και η περάτωση αυτής της μεταπτυχιακής διατριβής.

Πρωτίστως, πάνω από όλους θα ήθελα να ευχαριστήσω τον επιβλέποντα μου Δρ. Νικόλαο Σκλάβο, για την αμέριστη στήριξη και κατανόησή του σε κάθε επίπεδο καθ' όλη την διάρκεια της εκπόνησης της μεταπτυχιακής διατριβής. Τον ευχαριστώ προσωπικά για όλες εκείνες τις συμβουλές και τις παρατηρήσεις του για το πως πρέπει να ενεργεί ένας ερευνητής, επαγγελματίας και άνθρωπος, συμβουλές που θα προσπαθήσω να εφαρμόζω σε κάθε πτυχή της πορείας μου.

Ευχαριστίες από καρδίας, στην θεία μου Φωτεινή Μανώλη και τον θείο μου Κώστα Σφήκα για τις γονεϊκες τους συμβουλές και την ψυχολογική τους υποστήριξη, καθώς και στον εξαίρετο φίλο και συνάδελφο Δρ. Εμμανουήλ Σερρέλη για την στήριξή του.

Τέλος, ευχαριστώ με την ψυχή και την καρδιά μου την γυναίκα μου Άμπλα Τζεράχου, για όλη την αμέριστη και ανυπολόγιστη υποστήριξή της κατά την διάρκεια των δύσκολων στιγμών που ήρθαν.

Περιεχόμενα

Κεφάλαιο 1
1 ΕΙΣΑΓΩΓΗ

1.1 Σκοπός εργασίας

Καθώς από τις 25 Μαΐου 2018 τέθηκε σε εφαρμογή ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης, έχει γίνει πια εμφανής η «παρουσία» του σχεδόν σε όλες τις πτυχές του τομέα της τεχνολογίας της πληροφορικής (Information Technology) [4] [5]. Επίσης, έχει γίνει εμφανής η χρήση των μοντέλων διασφάλισης ωρίμανσης λογισμικού [6].

Με γνώμονα τα παραπάνω, δημιουργήθηκε η ανάγκη ενσωμάτωσης των απαιτήσεων του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation) στα μοντέλα διασφάλισης ωρίμανσης λογισμικού.

Βάσει των παραπάνω ως σκοπός της εργασίας τέθηκε η δημιουργία ενός εργαλείου που θα ενσωματώνει τις απαιτήσεις του νέου Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR - General Data Protection Regulation), σε ένα μοντέλο διασφάλισης ωρίμανσης λογισμικού, με σκοπό να απαντηθούν τα εξής ερωτήματα:

- Χρειάζεται να προβλεφθούν οι απαιτήσεις του κανονισμού σε ένα μοντέλο διασφάλισης ωρίμανσης λογισμικού;
- Ποια είναι τα πλεονεκτήματα ενός εργαλείου μοντέλου διασφάλισης ωρίμανσης λογισμικού το οποίο εμπεριέχει την σκοπιά του κανονισμού GDPR;
- Τι δεδομένα μπορούν να εξαχθούν από ένα τέτοιο εργαλείο;

- Θα μπορούσε ένα τέτοιο εργαλείο να χρησιμοποιηθεί σε πραγματικές συνθήκες;

1.2 **Δομή εργασίας**

Η εργασία οργανώθηκε με τον εξής τρόπο:

- Στο Κεφάλαιο 1 – Εισαγωγή, εξηγείται ο σκοπός της εργασίας και αποτυπώνονται οι βασικές έννοιες.
- Στο Κεφάλαιο 2 - Βιβλιογραφική Επισκόπησης, παρουσιάζεται η βιβλιογραφική έρευνα στην οποία βασίστηκε η εργασία ώστε να πραγματοποιηθεί.
- Στο Κεφάλαιο 3 - Μεθοδολογία, εμπεριέχεται ο σχεδιασμός και η μεθοδολογία που εφαρμόστηκε για την επίτευξη της εργασίας.
- Στο Κεφάλαιο 4 – Υλοποίηση, παρουσιάζεται ο τρόπος υλοποίησης του πρακτικού αποτελέσματος της εργασίας.
- Στο Κεφάλαιο 5 – Αποτελέσματα, παρατίθενται τα εξαχθέντα αποτελέσματα βάσει των δοκιμών που έγιναν στο εργαλείο.
- Στο Κεφάλαιο 6 - Ανάλυση Αποτελεσμάτων, πραγματοποιείται η ανάλυση των αποτελεσμάτων που προέκυψαν μέσω των δοκιμών που έγιναν στο εργαλείο.
- Στο Κεφάλαιο 7 – Συμπεράσματα, αποτυπώνεται η κριτική της εργασίας, ο σχολιασμός των αποτελεσμάτων. Τέλος, προτείνονται μελλοντικές επεκτάσεις πρακτικής χρήσης του εργαλείου.

1.3 **Βασικές έννοιες**

Στην ενότητα αυτή θα οριστούν οι βασικές έννοιες οι οποίες θα χρησιμοποιούνται στο υπόλοιπο της εργασίας.

Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) / General Data Protection Regulation (GDPR): Ως Γενικός Κανονισμός Προστασίας Δεδομένων ορίζεται ο Κανονισμός (ΕΕ) 2016/679 για την προστασία των φυσικών

προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών [7].

Ιδιωτικότητα δεδομένων (Data Privacy): Το ιδιωτικό απόρρητο δεδομένων, είναι η πτυχή της τεχνολογίας της πληροφορίας (Information Technology) που ασχολείται με την ικανότητα ενός οργανισμού ή ενός ατόμου να καθορίσει ποια δεδομένα σε ένα σύστημα υπολογιστή μπορούν να μοιραστούν με τρίτους [8].

Μοντέλο ωριμότητας ικανότητας για λογισμικό (Capability Maturity Model for Software): Είναι ένα μοντέλο που βασίζεται σε ένα πλαίσιο ωριμότητας με σκοπό να βοηθήσει τους οργανισμούς να βελτιώσουν τη διαδικασία παραγωγής του λογισμικού τους και την ποιότητα αυτού [9].

Κύκλος ζωής ανάπτυξης λογισμικού(Software Development Life Cycle – SDLC): Ο κύκλος ζωής ανάπτυξης λογισμικού (SDLC) είναι ένας όρος που χρησιμοποιείται στη μηχανική συστημάτων, στα συστήματα πληροφοριών και στην τεχνολογία λογισμικού για να περιγράψει μια διαδικασία σχεδιασμού, δημιουργίας, δοκιμών και ανάπτυξης ενός συστήματος πληροφοριών [4]. Η έννοια του κύκλου ζωής του συστήματος ανάπτυξης εφαρμόζεται σε ένα φάσμα διαμορφώσεων υλικού και λογισμικού, καθώς ένα σύστημα μπορεί να αποτελείται μόνο από υλικό, μόνο από λογισμικό ή από συνδυασμό των δύο [5]. Υπάρχουν συνήθως έξι στάδια αυτού του κύκλου: ανάλυση, σχεδιασμός, ανάπτυξη και δοκιμή, υλοποίηση, τεκμηρίωση και αξιολόγηση.

Κύκλος ζωής ανάπτυξης ασφαλούς λογισμικού (Secure Software Development Life Cycle – Secure SDLC): Ως κύκλος ζωής ανάπτυξης ασφαλούς λογισμικού ορίζεται η σειρά διαδικασιών σε έναν κύκλο ζωής ανάπτυξης λογισμικού, η οποία έχει σχεδιαστεί με τέτοιο τρόπο ώστε να επιτρέπει στις ομάδες ανάπτυξης να δημιουργούν λογισμικό και εφαρμογές κατά τέτοιο τρόπο, ώστε να μειώνονται σημαντικά οι κίνδυνοι ασφάλειας, να εξαλείφονται οι ευπάθειες ασφάλειας και εν τέλει να μειώνεται το κόστος. Η διαδικασία, όπως και ο παραδοσιακός κύκλος ανάπτυξης συστημάτων, χωρίζεται σε διάφορες, διαδοχικές και διακριτές μεταξύ τους φάσεις [10].

Μοντέλο διασφάλισης ωρίμανσης λογισμικού SAMM: Το μοντέλο SAMM (SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού - Software Assurance Maturity Model) είναι ένα πρότυπο ανεπτυγμένο από τον οργανισμό OWASP το οποίο έχει ως σκοπό να προσφέρει την απαραίτητη βοήθεια στους οργανισμούς ώστε να είναι σε θέση να αξιολογούν, να διαμορφώσουν και να εφαρμόσουν μια στρατηγική για την ασφάλεια του λογισμικού. Επίσης δημιουργήθηκε με γνώμονα να μπορεί να ενσωματωθεί είτε σε έναν υφιστάμενο κύκλο ζωής ανάπτυξης λογισμικού σε επίπεδο οργανισμού, είτε σε επίπεδο έργων [11].

Κεφάλαιο 2

2 Βιβλιογραφική Επισκόπησης

2.1 Κύκλος ζωής ανάπτυξης ασφαλούς λογισμικού (Secure-SDLC)

Στο προηγούμενο κεφάλαιο αποτυπώθηκε ο ορισμός του κύκλου ζωής ανάπτυξης ασφαλούς λογισμικού, όμως ο ρόλος του στην μελέτη θεωρείται αρκετά σημαντικός ώστε να πραγματοποιηθεί μια εκτενής ανάλυση του.

Στο παρελθόν η ασφάλεια σε έναν κύκλο ζωής ανάπτυξης λογισμικού περιοριζόταν μόνο στις συνηθισμένες τεχνικές ελέγχου παραβίασης και προσπάθειας διείσδυσης (penetration testing) κατά τη διάρκεια της φάσης των δοκίμων [12]. Όμως με την πάροδο του χρόνου και με τις εξελίξεις του κλάδου της ασφάλειας των πληροφοριών θεωρείται βέλτιστη πρακτική η πλήρης ενσωμάτωση της ασφάλειας σε κάθε φάση ενός κύκλου ζωής ανάπτυξης λογισμικού [10]. Έτσι προέκυψε η έννοια του κύκλου ζωής ανάπτυξης ασφαλούς λογισμικού. Όπου σε έναν τέτοιο κύκλο διασφαλίζεται ότι όλες οι απαραίτητες δραστηριότητες που αφορούν τον τομέα της ασφάλειας θα πραγματοποιηθούν σε όλες τις φάσεις [13].

Τα βασικά πλεονεκτήματα που προκύπτουν από την χρήση ενός μοντέλου Secure SDLC είναι τα εξής [14].

- Η συνειδητοποίηση των ζητημάτων ασφάλειας από τα ενδιαφερόμενα μέρη.
- Έγκαιρη ανίχνευση ελαττωμάτων στο σύστημα.

- Μείωση του κόστους ως αποτέλεσμα της έγκαιρης ανίχνευσης και επίλυσης των ζητημάτων.
- Συνολική μείωση των εγγενών επιχειρηματικών κινδύνων για τον οργανισμό.

2.1.1 Φάση σχεδιασμού

Στην φάση του σχεδιασμού ο πρωταρχικός στόχος είναι η δημιουργία ενός σχεδίου υψηλού επιπέδου της κατασκευής του λογισμικού. Οπού τα εμπλεκόμενα μέρη, οι χρήστες και οι προγραμματιστές, εξετάζουν τις απαιτήσεις και καθορίζουν το εύρος της εργασίας του συστήματος και του λογισμικού που πρόκειται να κατασκευαστεί [13].

Αυτός ο σχεδιασμός καθορίζει όλα τα μέρη του συστήματος που πρέπει να αναπτυχθούν, όπως οι επικοινωνίες με υπηρεσίες τρίτων συστημάτων, οι ροές χρηστών, ενδεχόμενες κλήσεις βάσεων δεδομένων, ενώ το κομμάτι της ασφάλειας επικεντρώνεται στα κάτωθι καίρια σημεία [14]:

- Ανάλυση κινδύνου αρχιτεκτονικής, δηλαδή την βεβαίωση ότι έχουν εφαρμοστεί οι βέλτιστες ασφαλείς πρακτικές σχεδίασης.
- Μοντελοποίηση απειλών (threat modeling), αποτύπωση τρόπων του πώς ένας επιτιθέμενος θα μπορούσε να εκμεταλλευτεί το σχέδιο.
- Ανάλυση σχεδιασμού ελέγχου ασφαλείας , δηλαδή την επιθεώρηση του λογισμικού για ελλείποντα ή αδύνατα στοιχεία ελέγχου ασφαλείας.

2.1.2 Φάση εφαρμογής

Στην φάση της εφαρμογής που είναι και γνωστή και ως φάση «κωδικοποίησης», οι προγραμματιστές εφαρμόζουν το σχεδιασμό του λογισμικού γράφοντας κώδικα. Ενώ, το κομμάτι της ασφάλειας επικεντρώνεται στον έλεγχο για την χρήση των βέλτιστων πρακτικών συγγραφής κώδικα από την μεριά των προγραμματιστών [13].

2.1.3 Φάση δοκιμής

Στην φάση της δοκιμής, το μέχρι στιγμής υλοποιημένο λογισμικό, περνάει διαφόρων ειδών δοκιμές και αξιολογείται ως προς συγκεκριμένες απαιτήσεις. Οι δοκιμές πραγματοποιούνται ως προς τις λειτουργικές απαιτήσεις καθώς και τις μη λειτουργικές δοκιμές [14].
Επίσης πραγματοποιούνται δοκιμές για τις απαιτήσεις ασφάλειας του προϊόντος με τις πιο συνηθισμένες να είναι οι εξής [14] :

- Στατικές δοκιμές ασφαλείας εφαρμογών (Static Code Analysis).
- Δυναμικές δοκιμές ασφάλειας εφαρμογών (Dynamic Code Analysis).
- Ανάλυση πηγαίου κώδικα (Source Code Review).
- Δοκιμές fuzzing.
- Δοκιμές διείσδυσης (Penetration Testing).

2.1.4 Φάση παραγωγής

Στην φάση της παραγωγής περιλαμβάνεται η έκδοση του ολοκληρωμένου λογισμικού σε παραγωγικό περιβάλλον, όπως επίσης και η εκτέλεση παραμετροποιήσεων και δραστηριοτήτων στο περιβάλλον παραγωγής.

Από την μεριά της ασφάλειας πληροφοριών πραγματοποιούνται κυρίως τα εξής [14]:

- Αξιολόγηση τυχόν ευπαθειών (Vulnerability Assessment).
- Παραμετροποίηση ασφάλειας (Secure Configuration – Hardening)

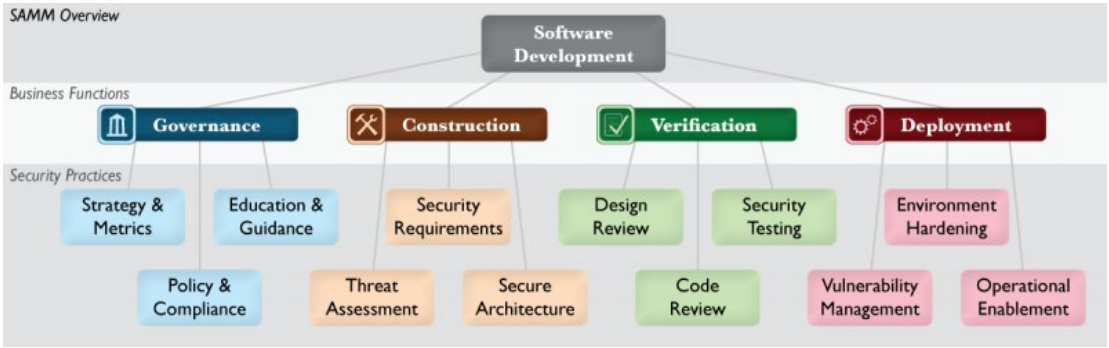
2.1.5 Μοντέλο διασφάλισης ωρίμανσης λογισμικού SAMM

Το μοντέλο διασφάλισης ωρίμανσης λογισμικού SAMM αποτελεί ένα πρότυπο που έχει δημιουργηθεί από τον οργανισμό OWASP. Ως σκοπό, έχει την διαμόρφωση στρατηγικής για την ενσωμάτωση της ασφάλειας του λογισμικού σε έναν υφιστάμενο κύκλο ανάπτυξης λογισμικού.

Βάσει των παραπάνω, θα μπορούσε κανείς να χαρακτηρίσει το SAMM ως έναν οδηγό που ορίζει τα βασικά στάδια για την εκτέλεση των κατάλληλων βημάτων ώστε να εφαρμοστεί ένας κύκλος ζωής ανάπτυξης ασφαλούς λογισμικού [11].

Το μοντέλο δεν χρησιμοποιεί μία ενιαία «φόρμουλα» για όλους τους οργανισμούς. Δηλαδή, είναι ευέλικτο και επιτρέπει στους οργανισμούς οι οποίοι το χρησιμοποιούν, να το εφαρμόζουν σε όποια φάση ή σε όλες τις φάσεις του κύκλου ζωής που επιλέγουν, βάσει της επικινδυνότητας και της ανεκτικότητας που καθορίζεται από τη στρατηγική του οργανισμού [11].

Δομικά, το μοντέλο SAMM βασίζεται σε ένα σύνολο 12 πρακτικών ασφαλείας, οι οποίες ομαδοποιούνται σε τέσσερις επιχειρηματικές λειτουργίες και η κάθε επιχειρηματική λειτουργία αποτελείται από τρεις πρακτικές ασφάλειας. Εν συνεχεία, κάθε πρακτική ασφάλειας περιέχει ένα σύνολο δραστηριοτήτων που είναι διαρθρωμένο σε τρία επίπεδα ωριμότητας (1-3). Οι δραστηριότητες στο χαμηλότερο επίπεδο ωριμότητας είναι συνήθως πιο εύκολο να εκτελεστούν και απαιτούν λιγότερη προσπάθεια από εκείνες που βρίσκονται στο υψηλότερο επίπεδο ωριμότητας [11].



Εικόνα 1. Διαγραμματική απεικόνιση δομής μοντέλου SAMM.

Η δομή και η αρχιτεκτονική του μοντέλου ωριμότητας του μοντέλου SAMM είναι διαρθρωμένη με τέτοιο τρόπο ώστε να υποστηρίζονται τα εξής καίρια σημεία [11]:

1. Αξιολόγηση της τρέχουσας κατάστασης ως προς τη διασφάλιση ασφάλειας του λογισμικού.
2. Καθορισμό του στρατηγικού στόχου που πρέπει να λάβει ένας οργανισμός.
3. Διαμόρφωση ενός πλάνου εφαρμογής για το πως και τί θα υλοποιηθεί.
4. Συμβουλές βασισμένες στις βέλτιστες πρακτικές για τον τρόπο υλοποίησης συγκεκριμένων δραστηριοτήτων.

2.1.6 Αρχές του μοντέλου SAMM

Το SAMM ως μοντέλο βασίζεται σε κάποιες γενικές αρχές οι οποίες αποτυπώνονται κάτωθι [11]:

1. Η συμπεριφορά του οργανισμού μεταβάλλεται αργά με την πάροδο του χρόνου. Ένα επιτυχημένο πρόγραμμα ασφάλειας λογισμικού, θα πρέπει να καθορίζεται σε μικρές επαναλήψεις που προσφέρουν απτά κέρδη διαβεβαίωσης, ενώ εργάζονται προοδευτικά για τους μακροπρόθεσμους στόχους.
2. Δεν υπάρχει ένα συγκεκριμένο μονοπάτι που να λειτουργεί το ίδιο σε όλους τους οργανισμούς, αλλά κάθε πλαίσιο ασφάλειας λογισμικού θα πρέπει να προσαρμόζεται στις ανάγκες και την κουλτούρα του κάθε οργανισμού, ώστε να προσφέρει τη μέγιστη ευελιξία.
3. Οι οδηγίες σχετικά με τις δραστηριότητες ασφάλειας πρέπει να είναι κανονιστικές. Θα πρέπει να πραγματοποιούνται όλα τα βήματα για τη δημιουργία και την αξιολόγηση ενός προγράμματος διασφάλισης, η οποία θα είναι καθορισμένη και μετρήσιμη.

2.2 **Επιχειρηματικές λειτουργίες**

Στο υψηλότερο επίπεδο, το μοντέλο SAMM ορίζει τέσσερις κρίσιμες επιχειρησιακές λειτουργίες. Κάθε επιχειρηματική λειτουργία είναι μια κατηγορία που εμπεριέχει δραστηριότητες που σχετίζονται με κλάδους της ανάπτυξης λογισμικού και κάθε οργανισμό που εκπληρώνει σε κάποιο βαθμό αυτές τις επιχειρηματικές λειτουργίες [11]. Επίσης για κάθε επιχειρηματική λειτουργία του μοντέλου SAMM, ορίζει τρεις πρακτικές ασφαλείας. Κάθε πρακτική ασφαλείας, είναι ένας τομέας σχετικός με τις δραστηριότητες που αντιστοιχούν σε μία επιχειρηματική λειτουργία. Επίσης για κάθε πρακτική ασφαλείας ορίζονται τρία επίπεδα ωριμότητας [11].

2.2.1 Διακυβέρνηση

Η «διακυβέρνηση» ως επιχειρηματική λειτουργία, εστιάζει στις διαδικασίες και τις δραστηριότητες που σχετίζονται με τον τρόπο με τον οποίο ένας οργανισμός διαχειρίζεται τη συνολική ανάπτυξη λογισμικού.
Συγκεκριμένα, περιλαμβάνει επίλυση προβλημάτων που επηρεάζουν την ορθή λειτουργία των ομάδων που εμπλέκονται στην ανάπτυξη, καθώς και επιχειρηματικές διαδικασίες που έχουν καθιερωθεί σε επίπεδο οργανισμού [11].

Οι πρακτικές ασφαλείας που εντάσσονται στα πλαίσια της διακυβέρνησης, βάσει του μοντέλου SAMM είναι οι εξής:

1. Η «στρατηγική και οι μετρήσεις», η οποία αφορά το σύνολο στρατηγικής κατεύθυνσης, της διασφάλισης του λογισμικού, το πρόγραμμα και την οργάνωση των διαδικασιών αλλά και τις δραστηριότητες για τη συλλογή μετρήσεων σχετικά με το επίπεδο ασφάλειας [11].
2. Η «πολιτική και η συμμόρφωση», η οποία αφορά τη ρύθμιση για την ασφάλεια, τη συμμόρφωση και τον έλεγχο του πλαίσιού ασφαλείας σε ολόκληρο τον οργανισμό [11].
3. Η «εκπαίδευση και η καθοδήγηση», η οποία αφορά την αύξηση των γνώσεων ασφάλειας πληροφοριών του προσωπικού. Το οποίο επιτυγχάνεται μέσω της κατάρτισης και της καθοδήγησης στα θέματα ασφάλειας που αφορούν τις λειτουργίες εργασίας κάθε ατόμου [11].

2.2.2 Κατασκευή

Η «κατασκευή» ως επιχειρηματική λειτουργία, αφορά τις διαδικασίες και τις δραστηριότητες που σχετίζονται με τον τρόπο με τον οποίο ένας οργανισμός ορίζει στόχους και παράγει λογισμικό στα αναπτυξιακά έργα. Ειδικότερα, περιλαμβάνεται η διαχείριση προϊόντων, η συλλογή των απαιτήσεων, η δημιουργία αρχιτεκτονικής υψηλού επιπέδου, και ο λεπτομερής σχεδιασμός της εφαρμογής [11].

Οι πρακτικές ασφαλείας που εντάσσονται στα πλαίσια της κατασκευής, βάσει του μοντέλου SAMM είναι οι εξής [11]:

1. Η «εκτίμηση απειλών», η οποία περιλαμβάνει τον εντοπισμό και την αποτύπωση δυνητικών επιθέσεων με σκοπό την καλύτερη κατανόηση των κινδύνων ασφαλείας.
2. Οι «απαιτήσεις ασφάλειας», οι οποίες αφορούν την αποτύπωση και συμπερίληψη των σχετικών με την ασφάλεια πληροφοριών επιχειρησιακών αναγκών του λογισμικού.
3. Η «ασφαλής αρχιτεκτονική», η οποία περιλαμβάνει την ενίσχυση της διαδικασίας του σχεδιασμού, ώστε να εξυπηρετούνται οι ανάγκες της ασφάλειας πληροφοριών και ο έλεγχος των τεχνολογιών που χρησιμοποιούνται για την παραγωγή του λογισμικού από την σκοπιά της ασφάλειας.

2.2.3 Επαλήθευση

Η «επαλήθευση» ως επιχειρηματική λειτουργία, επικεντρώνεται στις διαδικασίες και τις δραστηριότητες που σχετίζονται με τον τρόπο με τον οποίο ένας οργανισμός ελέγχει και δοκιμάζει το παραχθέν προϊόν. Κυρίως περιλαμβάνονται εργασίες διασφάλισης ποιότητας και διαφόρων ειδών δοκιμές του προϊόντος.

Οι πρακτικές ασφαλείας που εντάσσονται στα πλαίσια της επαλήθευσης, βάσει του μοντέλου SAMM είναι οι εξής [11]:

1. Η «επισκόπηση του σχεδιασμού», η οποία περιλαμβάνει την επιθεώρηση του σχεδιασμού του προϊόντος, ώστε να βεβαιωθεί η ύπαρξη επαρκών μηχανισμών ασφαλείας.
2. Η «αναθεώρηση κώδικα», περιλαμβάνει την αξιολόγηση του πηγαίου κώδικα με σκοπό την ανακάλυψη ευπαθειών και την καθιέρωση μίας βασικής γραμμής για ασφαλή κωδικοποίηση.
3. Η «δοκιμή ασφαλείας» περιλαμβάνει τη δοκιμή του λογισμικού κατά το χρόνο εκτέλεσης του, προκειμένου να ανακαλυφθούν τρωτά σημεία.

2.2.4 Παραγωγή

Η «παραγωγή» ως επιχειρηματική λειτουργία, περιλαμβάνει τις διαδικασίες και τις δραστηριότητες που σχετίζονται με τον τρόπο με τον οποίο ένας οργανισμός

διαχειρίζεται την κυκλοφορία σε παραγωγικό περιβάλλον ενός λογισμικού που έχει δημιουργηθεί.

Οι πρακτικές ασφαλείας που εντάσσονται στα πλαίσια της παραγωγής, με βάση το μοντέλο SAMM είναι οι εξής [11]:

1. Η «διαχείριση ευπάθειας» περιλαμβάνει τη δημιουργία συνεκτικών διαδικασιών διαχείρισης εσωτερικών και εξωτερικών αναφορών ευπάθειας.
2. Η «περιβαλλοντική σκλήρυνση» (Hardening), περιλαμβάνει την παραμετροποίηση του περιβάλλοντος που εκτελεί ένα λογισμικό.
3. Η «λειτουργική ενεργοποίηση» περιλαμβάνει τον εντοπισμό και την καταγραφή των σχετικών με την ασφάλεια πληροφοριών. Πληροφορίες που χρειάζεται ένας φορέας εκμετάλλευσης για να ρυθμίσει σωστά, να αναπτύξει και να εκτελέσει ένα λογισμικό για τον εκάστοτε οργανισμό.

2.3 Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR)

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων, (GDPR - General Data Protection Regulation), του Ευρωπαϊκού Κοινοβουλίου και του Συμβούλιου ο οποίος ψηφίστηκε στις Βρυξέλλες τον Απρίλιο του 2016 και με καταληκτική ημερομηνία εφαρμογής την 25η Μαΐου 2018, καθορίζει το νομοθετικό πλαίσιο στα κράτη μέλη της Ευρωπαϊκής Ένωσης όσον αφορά την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) [7], [15].

Ο νέος αυτός κανονισμός έχει εισάγει πλέον έννοιες όπως «Υπεύθυνος Προστασίας Δεδομένων» [16], «Υπεύθυνος επεξεργασίας», «Επεξεργασία δεδομένων», οι οποίες είναι έννοιες και ορισμοί αλληλένδετοι με την ανάπτυξη του εργαλείου μας καθότι επηρεάζει άμεσα την επιλογή των κριτήριων.

Ως «Υπεύθυνος επεξεργασίας», (άρθρο 4, παρ.7), ορίζεται «*το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους».* [7]

Ως «Επεξεργασία», (άρθρο 4, παρ.2), ορίζεται «*κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή*». [7]

2.3.1 Προσωπικά δεδομένα

Κατά συνέπεια ερμηνεύοντας τον κανονισμό, ως ***δεδομένα προσωπικού χαρακτήρα***, ορίζονται «*κάθε πληροφορία που αφορά ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο («υποκείμενο των δεδομένων»)· το ταυτοποιήσιμο φυσικό πρόσωπο είναι εκείνο του οποίου η ταυτότητα μπορεί να εξακριβωθεί, άμεσα ή έμμεσα […]*» (άρθρο 4, παρ.1) [15]. [7]

Επίσης, ερμηνεύοντας τον κανονισμό, ως «Προσωπικά Δεδομένα» ερμηνεύονται οι κάτωθι κατηγορίες που παρατίθενται στον Πίνακα 1:

Αριθμός Δελτίου Ταυτότητας	Τηλέφωνο
Αριθμός Φορολογικού Μητρώου (ΑΦΜ)	Διεύθυνση
Αριθμός Μητρώου Κοινωνικής Ασφάλισης	Επάγγελμα

Ονοματεπώνυμο	Εκπαίδευση
Δεδομένα Γεωγραφικής Θέσης (GPS)	Ενδιαφέροντα
Φυσικά Χαρακτηριστικά	Δραστηριότητες
Οικογενειακή Κατάσταση	Συνήθειες

Πίνακας 1. Πίνακας ενδεικτικών Προσωπικών Δεδομένων βάσει του GDPR.

Επίσης, σύμφωνα με το Άρθρο 5 του Κανονισμού, αναφέρονται έξι (6) αρχές οι οποίες διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα, και για τις οποίες ο υπεύθυνος επεξεργασίας τελεί υπό ευθύνη:

(1) την «νομιμότητα, αντικειμενικότητα και διαφάνεια» της επεξεργασίας.
(2) τον «περιορισμό του σκοπού» της επεξεργασίας.
(3) την «ελαχιστοποίηση των δεδομένων» της επεξεργασίας.
(4) την «ακρίβεια» της επεξεργασίας.
(5) τον «περιορισμό της περιόδου αποθήκευσης» της επεξεργασίας.
(6) την «ακεραιότητα και εμπιστευτικότητα» της επεξεργασίας.

Επιπρόσθετα, για την νομιμότητα της επεξεργασίας, όπως αναφέρεται στον κανονισμό, θα πρέπει να ισχύει τουλάχιστον μία από τις κατωτέρω προϋποθέσεις:

(1) συναίνεση του υποκειμένου των δεδομένων στην επεξεργασία.
(2) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος.
(3) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας.
(4) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.
(5) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας.

(6) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Επιπρόσθετα μέσα στο Γενικό Κανονισμό υπάρχουν άρθρα που υποβοηθούν και απαιτούν την εφαρμογή του Secure SDLC τα οποία παρατίθενται παρακάτω:

Αριθμός Άρθρου	Τίτλος Άρθρου
Άρθρο 24	Ευθύνη του υπευθύνου επεξεργασίας
Άρθρο 25	Προστασία των δεδομένων ήδη από το σχεδιασμό και εξ ορισμού
Άρθρο 28	Εκτελών την επεξεργασία
Άρθρο 32	Ασφάλεια επεξεργασίας
Άρθρο 33	Γνωστοποίηση παραβίασης δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή
Άρθρο 34	Ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων
Άρθρο 35	Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων
Άρθρο 37	Ορισμός του υπευθύνου προστασίας δεδομένων
Άρθρο 39	Καθήκοντα του υπευθύνου προστασίας δεδομένων

Πίνακας 2. Πίνακας άρθρων GDPR που απαιτούνται στο μοντέλο Secure SDLC.

Κεφάλαιο 3

3 Μεθοδολογία

Βάσει της έρευνας του υπάρχοντος ερευνητικού τομέα η οποία πραγματοποιήθηκε στο κεφάλαιο 2, διαπιστώθηκε ότι πληθώρα άρθρων του κανονισμού GDPR έχουν κοινά χαρακτηριστικά με τις διάφορες φάσεις του μοντέλου SAMM, ενώ επίσης πολλές απαιτήσεις αυτών μπορούν να καλυφθούν με εμπλουτισμό του ιδίου μοντέλου [15], [17], [18].

Επιπλέον, διαπιστώθηκε ότι οι αλλαγές που μπορεί να χρειαστεί μια εφαρμογή για την συμμόρφωση με τον κανονισμό έπειτα από την φάση της υλοποίησης, κοστίζουν χρηματικά αλλά και χρονικά αρκετά πιο πολύ για να πραγματοποιηθούν σε αυτή [19].

Τέλος, έγινε εμφανής η ανάγκη της υιοθέτησης του κανονισμού GDPR στα μοντέλα διασφάλισης ωρίμανσης λογισμικού όπως είναι το SAMM καθώς πλέον οι αρχές που διέπουν τον κανονισμό είναι υποχρεωτικές δια νόμου [8].

Σύμφωνα με τα συμπεράσματα αυτά, ως σκοπός της εργασίας τέθηκε η δημιουργία ενός ενοποιημένου εργαλείου, το οποίο θα έχει τις απαραίτητες απαιτήσεις του κανονισμού GDPR ενσωματωμένες στις διαδικασίες του μοντέλου SAMM. Ουσιαστικά, το εργαλείο αυτό θα έχει την δυνατότητα να εμφανίσει τους δείκτες συμμόρφωσης του κανονισμού στο μοντέλο.
Τεχνικά, το εργαλείο θα βασίζεται σε τροποποιήσεις ενός από τα υπάρχοντα εργαλεία (βασισμένο σε Excel) της εργαλειοθήκης του μοντέλου SAMM. Η επιλογή του συγκεκριμένου μοντέλου διασφάλισης ωρίμανσης λογισμικού διενεργήθηκε, καθώς βάσει της βιβλιογραφικής επισκόπησης θεωρείται ένα από τα πιο διαδεδομένα μοντέλα στο είδος του [20].

Τέλος, ως γνώμονας τέθηκε η μη αλλαγή των διαδικασιών του μοντέλου SAMM ώστε το τελικό αποτέλεσμα να μπορεί να χρησιμοποιηθεί από οργανισμούς που ήδη το εφαρμόζουν χωρίς να πραγματοποιηθεί σύγχυση.

3.1 **Υπάρχουσα κατάσταση εργαλείου**

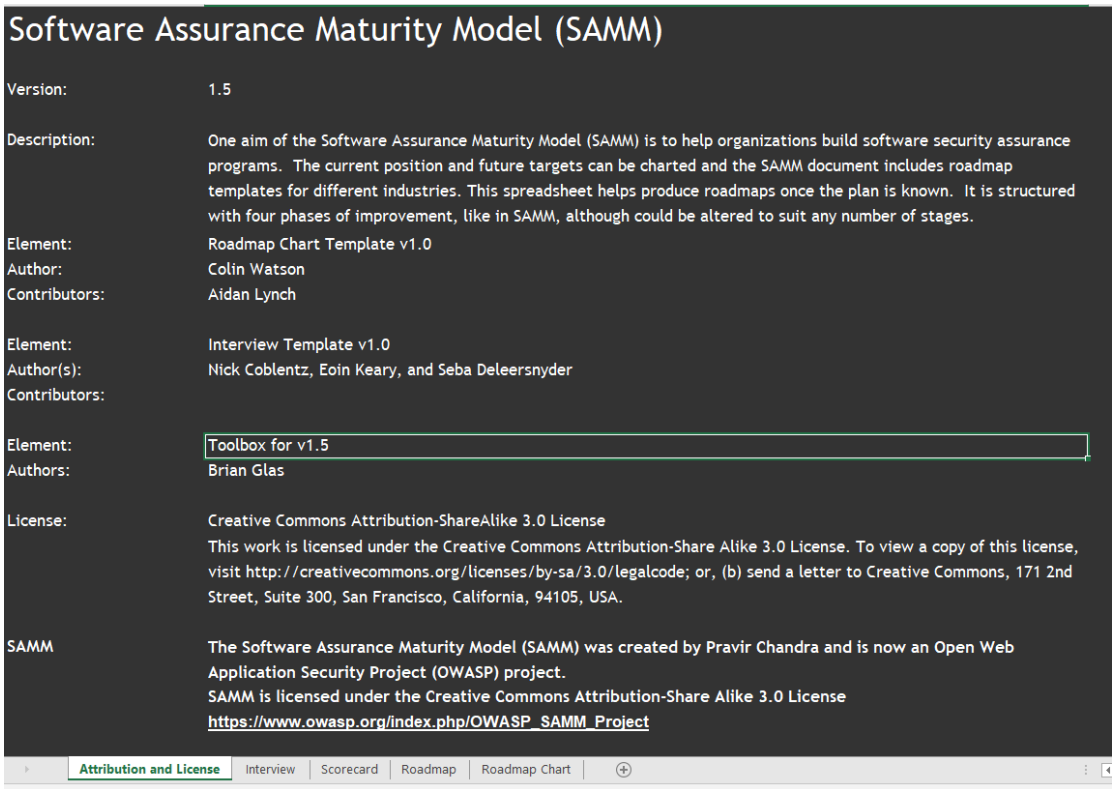
Το εργαλείο που θα αποτελέσει την βάση εκκίνησης μας είναι ένα εργαλείο excel, το οποίο έχει δημιουργηθεί από τον οργανισμό OWASP με σκοπό να αποτυπώνει τον υπάρχον δείκτη ωριμότητας σύμφωνα με το πρότυπο SAMM [21].

Αποτελείται από πέντε (5) συγκεκριμένα φύλλα και τα οποία επιγραμματικά είναι τα εξής:

- Attribution and License
- Interview
- Scorecard
- Roadmap
- Roadmap Chart

Δίνοντας μια γενική περιγραφή των προαναφερθέντων φύλλων θα λέγαμε ότι:

Το φύλλο «Attribution and License» περιέχει κάποιες γενικές πληροφορίες για το εργαλείο, όπως έκδοση και περιγραφή, που έχει αναπτυχθεί από τον οργανισμό OWASP.



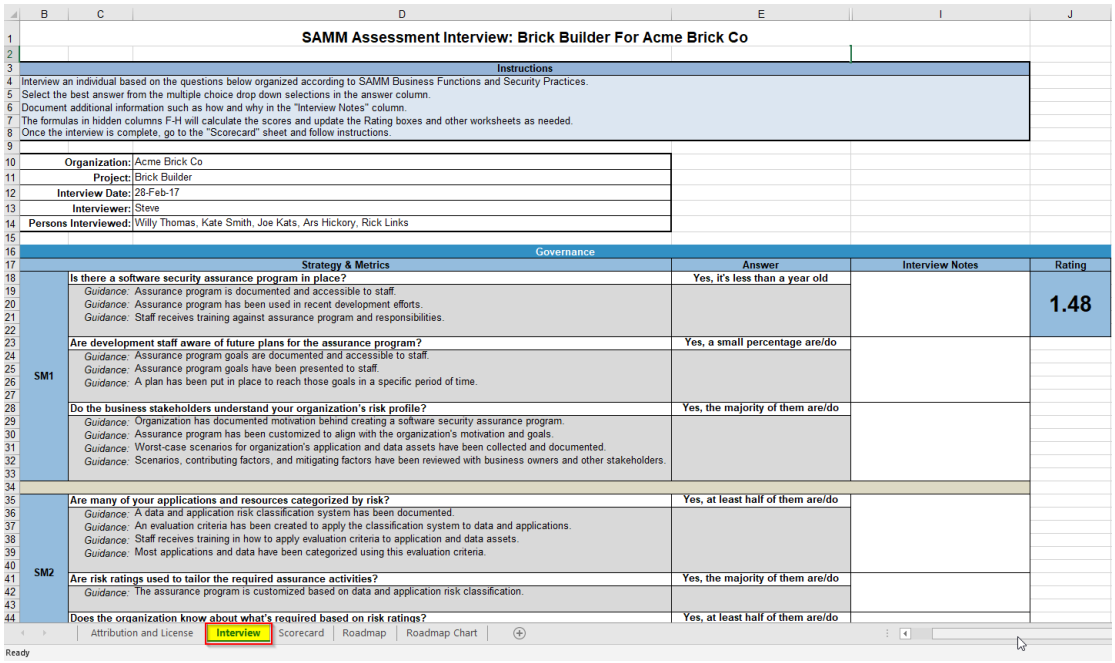
Software Assurance Maturity Model (SAMM)

Version:	1.5
Description:	One aim of the Software Assurance Maturity Model (SAMM) is to help organizations build software security assurance programs. The current position and future targets can be charted and the SAMM document includes roadmap templates for different industries. This spreadsheet helps produce roadmaps once the plan is known. It is structured with four phases of improvement, like in SAMM, although could be altered to suit any number of stages.
Element:	Roadmap Chart Template v1.0
Author:	Colin Watson
Contributors:	Aidan Lynch
Element:	Interview Template v1.0
Author(s):	Nick Coblentz, Eoin Keary, and Seba Deleersnyder
Contributors:	
Element:	Toolbox for v1.5
Authors:	Brian Glas
License:	Creative Commons Attribution-ShareAlike 3.0 License This work is licensed under the Creative Commons Attribution-Share Alike 3.0 License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/3.0/legalcode; or, (b) send a letter to Creative Commons, 171 2nd Street, Suite 300, San Francisco, California, 94105, USA.
SAMM	The Software Assurance Maturity Model (SAMM) was created by Pravir Chandra and is now an Open Web Application Security Project (OWASP) project. SAMM is licensed under the Creative Commons Attribution-Share Alike 3.0 License https://www.owasp.org/index.php/OWASP_SAMM_Project

Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart

Εικόνα 2. Φύλλο «Attribution and License» εργαλείου.

Στο φύλλο «Interview» συμπληρώνονται όλα εκείνα τα στοιχεία που αφορούν τον οργανισμό σε σχέση με τις τέσσερις (4) κύριες Επιχειρηματικές Λειτουργίες και συμπληρώνονται οι ερωτήσεις που αφορούν και τις δώδεκα (12) πρακτικές ασφάλειας για να μπορεί να υπολογισθεί έτσι ο δείκτης ωριμότητας.



SAMM Assessment Interview: Brick Builder For Acme Brick Co

Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

Organization:	Acme Brick Co
Project:	Brick Builder
Interview Date:	28-Feb-17
Interviewer:	Steve
Persons Interviewed:	Willy Thomas, Kate Smith, Joe Kats, Ars Hickory, Rick Links

Governance			
Strategy & Metrics	Answer	Interview Notes	Rating
SM1 — Is there a software security assurance program in place?	Yes, it's less than a year old		1.48
Guidance: Assurance program is documented and accessible to staff.			
Guidance: Assurance program has been used in recent development efforts.			
Guidance: Staff receives training against assurance program and responsibilities.			
SM1 — Are development staff aware of future plans for the assurance program?	Yes, a small percentage are/do		
Guidance: Assurance program goals are documented and accessible to staff.			
Guidance: Assurance program goals have been presented to staff.			
Guidance: A plan has been put in place to reach those goals in a specific period of time.			
SM1 — Do the business stakeholders understand your organization's risk profile?	Yes, the majority of them are/do		
Guidance: Organization has documented motivation behind creating a software security assurance program.			
Guidance: Assurance program has been customized to align with the organization's motivation and goals.			
Guidance: Worst-case scenarios for organization's application and data assets have been collected and documented.			
Guidance: Scenarios, contributing factors, and mitigating factors have been reviewed with business owners and other stakeholders.			
SM2 — Are many of your applications and resources categorized by risk?	Yes, at least half of them are/do		
Guidance: A data and application risk classification system has been documented.			
Guidance: An evaluation criteria has been created to apply the classification system to data and applications.			
Guidance: Staff receives training in how to apply evaluation criteria to application and data assets.			
Guidance: Most applications and data have been categorized using this evaluation criteria.			
SM2 — Are risk ratings used to tailor the required assurance activities?	Yes, the majority of them are/do		
Guidance: The assurance program is customized based on data and application risk classification.			
Does the organization know about what's required based on risk ratings?	Yes, at least half of them are/do		

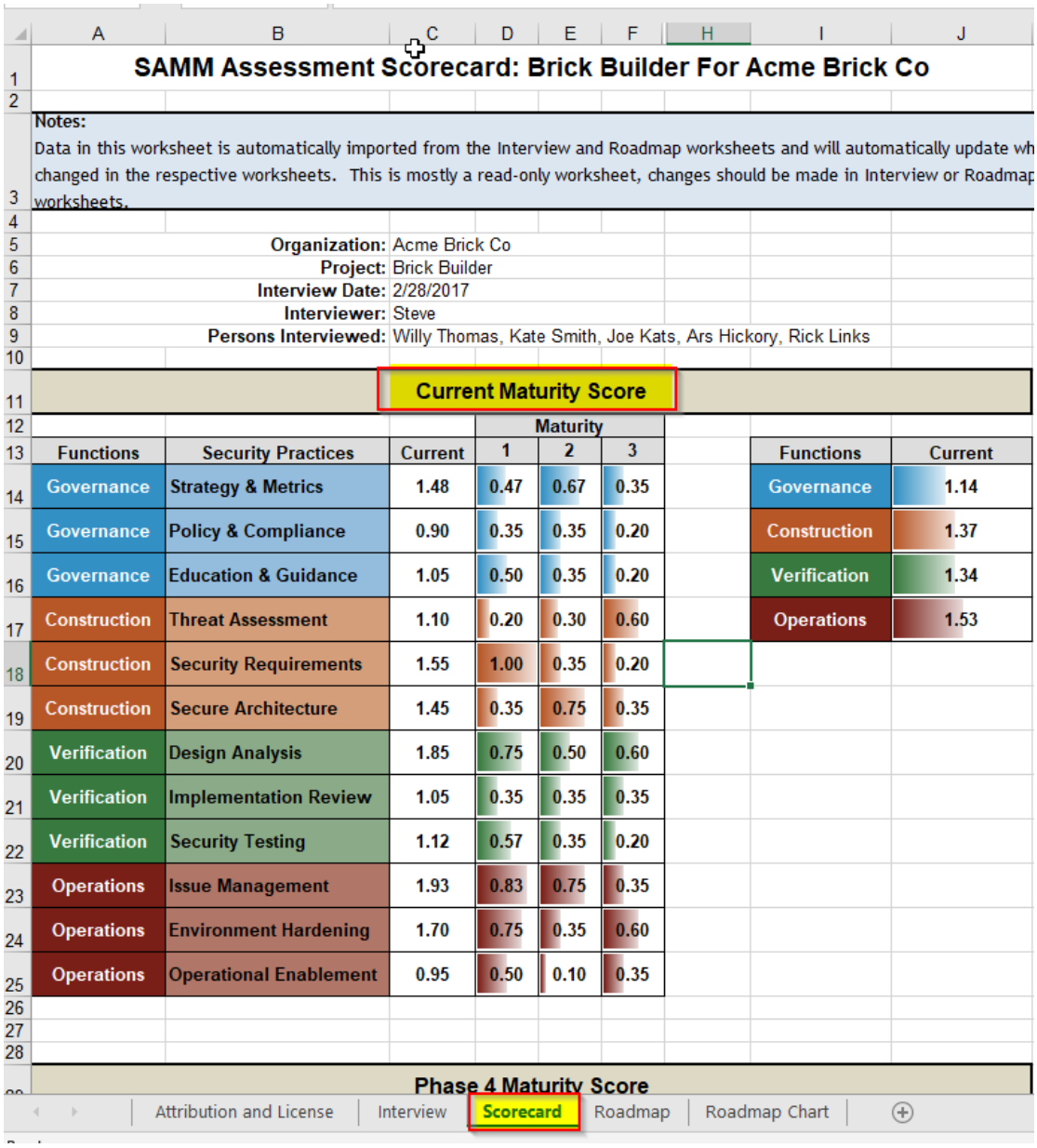
Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart

Ready

Εικόνα 3. Φύλλο «Interview» εργαλείου.

Στο επόμενο φύλλο «Scorecard» αποτυπώνονται συνολικά, σε δυναμικούς πίνακες και γραφήματα, οι δώδεκα (12) πρακτικές ασφαλείας σε συνδυασμό με τον υφιστάμενο δείκτη ωριμότητας και τα επιπλέον τρία (3) επίπεδα ωριμότητας που θέλει να φτάσει ο οργανισμός.

Στις εικόνες 4 έως 9 παρακάτω, φαίνονται τα περιεχόμενα του φύλλου «Scorecard».



SAMM Assessment Scorecard: Brick Builder For Acme Brick Co

Notes:
Data in this worksheet is automatically imported from the Interview and Roadmap worksheets and will automatically update wh
changed in the respective worksheets. This is mostly a read-only worksheet, changes should be made in Interview or Roadmap
worksheets.

Organization: Acme Brick Co
Project: Brick Builder
Interview Date: 2/28/2017
Interviewer: Steve
Persons Interviewed: Willy Thomas, Kate Smith, Joe Kats, Ars Hickory, Rick Links

Current Maturity Score

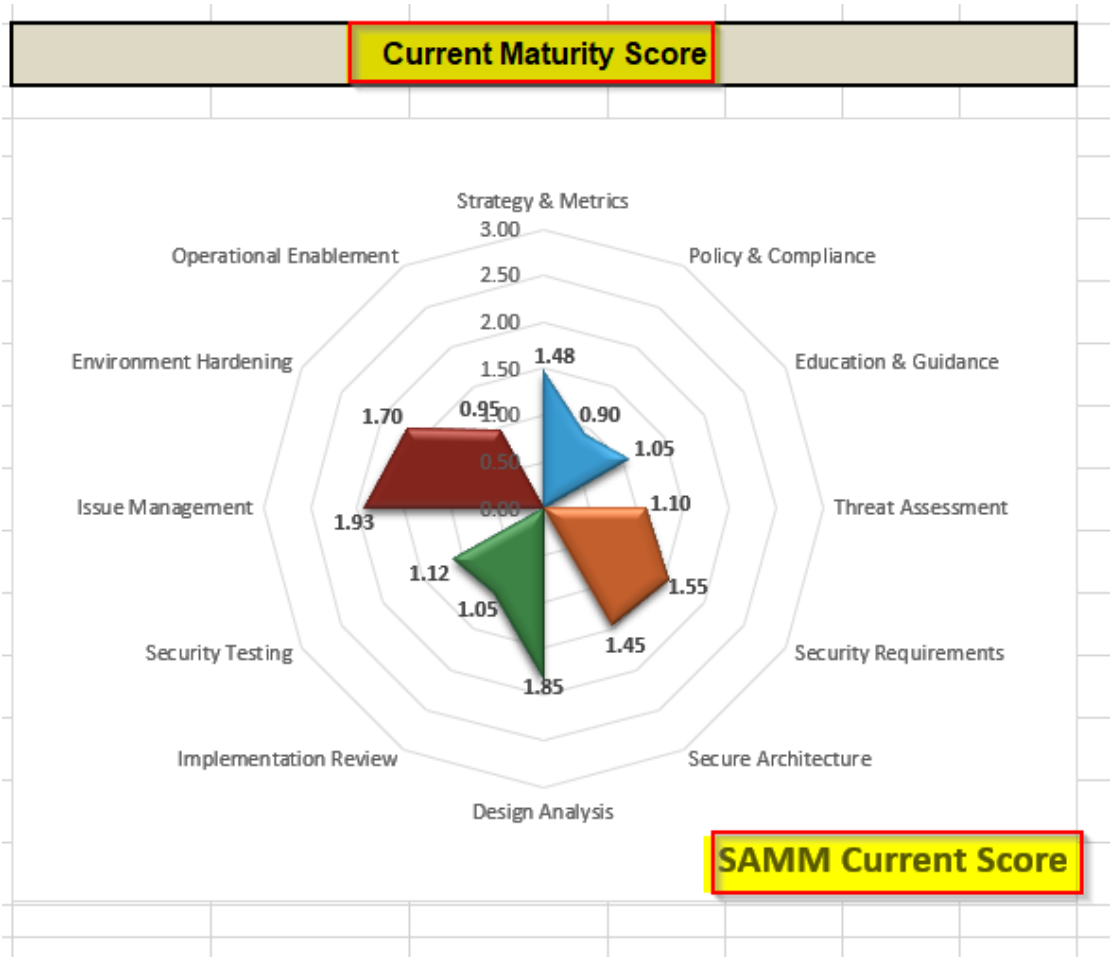
Functions	Security Practices	Current	Maturity 1	Maturity 2	Maturity 3
Governance	Strategy & Metrics	1.48	0.47	0.67	0.35
Governance	Policy & Compliance	0.90	0.35	0.35	0.20
Governance	Education & Guidance	1.05	0.50	0.35	0.20
Construction	Threat Assessment	1.10	0.20	0.30	0.60
Construction	Security Requirements	1.55	1.00	0.35	0.20
Construction	Secure Architecture	1.45	0.35	0.75	0.35
Verification	Design Analysis	1.85	0.75	0.50	0.60
Verification	Implementation Review	1.05	0.35	0.35	0.35
Verification	Security Testing	1.12	0.57	0.35	0.20
Operations	Issue Management	1.93	0.83	0.75	0.35
Operations	Environment Hardening	1.70	0.75	0.35	0.60
Operations	Operational Enablement	0.95	0.50	0.10	0.35

Functions	Current
Governance	1.14
Construction	1.37
Verification	1.34
Operations	1.53

Phase 4 Maturity Score

Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart

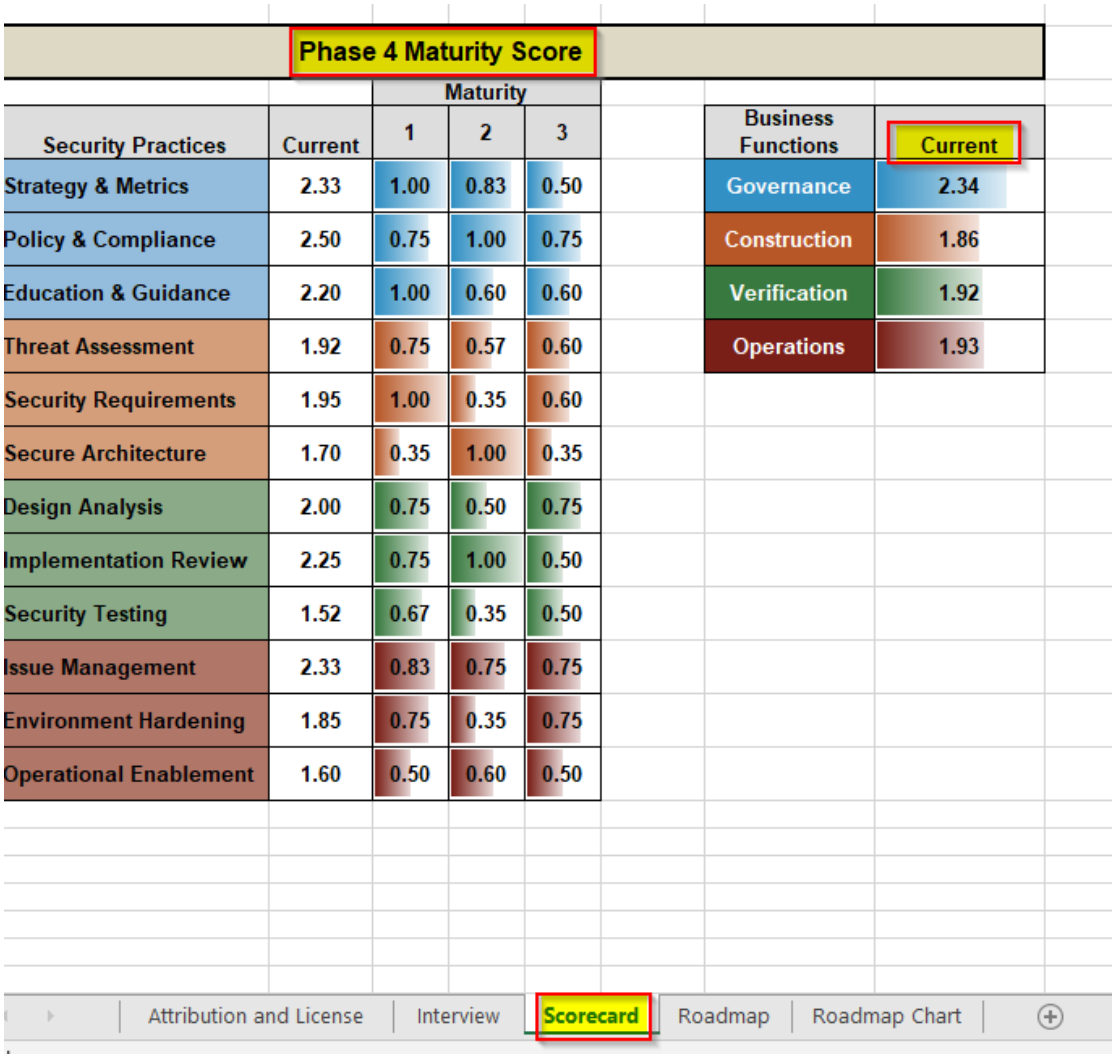
Εικόνα 4. Current Maturity Score πίνακας μέσα στο Φύλλο «Scorecard».



Εικόνα 5. Current Maturity Score διάγραμμα δομικού στοιχείου μέσα στο Φύλλο «Scorecard».

Current Maturity Score					
		Governance	Constructior	Verificatior	Operations
Governanc e	Strategy & Metrics	1.48	0.00	0.00	0.00
Governanc e	Policy & Compliance	0.90	0.00	0.00	0.00
Governanc e	Education & Guidance	1.05	0.00	0.00	0.00
Constructio n	Threat Assessment	0.00	1.10	0.00	0.00
Constructio n	Security Requirements	0.00	1.55	0.00	0.00
Constructio n	Secure Architecture	0.00	1.45	0.00	0.00
Verification	Design Analysis	0.00	0.00	1.85	0.00
Verification	Implementation Review	0.00	0.00	1.05	0.00
Verification	Security Testing	0.00	0.00	1.12	0.00
Operations	Issue Management	0.00	0.00	0.00	1.93
Operations	Environment Hardening	0.00	0.00	0.00	1.70
Operations	Operational Enablement	0.00	0.00	0.00	0.95

Εικόνα 6. Current Maturity Score συγκεντρωτικός πίνακας μέσα στο Φύλλο «Scorecard».

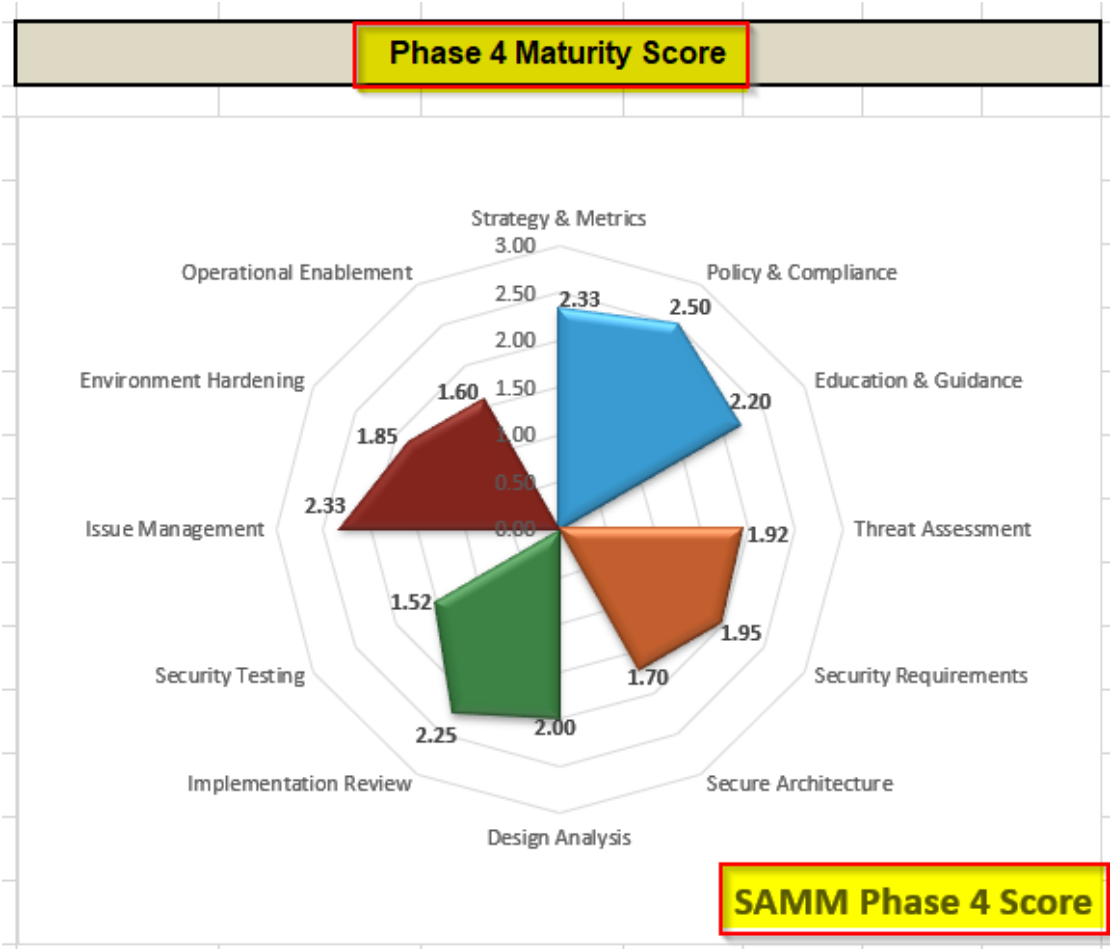


Phase 4 Maturity Score

Security Practices	Current	Maturity 1	2	3
Strategy & Metrics	2.33	1.00	0.83	0.50
Policy & Compliance	2.50	0.75	1.00	0.75
Education & Guidance	2.20	1.00	0.60	0.60
Threat Assessment	1.92	0.75	0.57	0.60
Security Requirements	1.95	1.00	0.35	0.60
Secure Architecture	1.70	0.35	1.00	0.35
Design Analysis	2.00	0.75	0.50	0.75
Implementation Review	2.25	0.75	1.00	0.50
Security Testing	1.52	0.67	0.35	0.50
Issue Management	2.33	0.83	0.75	0.75
Environment Hardening	1.85	0.75	0.35	0.75
Operational Enablement	1.60	0.50	0.60	0.50

Business Functions	Current
Governance	2.34
Construction	1.86
Verification	1.92
Operations	1.93

Εικόνα 7. Phase 4 Maturity Score πίνακας μέσα στο Φύλλο «Scorecard».

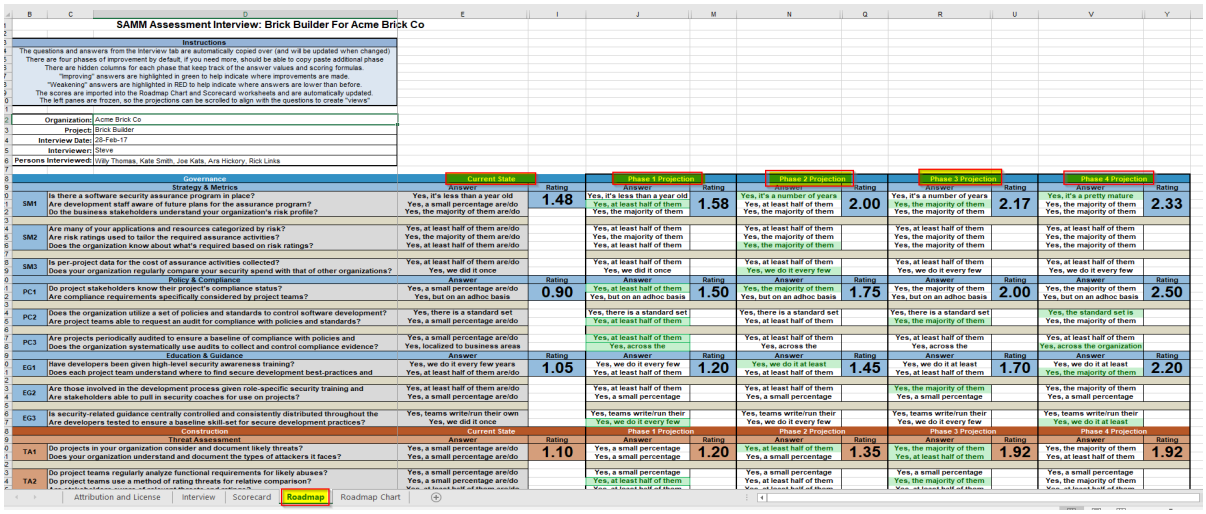


Εικόνα 8. Phase 4 Maturity Score διάγραμμα δομικού στοιχείου μέσα στο Φύλλο «Scorecard».

Phase 4 Maturity Score					
		Governance	Constructior	Verificatior	Operations
Governanc e	Strategy & Metrics	2.33	0.00	0.00	0.00
Governanc e	Policy & Compliance	2.50	0.00	0.00	0.00
Governanc e	Education & Guidance	2.20	0.00	0.00	0.00
Constructio n	Threat Assessment	0.00	1.92	0.00	0.00
Constructio n	Security Requirements	0.00	1.95	0.00	0.00
Constructio n	Secure Architecture	0.00	1.70	0.00	0.00
Verification	Design Analysis	0.00	0.00	2.00	0.00
Verification	Implementation Review	0.00	0.00	2.25	0.00
Verification	Security Testing	0.00	0.00	1.52	0.00
Operations	Issue Management	0.00	0.00	0.00	2.33
Operations	Environment Hardening	0.00	0.00	0.00	1.85
Operations	Operational Enablement	0.00	0.00	0.00	1.60

Εικόνα 9. Phase 4 Maturity Score συγκεντρωτικός πίνακας μέσα στο Φύλλο «Scorecard».

Ακολούθως το φύλλο «Roadmap» αντλεί στοιχεία από τις καρτέλες «Interview» και αποτυπώνονται σε συγκεκριμένες στήλες οι δοθείσες απαντήσεις και η κλίμακα συμμόρφωσης του μοντέλου SAMM, τόσο για την υφιστάμενη κατάσταση όσο και για τις υπόλοιπες τέσσερις (4) φάσεις ωριμότητας, όπως φαίνεται και στην εικόνα 10.



SAMM Assessment Interview: Brick Builder For Acme Brick Co

Instructions
The questions and answers from the Interview tab are automatically copied over (and will be updated when changed)
There are four phases of improvement by default, if you need more, should be able to copy paste additional phase
There are hidden columns for each phase that keep track of the answer values and scoring formulas.
"Improving" answers are highlighted in green to help indicate where improvements are made.
"Weakening" answers are highlighted in RED to help indicate where answers are lower than before.
The scores are imported into the Roadmap Chart and Scorecard worksheets and are automatically updated.
The left panes are frozen, so the projections can be scrolled to align with the questions to create "views"

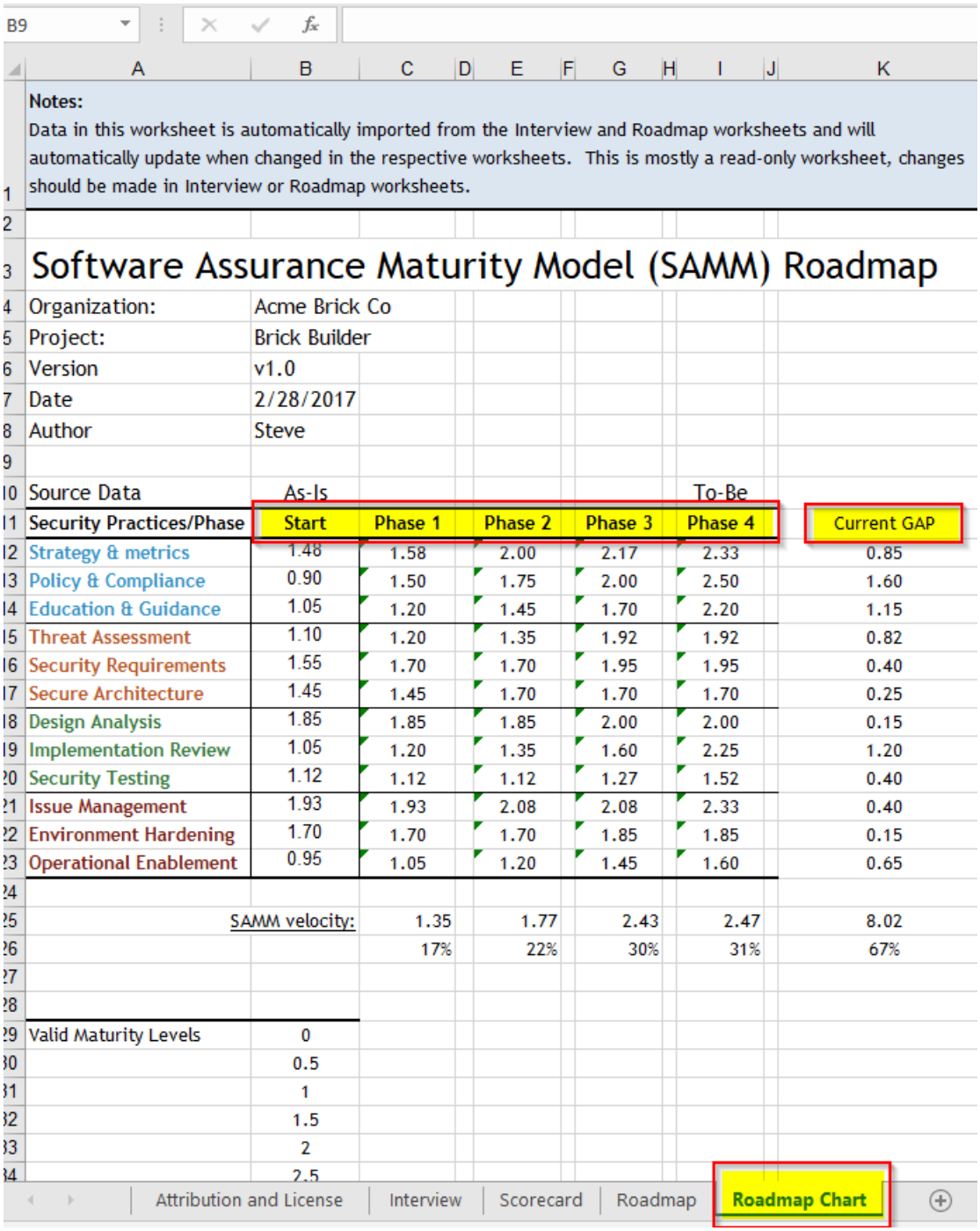
Organization:	Acme Brick Co
Project:	Brick Builder
Interview Date:	28-Feb-17
Interviewer:	Steve
Persons Interviewed:	Willy Thomas, Kate Smith, Joe Kats, Ars Hickory, Rick Links

		Current State		Phase 1 Projection		Phase 2 Projection		Phase 3 Projection		Phase 4 Projection	
Governance	Strategy & Metrics	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating
SM1	Is there a software security assurance program in place? Are development staff aware of future plans for the assurance program? Do the business stakeholders understand your organization's risk profile?	Yes, it's less than a year old Yes, a small percentage are/do Yes, the majority of them are/do	1.48	Yes, it's less than a year old Yes, at least half of them Yes, the majority of them	1.58	Yes, it's a number of years Yes, at least half of them Yes, the majority of them	2.00	Yes, it's a number of years Yes, the majority of them Yes, the majority of them	2.17	Yes, it's a pretty mature Yes, the majority of them Yes, the majority of them	2.33
SM2	Are many of your applications and resources categorized by risk? Are risk ratings used to tailor the required assurance activities? Does the organization know about what's required based on risk ratings?	Yes, at least half of them are/do Yes, the majority of them are/do Yes, at least half of them are/do		Yes, at least half of them Yes, the majority of them Yes, at least half of them		Yes, at least half of them Yes, the majority of them Yes, the majority of them		Yes, at least half of them Yes, the majority of them Yes, the majority of them		Yes, at least half of them Yes, the majority of them Yes, the majority of them	
SM3	Is per-project data for the cost of assurance activities collected? Does your organization regularly compare your security spend with that of other organizations?	Yes, at least half of them are/do Yes, we did it once		Yes, at least half of them Yes, we did it once		Yes, at least half of them Yes, we do it every few		Yes, at least half of them Yes, we do it every few		Yes, at least half of them Yes, we do it every few	
	Policy & Compliance	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating
PC1	Do project stakeholders know their project's compliance status? Are compliance requirements specifically considered by project teams?	Yes, a small percentage are/do Yes, but on an adhoc basis	0.90	Yes, at least half of them Yes, but on an adhoc basis	1.50	Yes, the majority of them Yes, but on an adhoc basis	1.75	Yes, the majority of them Yes, but on an adhoc basis	2.00	Yes, the majority of them Yes, but on an adhoc basis	2.50
PC2	Does the organization utilize a set of policies and standards to control software development? Are project teams able to request an audit for compliance with policies and standards?	Yes, there is a standard set Yes, a small percentage are/do		Yes, there is a standard set Yes, at least half of them		Yes, there is a standard set Yes, at least half of them		Yes, there is a standard set Yes, the majority of them		Yes, the standard set is Yes, the majority of them	
PC3	Are projects periodically audited to ensure a baseline of compliance with policies and Does the organization systematically use audits to collect and control compliance evidence?	Yes, a small percentage are/do Yes, localized to business areas		Yes, at least half of them Yes, across the		Yes, at least half of them Yes, across the		Yes, at least half of them Yes, across the		Yes, at least half of them Yes, across the organization	
	Education & Guidance	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating	Answer	Rating
EG1	Have developers been given high-level security awareness training? Does each project team understand where to find secure development best-practices and	Yes, we do it every few years Yes, at least half of them are/do	1.05	Yes, we do it every few Yes, at least half of them	1.20	Yes, we do it at least Yes, at least half of them	1.45	Yes, we do it at least Yes, at least half of them	1.70	Yes, we do it at least Yes, the majority of them	2.20
EG2	Are those involved in the development process given role-specific security training and Are stakeholders able to pull in security coaches for use on projects?	Yes, at least half of them are/do Yes, a small percentage are/do		Yes, at least half of them Yes, a small percentage		Yes, at least half of them Yes, a small percentage		Yes, the majority of them Yes, a small percentage		Yes, the majority of them Yes, a small percentage	
EG3	Is security-related guidance centrally controlled and consistently distributed throughout the Are developers tested to ensure a baseline skill-set for secure development practices?	Yes, teams write/run their own Yes, we did it once		Yes, teams write/run their Yes, we do it every few		Yes, teams write/run their Yes, we do it every few		Yes, teams write/run their Yes, we do it every few		Yes, teams write/run their Yes, we do it at least	
Construction	Threat Assessment	Current State Answer	Rating	Phase 1 Projection Answer	Rating	Phase 2 Projection Answer	Rating	Phase 3 Projection Answer	Rating	Phase 4 Projection Answer	Rating
TA1	Do projects in your organization consider and document likely threats? Does your organization understand and document the types of attackers it faces?	Yes, a small percentage are/do Yes, a small percentage are/do	1.10	Yes, a small percentage Yes, a small percentage	1.20	Yes, at least half of them Yes, a small percentage	1.35	Yes, the majority of them Yes, at least half of them	1.92	Yes, the majority of them Yes, at least half of them	1.92
TA2	Do project teams regularly analyze functional requirements for likely abuses? Do project teams use a method of rating threats for relative comparison?	Yes, a small percentage are/do Yes, a small percentage are/do		Yes, a small percentage Yes, at least half of them		Yes, a small percentage Yes, at least half of them		Yes, a small percentage Yes, the majority of them		Yes, a small percentage Yes, the majority of them	

Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart

Εικόνα 10. Φύλλο «Roadmap» εργαλείου.

Τέλος, στις εικόνες 11 και 12, για το φύλλο «Roadmap Chart», υπάρχει η αποτύπωση με πίνακα και γραφήματα από την αρχική κατάσταση έως την τέταρτη φάση, με τελικό δείκτη αποτύπωσης την απόκλιση από το μοντέλο.



Notes:
Data in this worksheet is automatically imported from the Interview and Roadmap worksheets and will automatically update when changed in the respective worksheets. This is mostly a read-only worksheet, changes should be made in Interview or Roadmap worksheets.

Software Assurance Maturity Model (SAMM) Roadmap

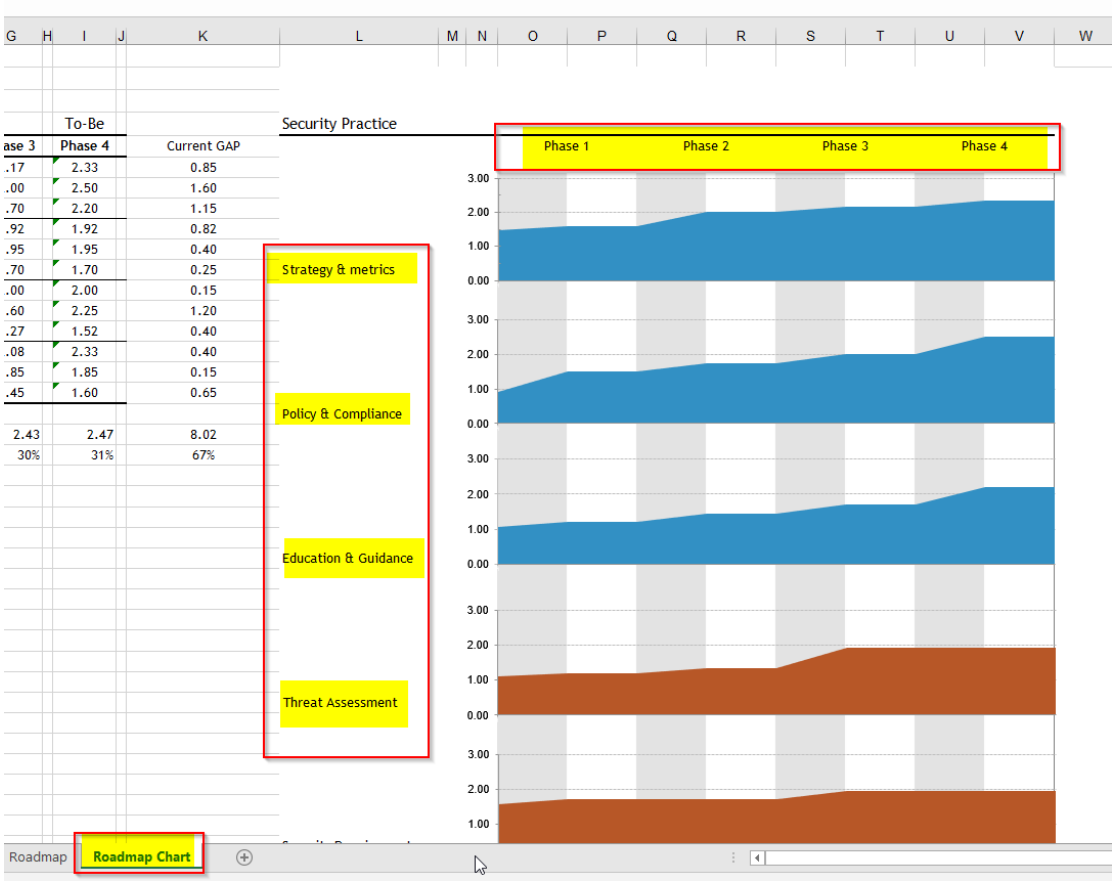
Organization:	Acme Brick Co
Project:	Brick Builder
Version	v1.0
Date	2/28/2017
Author	Steve

Source Data	As-Is				To-Be	
Security Practices/Phase	Start	Phase 1	Phase 2	Phase 3	Phase 4	Current GAP
Strategy & metrics	1.48	1.58	2.00	2.17	2.33	0.85
Policy & Compliance	0.90	1.50	1.75	2.00	2.50	1.60
Education & Guidance	1.05	1.20	1.45	1.70	2.20	1.15
Threat Assessment	1.10	1.20	1.35	1.92	1.92	0.82
Security Requirements	1.55	1.70	1.70	1.95	1.95	0.40
Secure Architecture	1.45	1.45	1.70	1.70	1.70	0.25
Design Analysis	1.85	1.85	1.85	2.00	2.00	0.15
Implementation Review	1.05	1.20	1.35	1.60	2.25	1.20
Security Testing	1.12	1.12	1.12	1.27	1.52	0.40
Issue Management	1.93	1.93	2.08	2.08	2.33	0.40
Environment Hardening	1.70	1.70	1.70	1.85	1.85	0.15
Operational Enablement	0.95	1.05	1.20	1.45	1.60	0.65
SAMM velocity:		1.35	1.77	2.43	2.47	8.02
		17%	22%	30%	31%	67%

Valid Maturity Levels
0
0.5
1
1.5
2
2.5

Attribution and License | Interview | Scorecard | Roadmap | Roadmap Chart

Εικόνα 11. Φύλλο «Roadmap Chart» συγκεντρωτικός πίνακας.



Εικόνα 12. Φύλλο «Roadmap Chart» διάγραμμα.

3.2 **Γενική περιγραφή του νέου εργαλείου**

Στο παρόν κεφάλαιο γίνεται μια γενική περιγραφή του πως θα εμπλουτιστεί με νέα στοιχεία, στήλες και φύλλα το τροποποιημένο από εμάς εργαλείο και παρουσιάζεται η τελική του έκδοση.

Θα βασιστούμε σε ένα ήδη υπάρχων εργαλείο από την εργαλειοθήκη του OWASP, το «SAMM Assessment Toolbox v1.5», όπου μετά από την απαραίτητη εισαγωγή δεδομένων από ένα χρήστη, θα αποτυπώνει την υφιστάμενη κατάσταση ωριμότητας του μοντέλου SAMM καθώς και τις τέσσερις (4)διαφορετικές φάσεις που επιθυμεί να φτάσει ένας οργανισμός.

Πιο συγκεκριμένα η δική μας παρέμβαση στην παρούσα έρευνα είναι η τροποποίηση του εργαλείου με τέτοιο τρόπο, ώστε να παραμένει ως έχει η μέτρηση των δεικτών που έχουν σχέση με την μέτρηση των δεικτών ωριμότητας

ως προς το μοντέλο SAMM και ο εμπλουτισμός του υπάρχοντος εργαλείου με την προσθήκη νέων καρτελών, στηλών, πινάκων και γραφημάτων, έχοντας ως τελικό σκοπό την αποτύπωση της υπάρχουσας συμμόρφωσης του GDPR σε σχέση με το SAMM, την επιθυμητή συμμόρφωση για κάθε έναν από τους τρείς (3) κύκλους που επιθυμεί να φτάσει ο οργανισμός και τέλος η υπάρχουσα απόκλιση του GDPR γενικά σε σχέση με το πρότυπο SAMM.

Το αποτέλεσμά μας, στοχεύει στο να δημιουργηθεί ένα εργαλείο όπου μετά την εισαγωγή δεδομένων θα αναλύει και θα παρουσιάζει τα όποια κενά σημεία υπάρχουν σε ένα κύκλο ανάπτυξης λογισμικού (Software Development Lifecycle - SDLC) καθώς κυρίως θα εστιάσει σε δυο (2) σημαντικές περιοχές, όπως και κατά πόσον ένα έργο ή ένας οργανισμός εναρμονίζεται με το μοντέλο SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού) και ταυτοχρόνως αν καλύπτεται ο νέος Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) και σε τι βαθμό.

Επιπρόσθετα, ένα σημαντικό στοιχείο που θα αναπτύξουμε στο εργαλείο είναι η δυνατότητα να αποτυπώνει τις οποίες αποκλίσεις από το GDPR.

Αυτό θα μας δώσει τη δυνατότητα, με βάση τα συμπεράσματα που θα εξαχθούν να μπορέσουν να προταθούν σημεία και μέτρα βελτίωσης μέσω αυτόνομων ενεργειών ή συμπληρωματική εφαρμογή άλλων προτύπων και μοντέλων ούτως ώστε το τελικό μας αποτέλεσμα να είναι σε πλήρη κάλυψη του μοντέλου SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού) και των απαιτήσεων του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

3.3 Σχεδιασμός Εργαλείου και Απαιτούμενες προδιαγραφές

Εφόσον έχει περιγραφεί η υφιστάμενη κατάσταση του εργαλείου, θα πρέπει να απαντηθεί το ερώτημα «Τι» θέλουμε να κάνει το εργαλείο.

Αποτέλεσμα αυτού είναι η δημιουργία όλων εκείνων των τεχνικών προδιαγραφών, χαρακτηριστικών και απαιτήσεων που πρέπει να διαθέτει το

εργαλείο, για να μπορέσει να ανταποκριθεί με σωστό και βέλτιστο τρόπο στον σκοπό της δημιουργίας του.

Κατά την διάρκεια του σχεδιασμού του εργαλείου, θα χαρτογραφήσουμε τις απαιτήσεις του GDPR μέσα στις τυπικές δραστηριότητες ενός κύκλου SAMM και θα καλύπτονται τα βασικά σημεία τα οποία είναι:

- Σε ποιο σημείο της διαδικασίας θα πρέπει να συμπεριλαμβάνεται και να εμπλέκεται ο Υπεύθυνος Διαχείρισης Δεδομένων (ΥΠΔ) στο πλαίσιο της διακυβέρνησης για την ασφάλεια των λογισμικών;
- Μια χαρτογράφηση σχετικά με τις απαιτήσεις του GDPR, σε σχέση με τις απαιτήσεις που υπάρχουν στην ασφάλεια του λογισμικού.
- Την εφαρμογή της προστασίας των ιδιωτικών δεδομένων (Data Privacy) από την πρώτη φάση της δημιουργίας ενός ασφαλούς λογισμικού και ενσωμάτωση στην αρχιτεκτονική του.
- Την ενσωμάτωση της έννοιας της «Ιδιωτικότητας» σε πολίτικες και οδηγίες που σχετίζονται με την συγγραφή ασφαλούς λογισμικού για προγραμματιστές.
- Την διενέργεια λίστας ελέγχου σε σημεία που άπτονται του GDPR κατά την διάρκεια δοκίμων διείσδυσης και δοκιμών ασφάλειας λογισμικού.
- Ενσωμάτωση και εφαρμογή των ειδικών απαιτήσεων γνωστοποίησης παραβίασης GDPR στις διαδικασίες διαχείρισης ευπάθειας και συμβάντων.

Κεφάλαιο 4

4 Υλοποίηση

Στο προηγούμενο κεφάλαιο αποτυπώνεται η περιγραφή του εργαλείου και οι απαιτήσεις του. Στο παρόν κεφάλαιο παρουσιάζεται η διαδικασία της υλοποίησης. Επεξηγείται δηλαδή το «Πως» δουλεύει το εργαλείο, και ποιες είναι οι απαραίτητες προσθήκες που έχουν γίνει στο εργαλείο για να μπορέσει να ανταποκριθεί στα ανωτέρω ζητούμενα και τις απαιτήσεις που αναλύονται στα παραπάνω κεφάλαια, καθώς και μια αναλυτική επεξήγηση των φύλλων του εργαλείου για τον τρόπο που δουλεύει και ανταποκρίνεται στην εισαγωγή δεδομένων.

Αυτό επιτεύχθηκε με τον εμπλουτισμό του βασικού εργαλείου αξιολόγησης [20] όπως αυτό καταγράφεται στο φύλλο «Interview» και αποτυπώνεται στο φύλλο «SAMM-GDPR Scorecard», το οποίο αποτελεί μια εμπλουτισμένη έκδοση του φύλλου «Scorecard». Αντίστοιχα στο φύλλο «SAMM-GDPR Roadmap chart» αποτυπώνεται ο οδικός χάρτης και για τη σταδιακή αύξηση του επιπέδου συμμόρφωσης του GDPR. Το φύλλο «SAMM-GDPR Roadmap chart» αποτελεί την εμπλουτισμένη έκδοση του φύλλου «Roadmap chart».

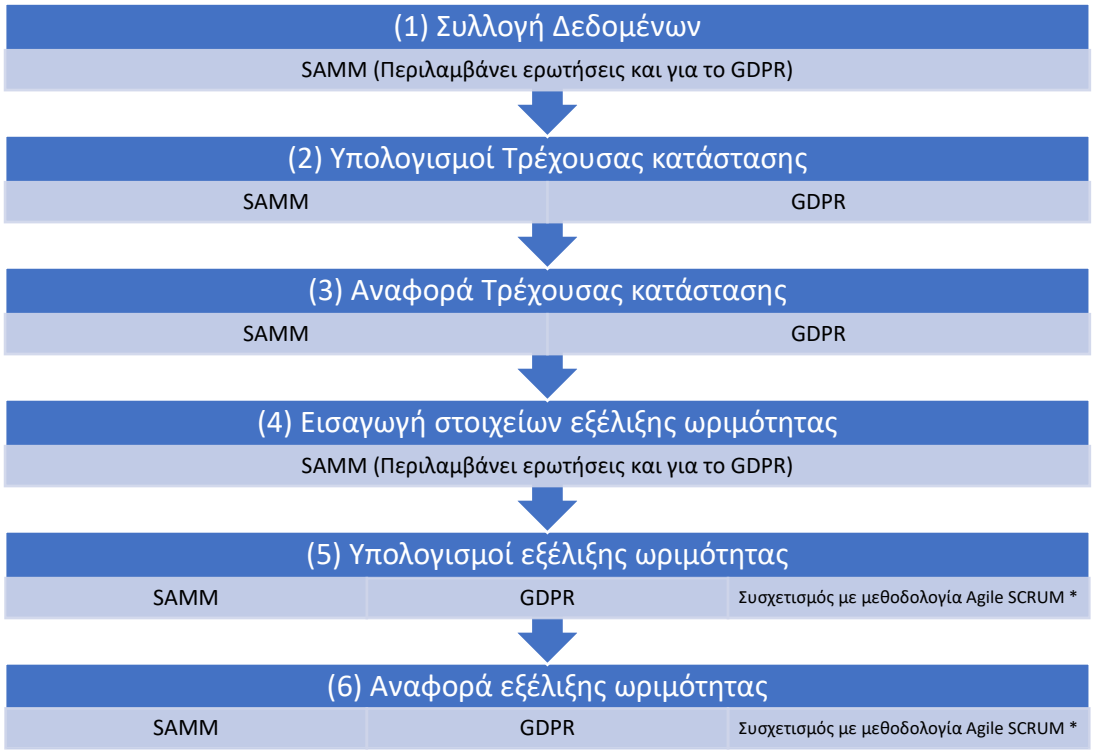
Ειδικότερα αλλαγές έχουν πραγματοποιηθεί στα παρακάτω σημεία:

1. Φύλλο «Interview»
    a. Στήλη K: Προστέθηκε το «Rating» που αφορά το GDPR.
    b. Στήλη L: Προστέθηκε η συσχέτιση με το GDPR σύμφωνα με την μελέτη της TOREON [22].
2. Φύλλο «Roadmap»
    a. Στήλη K: Προστέθηκε το «GDPR-SAMM Rating» για κάθε ένα επίπεδο ωριμότητας (Maturity Level), καθώς και για την τρέχουσα κατάσταση (Current State).

    b. Στήλη L: Προστέθηκε η συσχέτιση με το GDPR σύμφωνα με την μελέτη της TOREON [22].
3. Φύλλο «SAMM-GDPR Scorecard»
    a. Στήλη H: Προστέθηκε το «GDPR-SAMM».
    b. Στήλες I&J: Προστέθηκε Πίνακας «Current GDPR-SAMM Maturity» τόσο για την τρέχουσα κατάσταση όσο και για την 4η φάση ωριμότητας (Maturity Level).
    c. Στήλες L έως R: Προστέθηκε Διάγραμμα.
4. Φύλλο «SAMM-GDPR Roadmap chart»
    a. Προσθήκη στηλών στον πίνακα «Source Data» με τα δεδομένα που αφορούν το GDPR.
    b. Αντικατάσταση του διαγράμματος με τις φάσεις (πιο ευανάγνωστο) και overlay 2 διαγραμμάτων (SAMM και GDPR).
5. Φύλλο «Lookups»
    a. Εμφάνιση (Unhide).
    b. Δημιουργία λίστας «Yes_No» από τα κελιά $A$4:$A$5

Επίσης στο παρακάτω διάγραμμα ροής (flowchart) αναπαρίσταται η διαδικασία που ακολουθείται ως προς τον τρόπο λειτουργίας που ακολουθεί το νέο εργαλείο. Παρουσιάζεται με ξεκάθαρο τρόπο η ροή των εργασιών μέσα στο εργαλείο και οι δραστηριότητες που λαμβάνουν χώρα. Οι ενέργειες που γίνονται από τη μεριά του χρήστη καθώς και οι διεργασίες που λαμβάνουν μέρος αυτοματοποιημένα στα σχετικά φύλλα βάσει των συναρτήσεων που έχουν δημιουργηθεί μέσα στο εργαλείο.

Διαδικασία υπολογισμού της τρέχουσας και της βελτιωμένης συμμόρφωσης με το GDPR.



Διάγραμμα 1. Διαδικασία υπολογισμού της τρέχουσας και της βελτιωμένης συμμόρφωσης με το GDPR.

#	Βήμα διαδικασίας	Σχετικό φύλλο εμπλουτισμένου excel	Απαιτεί δεδομένα από τον χρήστη	Σύντομη περιγραφή λειτουργίας
1	Συλλογή Δεδομένων	*Interview*	Ναι	Εισαγωγή απαντήσεων για την τρέχουσα κατάσταση σε δομημένο ερωτηματολόγιο
2	Υπολογισμοί Τρέχουσας κατάστασης	*Interview*	Ναι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά security practice για τη συμμόρφωση με το SAMM και το GPDR
		Scorecard	Όχι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά business function για τη συμμόρφωση με το SAMM
		SAMM-GDPR Scorecard	Όχι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά business function για τη συμμόρφωση με το SAMM και το GPDR
3	Αναφορά Τρέχουσας κατάστασης	*Scorecard*	Όχι	Επισκόπηση επιπέδου συμμόρφωσης ανά security practice και business function για τη συμμόρφωση με το SAMM (Γράφημα Radar)

		SAMM-GDPR Scorecard	Όχι	Επισκόπηση επιπέδου συμμόρφωσης ανά security practice και business function για τη συμμόρφωση με το SAMM και το GPDR (Γράφημα Radar)
4	Εισαγωγή στοιχείων εξέλιξης ωριμότητας	*Roadmap*	Ναι	Εισαγωγή απαντήσεων για την επιθυμητή μελλοντική ωριμότητα SAM σε δομημένο ερωτηματολόγιο (αντίστοιχο του ερωτηματολογίου του φύλλου *Interview*
5	Υπολογισμοί εξέλιξης ωριμότητας	*Roadmap*	Ναι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά security practice και ανά φάση ωριμότητας για τη συμμόρφωση με το SAMM και το GDPR
		Roadmap Chart	Όχι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά security practice, business function και ανά φάση ωριμότητας για τη συμμόρφωση με το SAMM
		SAMM-GDPR Roadmap Chart	Όχι	Αυτόματος υπολογισμός δείκτη συμμόρφωσης (rating) ανά security practice, business function και ανά φάση ωριμότητας για τη συμμόρφωση με το SAMM και το GDPR
6	Αναφορά εξέλιξης ωριμότητας	*Roadmap Chart*	Όχι	Επισκόπηση επιπέδου συμμόρφωσης ανά security practice, business function και φάση ωριμότητας για τη συμμόρφωση με το SAMM (Γραφήματα Radar και Area). Αποτύπωση velocity της διαδικασίας ωρίμανσης με το SAMM
		SAMM-GDPR Roadmap Chart	Όχι	Επισκόπηση επιπέδου συμμόρφωσης ανά security practice, business function και φάση ωριμότητας για τη συμμόρφωση με το SAMM και το GDPR (Γραφήματα Radar και Stacked Bar). Αποτύπωση velocity της διαδικασίας ωρίμανσης με το SAMM και το GDPR.

Διάγραμμα 2. Βήματα διαδικασίας υπολογισμού της τρέχουσας και της βελτιωμένης συμμόρφωσης με το GDPR.

Παρακάτω περιγράφονται αναλυτικότερα οι όποιες παρεμβάσεις έγιναν στο πλαίσιο του εμπλουτισμού του εργαλείου.

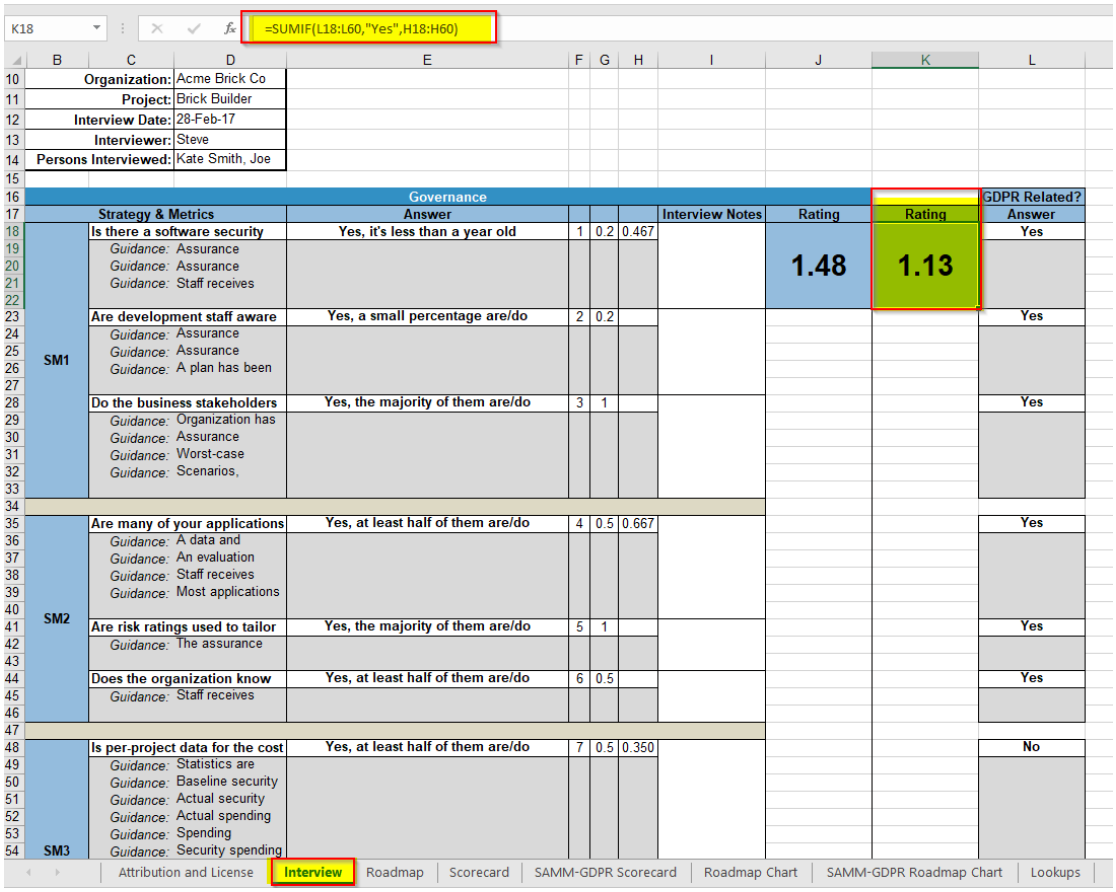
4.1 **Φύλλο «Interview»**

Στο φύλλο «Interview» έχουν πραγματοποιηθεί κάποιες προσθήκες για να μπορέσει να υπολογιστεί και αντίστοιχα ο ανάλογος δείκτης ωριμότητας για το GDPR. Έτσι έλαβαν χώρα δυο πολύ συγκεκριμένες παρεμβάσεις.

Πρώτον εισήχθη μια νέα στήλη «Rating» ακριβώς δίπλα από την ανάλογη στήλη Rating που υπολογίζει το SAMM, με τη διαφορά ότι αυτή η νέα στήλη «Rating» υπολογίζει τον υφιστάμενο δείκτη ωρίμανσης του GDPR. Η δεύτερη στήλη που προστέθηκε ονομάζεται «GDPR Related?» (στήλη «L»), όπου ο χρήστης που εισάγει τα δεδομένα, επιλεγεί μεταξύ δυο δυνητικών απαντήσεων, Ναι ή Όχι (Yes / No).

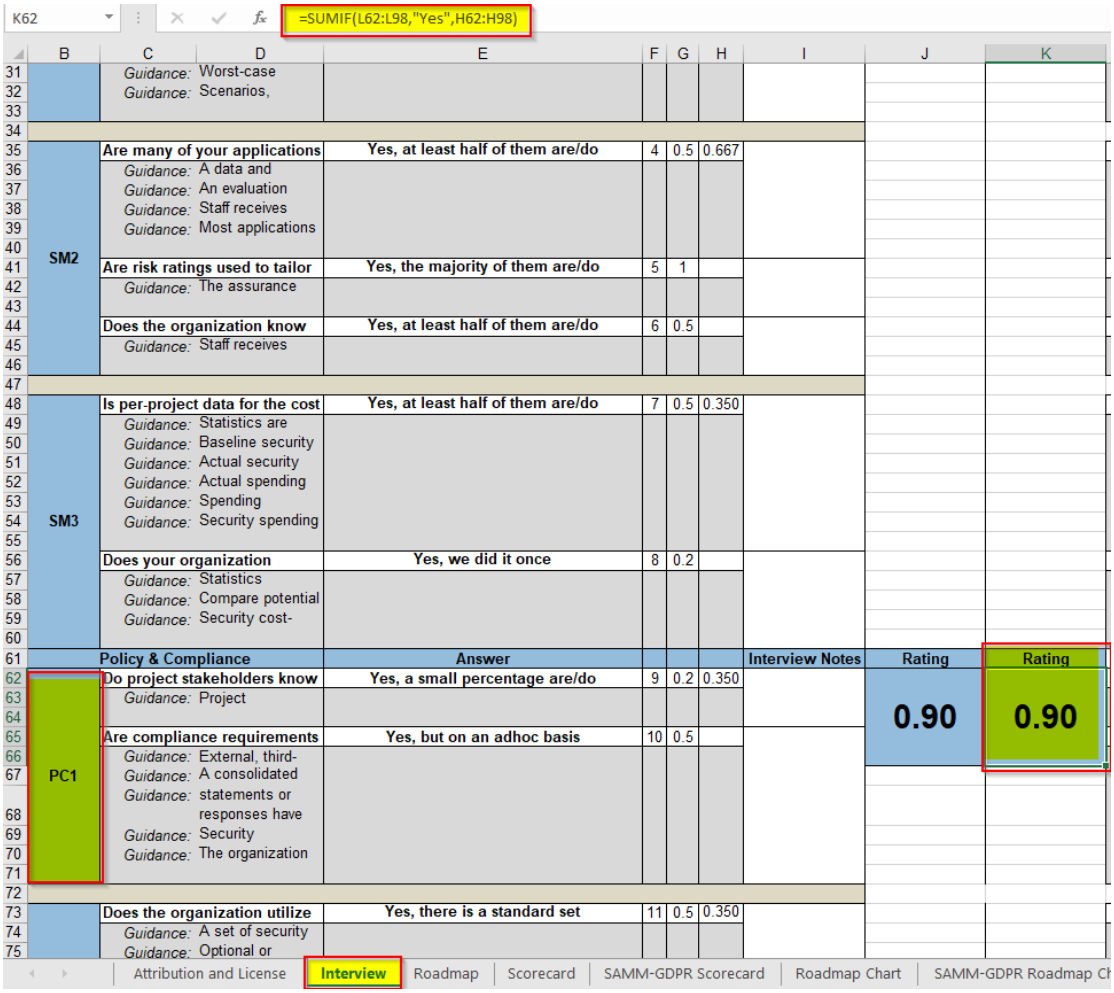
Ο αλγόριθμος που δημιουργήθηκε για να μπορέσει να υπολογιστεί ο τρέχων δείκτης ωρίμανσης του GDPR βασίζεται στην συνάρτηση SUMIF και είναι «=SUMIF(L18:L60,"Yes",H18:H60)».

Επί της ουσίας αθροίζει τις τιμές στις περιοχές L18 έως L60 της στήλης L που είναι η στήλη «GDPR Related?», διαβάζει αν έχει επιλεχθεί ως απάντηση το Ναι (Yes) και υπολογίζει αυτές τις απαντήσεις μόνο για την πρώτη πρακτική ασφάλειας η οποία είναι η «Στρατηγική & μετρήσεις» (Strategy & Metrics), το SM1 έως SM3 που ανήκει στις περιοχές H18 έως H60.



Εικόνα 13. Φύλλο «Interview», συνάρτηση SUMIF για Στρατηγική και Μετρήσεις .

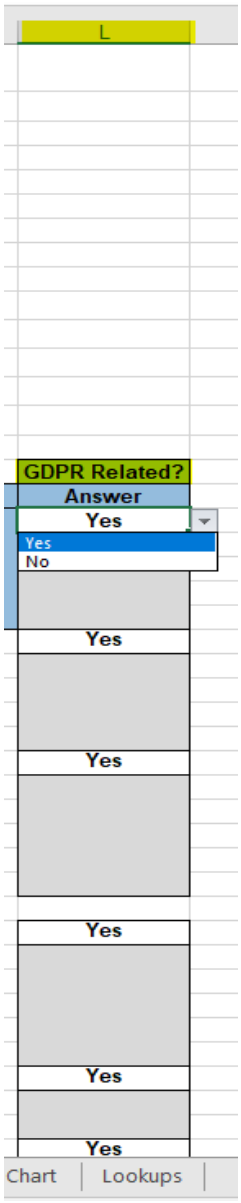
Αντίστοιχοι αλγόριθμοι βασισμένοι στον ίδιο τύπο συνάρτησης έχουν δημιουργηθεί και για τις υπόλοιπες έντεκα πρακτικές ασφάλειας με τις ανάλογες αλλαγές στις περιοχές του φύλλου, για να είναι ικανό το εργαλείο να υπολογίζει με σωστό τρόπο τους αντίστοιχους δείκτες ωριμότητας ανά πρακτική ασφάλειας όπως φαίνεται και στην εικόνα 14 (Φύλλο «Interview», συνάρτηση SUMIF για Πολιτική και Συμμόρφωση) που βρίσκεται ακριβώς παρακάτω, και η οποία παρουσιάζει την συνάρτηση SUMIF για την πρακτική ασφάλειας PC1, Πολιτική και Συμμόρφωση (Policy & Compliance).



31		Guidance: Worst-case								
32		Guidance: Scenarios,								
33										
34										
35	SM2	Are many of your applications	Yes, at least half of them are/do	4	0.5	0.667				
36		Guidance: A data and								
37		Guidance: An evaluation								
38		Guidance: Staff receives								
39		Guidance: Most applications								
40										
41		Are risk ratings used to tailor	Yes, the majority of them are/do	5	1					
42		Guidance: The assurance								
43										
44		Does the organization know	Yes, at least half of them are/do	6	0.5					
45		Guidance: Staff receives								
46										
47										
48	SM3	Is per-project data for the cost	Yes, at least half of them are/do	7	0.5	0.350				
49		Guidance: Statistics are								
50		Guidance: Baseline security								
51		Guidance: Actual security								
52		Guidance: Actual spending								
53		Guidance: Spending								
54		Guidance: Security spending								
55										
56		Does your organization	Yes, we did it once	8	0.2					
57		Guidance: Statistics								
58		Guidance: Compare potential								
59		Guidance: Security cost-								
60										
61		Policy & Compliance	Answer				Interview Notes	Rating	Rating	
62	PC1	Do project stakeholders know	Yes, a small percentage are/do	9	0.2	0.350		0.90	0.90	
63		Guidance: Project								
64										
65		Are compliance requirements	Yes, but on an adhoc basis	10	0.5					
66		Guidance: External, third-								
67		Guidance: A consolidated								
		Guidance: statements or								
68		responses have								
69		Guidance: Security								
70		Guidance: The organization								
71										
72										
73		Does the organization utilize	Yes, there is a standard set	11	0.5	0.350				
74		Guidance: A set of security								
75		Guidance: Optional or								

Εικόνα 14. Φύλλο «Interview», συνάρτηση SUMIF για Πολιτική και Συμμόρφωση.

Κατά την διάρκεια επιλογής της απάντησης από τον χρήστη στην στήλη «GDPR Related?» (στήλη «L»), οι επιλογές των δυο δυνητικών απαντήσεων, Ναι ή Όχι (Yes / No) καθορίζονται στο φύλλο «Lookups» με την δημιουργία λίστας. Αυτό περιγράφεται παρακάτω στο κεφάλαιο 4.5



Εικόνα 15. Φύλλο «Interview», στήλη GDPR Related με απαντήσεις.

Στα παραπάνω κεφάλαια έχει περιγραφεί ότι το μοντέλο SAMM αποτελείται από τέσσερις επιχειρηματικές λειτουργίες. Η κάθε επιχειρηματική λειτουργία περιέχει τρεις πρακτικές ασφάλειας οπότε έχουμε συνολικά δώδεκα πρακτικές ασφαλείας. Κάθε πρακτική ασφαλείας αποτελεί μια περιοχή άμεσα συνδεδεμένη με την επιχειρηματική λειτουργία που πρεσβεύει.

Επίσης κάθε πρακτική ασφαλείας, αποτελείται από συγκεκριμένες ερωτήσεις όπου αυτές αποτελούν ένα σύνολο δραστηριοτήτων και οι οποίες δουλεύουν ακριβώς με τον ίδιο τρόπο όπως δουλεύουν στο υπάρχων εργαλείο του μοντέλου

SAMM. Το μοντέλο SAMM για καθεμιά από τις δώδεκα πρακτικές ασφάλειας καθορίζει ως στόχους, τρία επίπεδα ωριμότητας.

Αυτά αντιπροσωπεύονται από τη διαβάθμιση των απαντήσεων που θα δοθούν στο ερωτηματολόγιο. Οι απαντήσεις είναι πάντα διαρθρωμένες σε μια κλίμακα τεσσάρων (4) δυνητικών απαντήσεων με πιθανές επιλογές το όχι, μερικώς, περίπου μισό και πολύ.

Αν θα έπρεπε να αποτυπωθεί μια συσχέτιση ανάμεσα στις απαντήσεις και τον βαθμό μέτρησης του δείκτη ωριμότητας τους θα ήταν ως εξής:

- Το «όχι» ισούται με βαθμό μέτρησης 0, δηλαδή με την παντελής έλλειψη ωριμότητας.
- Το «Μερικώς» με βαθμό μέτρησης 0,2.
- Το «περίπου μισό» βαθμό μέτρησης 0,5.
- Το «πολύ» με τον μέγιστο βαθμό μέτρησης που είναι το 1.

Όσον αφορά την μέτρηση της ωριμότητας αυτή αποτυπώνεται στον πίνακα 3 (Πίνακας μέτρησης ωριμότητας) ως εξής:

Κλίμακα Ωριμότητας	**Περιγραφή**	**Βαθμός μέτρησης στο ερωτηματολόγιο**
Όχι	Παντελής έλλειψη ωριμότητας που αντιπροσωπεύει το χαμηλότερο σημείο όπου πλέον είναι υποχρεωτικό αυτό το σημείο εκκίνησης για τις όποιες δραστηριότητες.	0
Μερικώς	Αρχική κατανόηση και αυτόνομες ενέργειες σε θέματα ασφαλείας.	0,2
Περίπου	Αύξηση της αποτελεσματικότητα στον τομέα της ασφάλειας.	0,5
Πολύ	Πλήρης γνώση της πρακτικής ασφάλειας στο μέγιστο βαθμό.	1

Πίνακας 3. Πίνακας μέτρησης ωριμότητας.

Όλες οι παραπάνω πληροφορίες παρατηρούνται μέσα στις διάφορες στήλες του φύλλου «Interview».

Να σημειωθεί ότι κάθε πρακτική ασφάλειας μπορεί να βελτιωθεί ανεξάρτητα από τις άλλες μέσω αυτόνομων δράσεων.

Σε έναν συγκεντρωτικό πίνακα που έχει δημιουργηθεί ακριβώς παρακάτω, ο πίνακας 4, παρατηρούνται οι 4 επιχειρηματικές λειτουργίες και οι 12 πρακτικές ασφαλείας που εμπεριέχονται και οι οποίες υπάρχουν μέσα στο φύλλο «Interview».

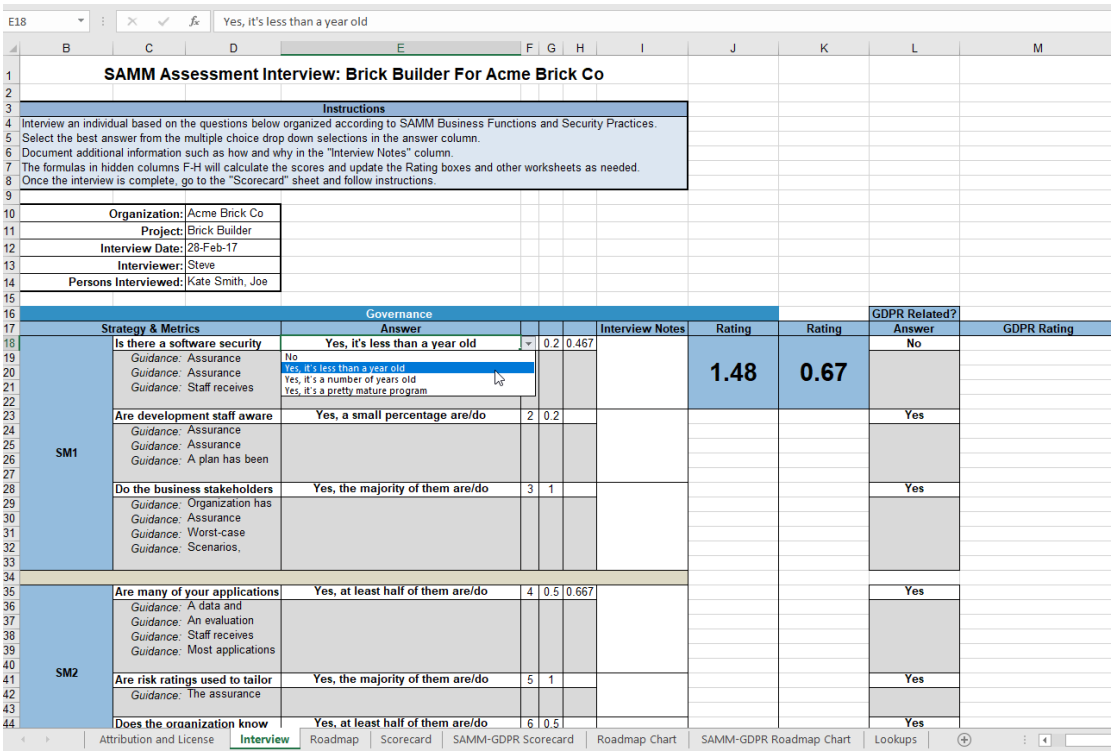
Επιχειρηματικές Λειτουργίες			
1) Διακυβέρνηση	**2) Κατασκευή**	**3) Επαλήθευση**	**4) Λειτουργίες**
Στρατηγική & μετρήσεις (SM)	Αξιολόγηση απειλών (TA)	Κριτική σχεδίου (DR)	Διαχείριση ζητημάτων (IM)
Πολιτική και συμμόρφωση (PC)	Απαιτήσεις ασφαλείας (SR)	Ανασκόπηση εφαρμογής (IR)	Περιβάλλον Σκλήρυνση (EH)
Εκπαίδευση & Καθοδήγηση (EG)	Ασφαλής αρχιτεκτονική (SA)	Δοκιμές ασφαλείας (ST)	Λειτουργική Ενεργοποίηση (OE)

Πίνακας 4. Επιχειρηματικές Λειτουργίες.

Εν συνεχεία, κάθε πρακτική ασφαλείας περιέχει ένα σύνολο δραστηριοτήτων που είναι διαρθρωμένο σε τρία επίπεδα ωριμότητας (1-3) τα οποία περιγράψαμε παραπάνω.

Οι δραστηριότητες στο χαμηλότερο επίπεδο ωριμότητας είναι συνήθως πιο εύκολο να εκτελεστούν και απαιτούν λιγότερη προσπάθεια από εκείνες που βρίσκονται στο υψηλότερο επίπεδο

Ο χρήστης καλείται να απαντήσει σε όλες τις ερωτήσεις από την στήλη «E» σύμφωνα με την υφιστάμενη πάντα κατάσταση ωριμότητας που υπάρχει στον οργανισμό, καθώς και να επιλέξει από την στήλη (L) αν η συγκεκριμένη ερώτηση σχετίζεται με τον Γενικό Κανονισμό για την Προστασία Δεδομένων (GDPR).



SAMM Assessment Interview: Brick Builder For Acme Brick Co

Instructions
Interview an individual based on the questions below organized according to SAMM Business Functions and Security Practices.
Select the best answer from the multiple choice drop down selections in the answer column.
Document additional information such as how and why in the "Interview Notes" column.
The formulas in hidden columns F-H will calculate the scores and update the Rating boxes and other worksheets as needed.
Once the interview is complete, go to the "Scorecard" sheet and follow instructions.

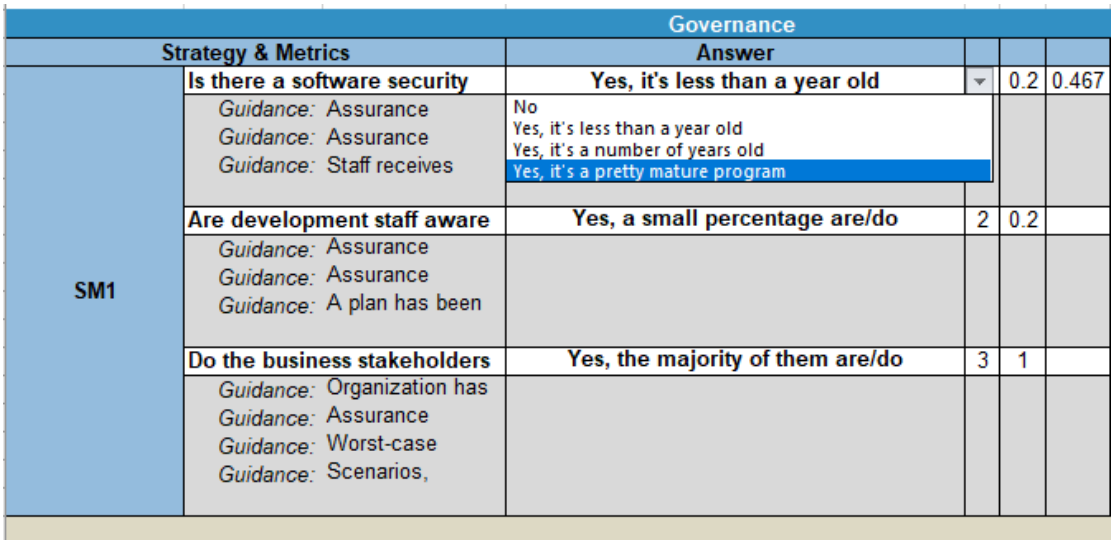
Organization:	Acme Brick Co
Project:	Brick Builder
Interview Date:	28-Feb-17
Interviewer:	Steve
Persons Interviewed:	Kate Smith, Joe

Governance									
Strategy & Metrics		Answer				Interview Notes	Rating	Rating	GDPR Related? Answer	GDPR Rating
SM1	Is there a software security	Yes, it's less than a year old		0.2	0.467		1.48	0.67	No	
	Guidance: Assurance Guidance: Assurance Guidance: Staff receives	No Yes, it's less than a year old Yes, it's a number of years old Yes, it's a pretty mature program								
	Are development staff aware	Yes, a small percentage are/do	2	0.2					Yes	
	Guidance: Assurance Guidance: Assurance Guidance: A plan has been									
	Do the business stakeholders	Yes, the majority of them are/do	3	1					Yes	
	Guidance: Organization has Guidance: Assurance Guidance: Worst-case Guidance: Scenarios,									
SM2	Are many of your applications	Yes, at least half of them are/do	4	0.5	0.667				Yes	
	Guidance: A data and Guidance: An evaluation Guidance: Staff receives Guidance: Most applications									
	Are risk ratings used to tailor	Yes, the majority of them are/do	5	1					Yes	
	Guidance: The assurance									
	Does the organization know	Yes, at least half of them are/do	6	0.5					Yes	

Attribution and License | Interview | Roadmap | Scorecard | SAMM-GDPR Scorecard | Roadmap Chart | SAMM-GDPR Roadmap Chart | Lookups

Εικόνα 16. Φύλλο «Interview» με GDPR.

Στην παρακάτω εικόνα, εικόνα 17, φαίνονται όλες οι δυνητικές απαντήσεις που μπορεί ένας χρήστης να επιλέξει για καθεμιά από τις ερωτήσεις που καλείται να συμπληρώσει μέσα στο εργαλείο.

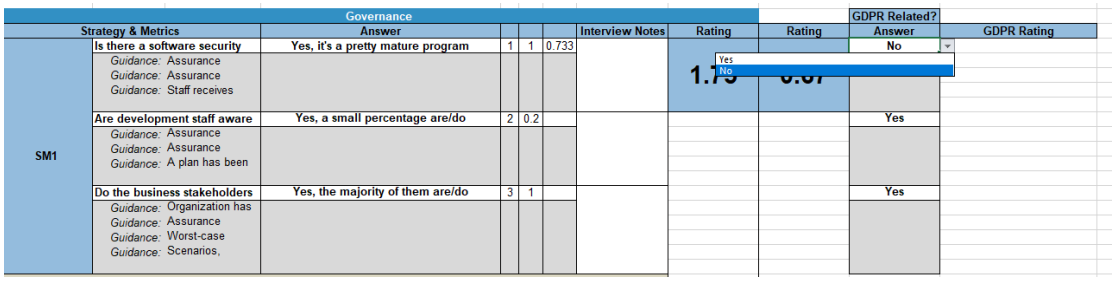


Governance					
Strategy & Metrics		Answer			
SM1	Is there a software security	Yes, it's less than a year old		0.2	0.467
	Guidance: Assurance Guidance: Assurance Guidance: Staff receives	No Yes, it's less than a year old Yes, it's a number of years old Yes, it's a pretty mature program			
	Are development staff aware	Yes, a small percentage are/do	2	0.2	
	Guidance: Assurance Guidance: Assurance Guidance: A plan has been				
	Do the business stakeholders	Yes, the majority of them are/do	3	1	
	Guidance: Organization has Guidance: Assurance Guidance: Worst-case Guidance: Scenarios,				

Εικόνα 17. Φύλλο «Interview», πιθανές απαντήσεις για SAMM.

Η βαθμολογία που προκύπτει βάσει της κάθε απάντησης είναι αυτή που περιγράφεται πιο πάνω.

Αντίστοιχα για το GDPR έχουμε τις 2 δυνητικές απαντήσεις που αναφέραμε παραπάνω που είναι, «Ναι ή Όχι», αναλόγως αν σχετίζεται η ερώτηση με το GDPR.



Governance								GDPR Related?	
Strategy & Metrics	Answer				Interview Notes	Rating	Rating	Answer	GDPR Rating
SM1	Is there a software security	Yes, it's a pretty mature program	1	1	0.733		1.75	No	
	Guidance: Assurance Guidance: Assurance Guidance: Staff receives								
	Are development staff aware	Yes, a small percentage are/do	2	0.2				Yes	
	Guidance: Assurance Guidance: Assurance Guidance: A plan has been								
	Do the business stakeholders	Yes, the majority of them are/do	3	1				Yes	
	Guidance: Organization has Guidance: Assurance Guidance: Worst-case Guidance: Scenarios,								

Εικόνα 18. Φύλλο «Interview», πιθανές απαντήσεις για GDPR.

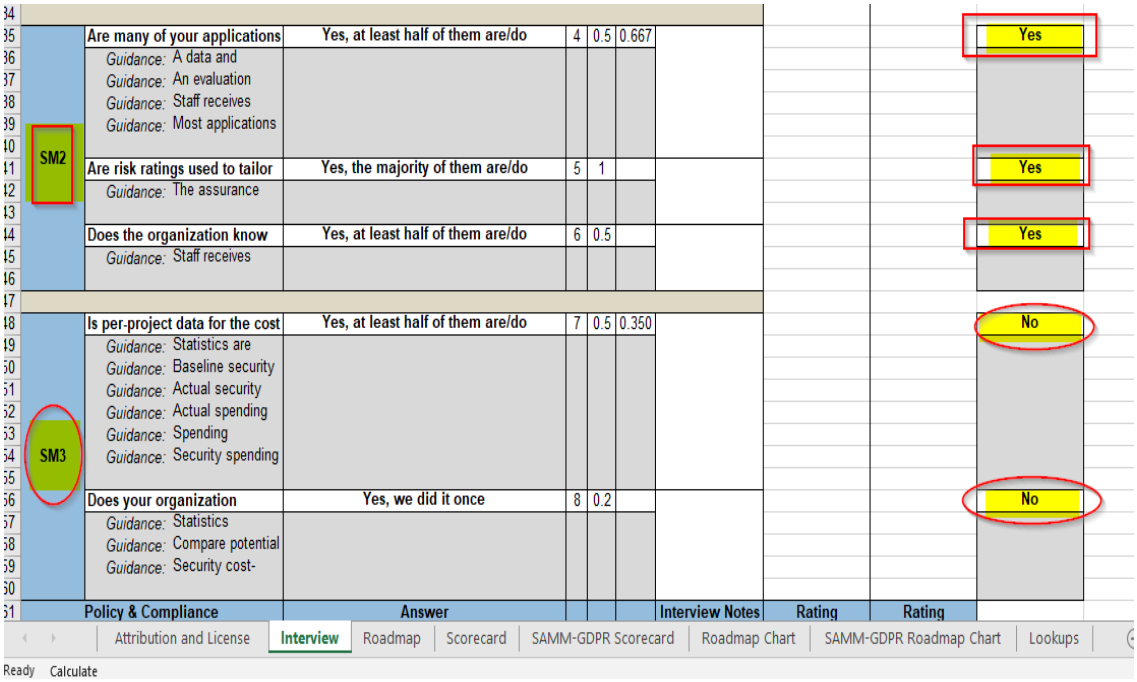
Το φύλλο «Interview» είναι από τις πιο βασικές καρτέλες διότι από τη συγκεκριμένη καρτέλα γίνεται η εισαγωγή των δεδομένων, τα οποία εν συνεχεία τροφοδοτούν τα υπόλοιπα φύλλα βάσει του αλγορίθμου που έχει δημιουργηθεί.

Στο παρόν σημείο να σημειωθεί ότι στην στήλη «GDPR Related?» οι απαντήσεις που έχουν δοθεί για το αν υπάρχει συσχέτιση της κάθε ερώτησης με τον GDPR, είναι τελικές. Καθώς επίσης η επιλογή της απάντησης «Ναι ή Όχι», έγινε μετά από προσεκτική μελέτη και αντίληψη της κάθε ερώτησης ξεχωριστά και το ειδικό βάρος αυτής.

Επίσης για κάθε πρακτική ασφαλείας όπως η «Στρατηγική και Μετρήσεις» (SM), υπάρχουν 3 επίπεδα, (SM1, SM2 και SM3).

Κάθε επίπεδο αποτελείται από κάποιες ερωτήσεις που είναι στην ουσία οι δραστηριότητες σε σχέση με το GDPR, και το κάθε επίπεδο, όπως για παράδειγμα το (SM1), είτε θα έχει όλες τις ερωτήσεις σχετιζόμενες με το GDPR είτε όχι. Δεν δύναται δηλαδή να υπάρχει μέσα σε μια πρακτική ασφάλειας ανά επίπεδο πάντα, ερώτηση που σχετίζεται με το GDPR και στο ίδιο επίπεδο άλλη ερώτηση που δεν σχετίζεται με το GDPR.

Όπως φαίνεται και στην παρακάτω εικόνα, για την πρακτική ασφάλειας SM2 και SM3 της πρακτικής ασφάλειας «Στρατηγική και Μετρήσεις» (SM), οι ερωτήσεις στο μεν SM2 που έχουν σχέση με το GDPR είναι όλες «Ναι – Yes», ενώ οι ερωτήσεις στο SM3 που δεν έχουν σχέση με το GDPR είναι όλες «Όχι – No».

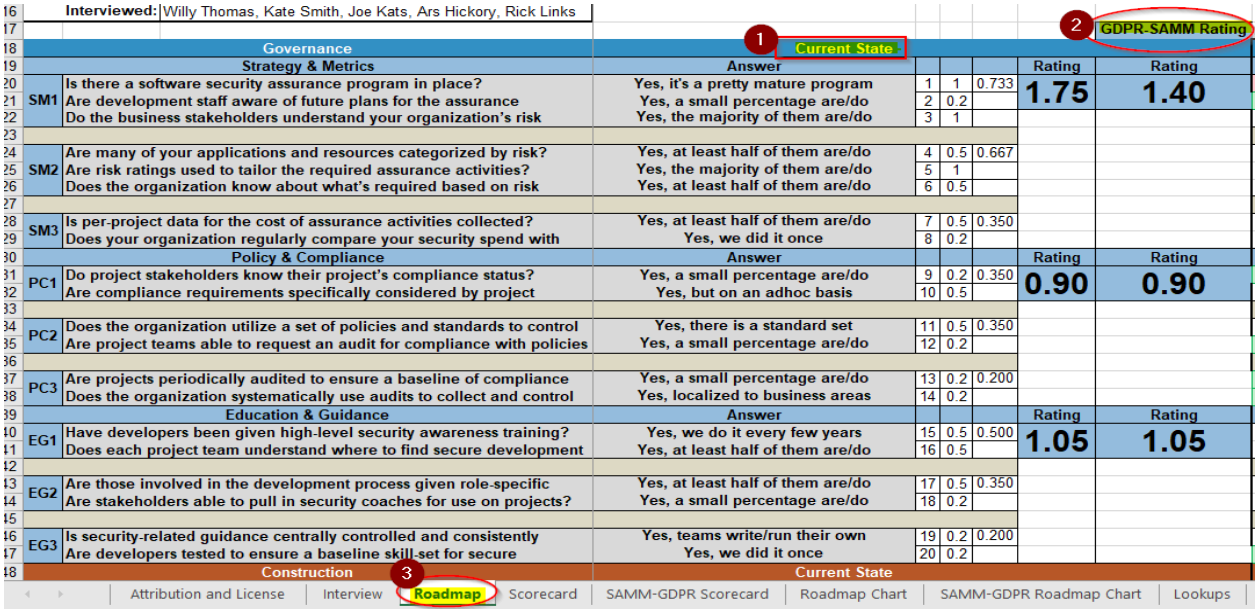


Εικόνα 19. Φύλλο «Interview», επίπεδα και GDPR συσχέτιση ερωτήσεων.

4.2 **Φύλλο «Roadmap»**

Στο φύλλο «Roadmap» η παρέμβαση είναι η πρόσθεση των στηλών «GDPR-SAMM rating» , για κάθε ένα από τα τέσσερα maturity level (στήλες O, T, Y, AD) αλλά και για την τρέχουσα κατάσταση (στήλη J) όπως φαίνεται και στους παρακάτω πίνακες.

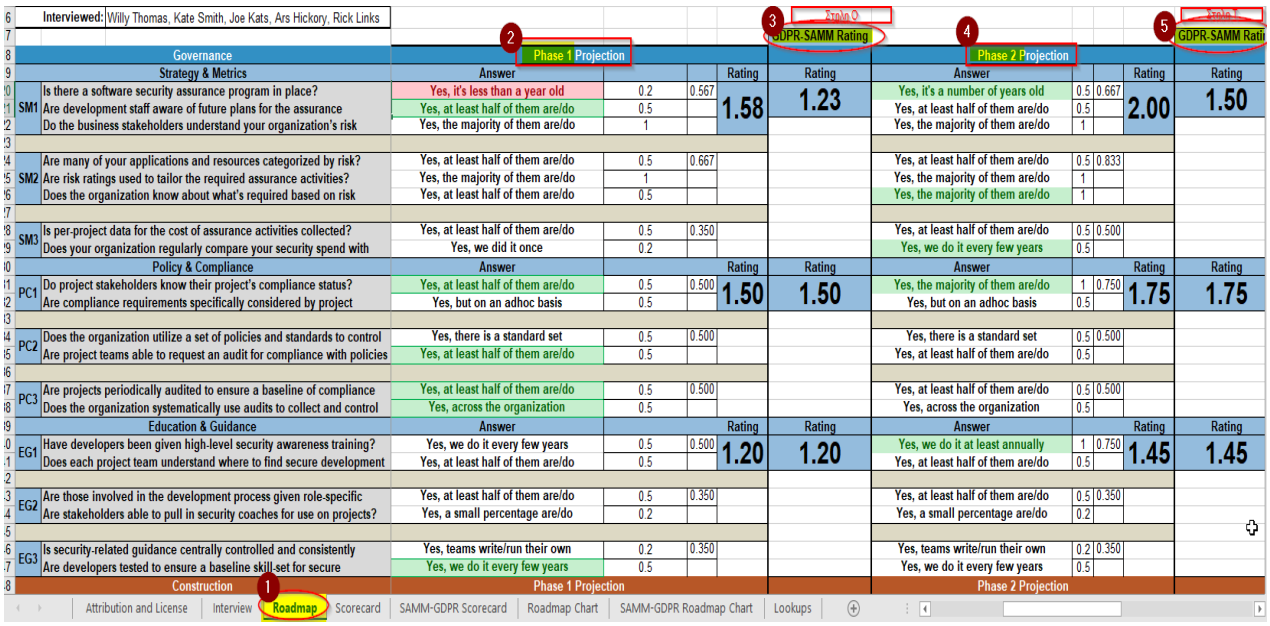
Παράλληλα στην στήλη AE, προστέθηκε η συσχέτιση με το GDPR.



Interviewed:	Willy Thomas, Kate Smith, Joe Kats, Ars Hickory, Rick Links								
								2 GDPR-SAMM Rating	
Governance		1 Current State							
Strategy & Metrics		Answer					Rating	Rating	
SM1	Is there a software security assurance program in place?	Yes, it's a pretty mature program	1	1	0.733		1.75	1.40	
	Are development staff aware of future plans for the assurance	Yes, a small percentage are/do	2	0.2					
	Do the business stakeholders understand your organization's risk	Yes, the majority of them are/do	3	1					
SM2	Are many of your applications and resources categorized by risk?	Yes, at least half of them are/do	4	0.5	0.667				
	Are risk ratings used to tailor the required assurance activities?	Yes, the majority of them are/do	5	1					
	Does the organization know about what's required based on risk	Yes, at least half of them are/do	6	0.5					
SM3	Is per-project data for the cost of assurance activities collected?	Yes, at least half of them are/do	7	0.5	0.350				
	Does your organization regularly compare your security spend with	Yes, we did it once	8	0.2					
Policy & Compliance		Answer					Rating	Rating	
PC1	Do project stakeholders know their project's compliance status?	Yes, a small percentage are/do	9	0.2	0.350		0.90	0.90	
	Are compliance requirements specifically considered by project	Yes, but on an adhoc basis	10	0.5					
PC2	Does the organization utilize a set of policies and standards to control	Yes, there is a standard set	11	0.5	0.350				
	Are project teams able to request an audit for compliance with policies	Yes, a small percentage are/do	12	0.2					
PC3	Are projects periodically audited to ensure a baseline of compliance	Yes, a small percentage are/do	13	0.2	0.200				
	Does the organization systematically use audits to collect and control	Yes, localized to business areas	14	0.2					
Education & Guidance		Answer					Rating	Rating	
EG1	Have developers been given high-level security awareness training?	Yes, we do it every few years	15	0.5	0.500		1.05	1.05	
	Does each project team understand where to find secure development	Yes, at least half of them are/do	16	0.5					
EG2	Are those involved in the development process given role-specific	Yes, at least half of them are/do	17	0.5	0.350				
	Are stakeholders able to pull in security coaches for use on projects?	Yes, a small percentage are/do	18	0.2					
EG3	Is security-related guidance centrally controlled and consistently	Yes, teams write/run their own	19	0.2	0.200				
	Are developers tested to ensure a baseline skill-set for secure	Yes, we do it once	20	0.2					
Construction		3 Current State							

Attribution and License | Interview | Roadmap | Scorecard | SAMM-GDPR Scorecard | Roadmap Chart | SAMM-GDPR Roadmap Chart | Lookups

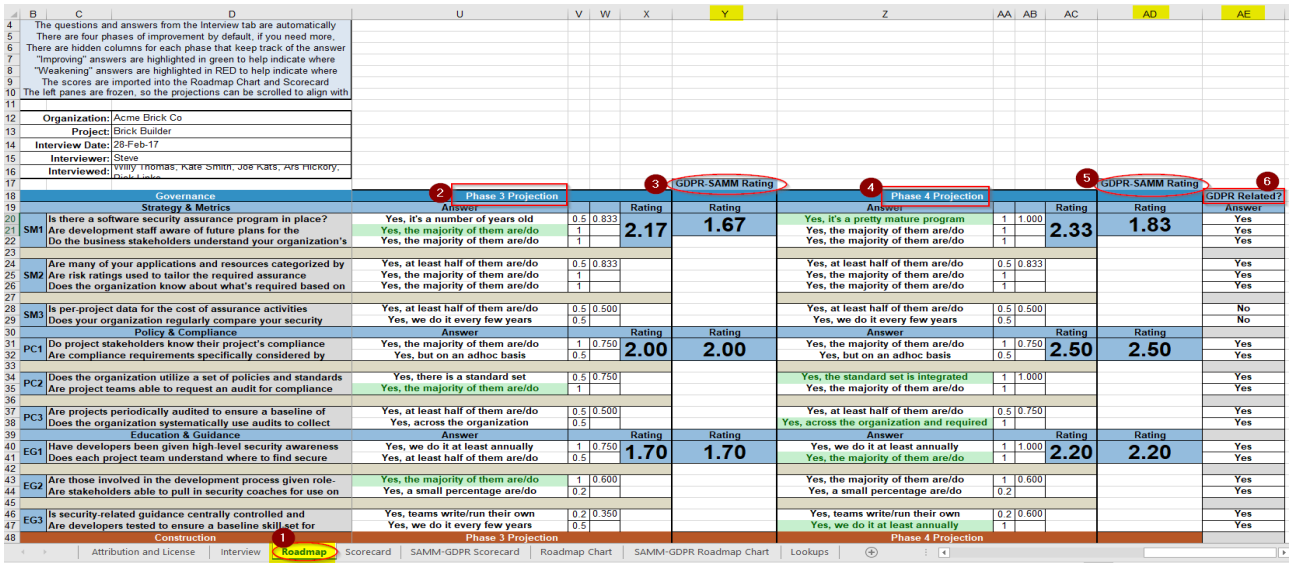
Εικόνα 20. Φύλλο «Roadmap», προσθήκη στήλης J.



Interviewed:	Willy Thomas, Kate Smith, Joe Kats, Ars Hickory, Rick Links					3 Στήλη Ο			4			5 Στήλη Τ	
		2 Phase 1 Projection				GDPR-SAMM Rating			Phase 2 Projection			GDPR-SAMM Rati	
Governance													
Strategy & Metrics		Answer			Rating	Rating			Answer			Rating	Rating
SM1	Is there a software security assurance program in place?	Yes, it's less than a year old	0.2	0.567					Yes, it's a number of years old	0.5	0.667		
	Are development staff aware of future plans for the assurance	Yes, at least half of them are/do	0.5		1.58	1.23			Yes, at least half of them are/do	0.5		2.00	1.50
	Do the business stakeholders understand your organization's risk	Yes, the majority of them are/do	1						Yes, the majority of them are/do	1			
SM2	Are many of your applications and resources categorized by risk?	Yes, at least half of them are/do	0.5	0.667					Yes, at least half of them are/do	0.5	0.833		
	Are risk ratings used to tailor the required assurance activities?	Yes, the majority of them are/do	1						Yes, the majority of them are/do	1			
	Does the organization know about what's required based on risk	Yes, at least half of them are/do	0.5						Yes, the majority of them are/do	1			
SM3	Is per-project data for the cost of assurance activities collected?	Yes, at least half of them are/do	0.5	0.350					Yes, at least half of them are/do	0.5	0.500		
	Does your organization regularly compare your security spend with	Yes, we did it once	0.2						Yes, we do it every few years	0.5			
Policy & Compliance		Answer			Rating	Rating			Answer			Rating	Rating
PC1	Do project stakeholders know their project's compliance status?	Yes, at least half of them are/do	0.5	0.500					Yes, the majority of them are/do	1	0.750		
	Are compliance requirements specifically considered by project	Yes, but on an adhoc basis	0.5		1.50	1.50			Yes, but on an adhoc basis	0.5		1.75	1.75
PC2	Does the organization utilize a set of policies and standards to control	Yes, there is a standard set	0.5	0.500					Yes, there is a standard set	0.5	0.500		
	Are project teams able to request an audit for compliance with policies	Yes, at least half of them are/do	0.5						Yes, at least half of them are/do	0.5			
PC3	Are projects periodically audited to ensure a baseline of compliance	Yes, at least half of them are/do	0.5	0.500					Yes, at least half of them are/do	0.5	0.500		
	Does the organization systematically use audits to collect and control	Yes, across the organization	0.5						Yes, across the organization	0.5			
Education & Guidance		Answer			Rating	Rating			Answer			Rating	Rating
EG1	Have developers been given high-level security awareness training?	Yes, we do it every few years	0.5	0.500					Yes, we do it at least annually	1	0.750		
	Does each project team understand where to find secure development	Yes, at least half of them are/do	0.5		1.20	1.20			Yes, at least half of them are/do	0.5		1.45	1.45
EG2	Are those involved in the development process given role-specific	Yes, at least half of them are/do	0.5	0.350					Yes, at least half of them are/do	0.5	0.350		
	Are stakeholders able to pull in security coaches for use on projects?	Yes, a small percentage are/do	0.2						Yes, a small percentage are/do	0.2			
EG3	Is security-related guidance centrally controlled and consistently	Yes, teams write/run their own	0.2	0.350					Yes, teams write/run their own	0.2	0.350		
	Are developers tested to ensure a baseline skill-set for secure	Yes, we do it every few years	0.5						Yes, we do it every few years	0.5			
Construction		1 Phase 1 Projection							Phase 2 Projection				

Attribution and License | Interview | Roadmap | Scorecard | SAMM-GDPR Scorecard | Roadmap Chart | SAMM-GDPR Roadmap Chart | Lookups

Εικόνα 21. Φύλλο «Roadmap», προσθήκη στηλών Ο και Τ.



Εικόνα 22. Φύλλο «Roadmap», προσθήκη στηλών Y, AD και AE.

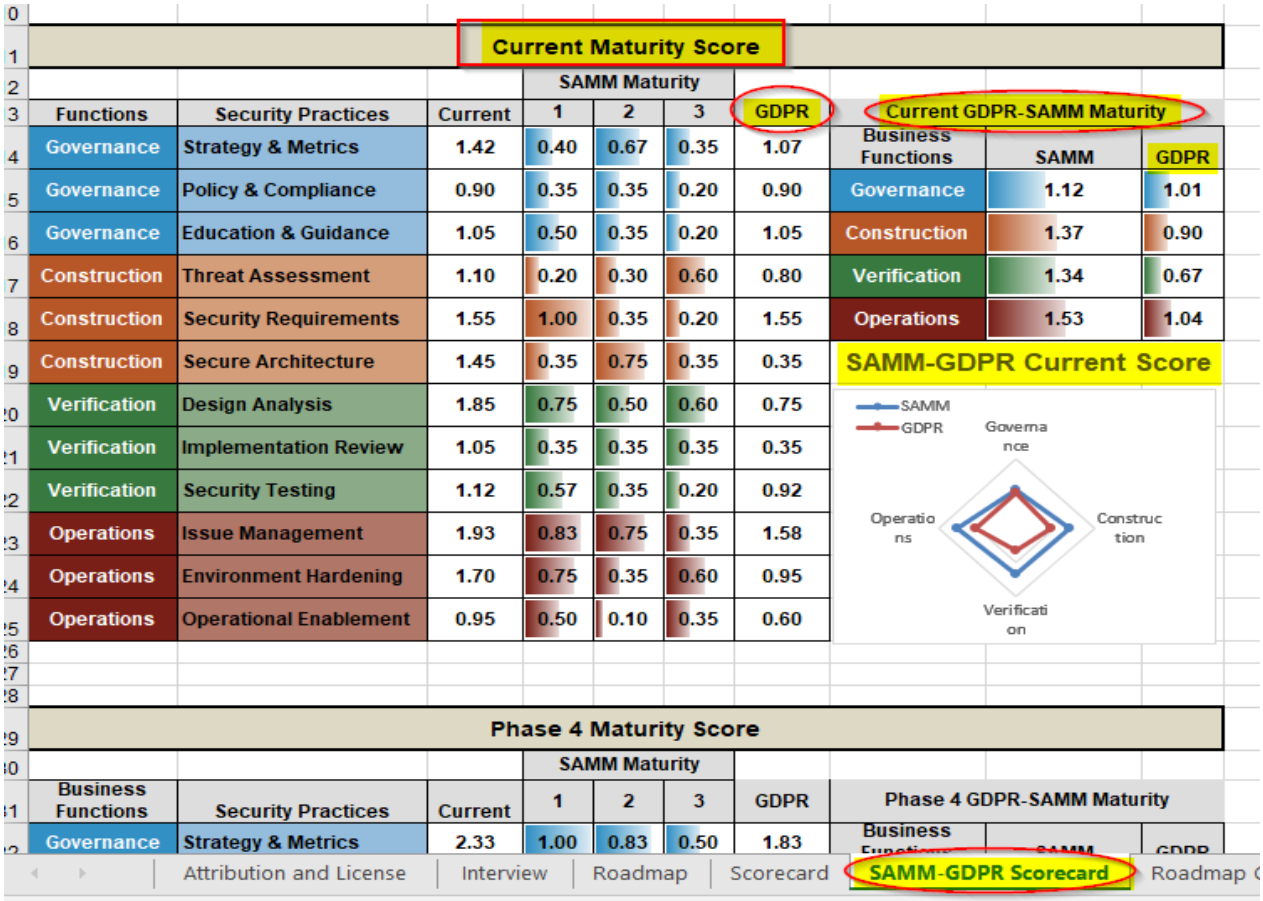
4.3 **Φύλλο «SAMM-GDPR Scorecard»**

Στο φύλλο «SAMM-GDPR Scorecard» έγιναν παρεμβάσεις σε πίνακες με την προσθήκη νέων στηλών και διαγραμμάτων. Έτσι για αυτό το λόγο στον πίνακα «Current Maturity Score» έγινε προσθήκη νέας στήλης (στήλης H) που μετράει το δείκτη ωριμότητας του GDPR σε καθεμιά από τις 12 πρακτικές ασφάλειας ξεχωριστά.

Τα δεδομένα αυτά τα αντλεί αυτόματα από την εισαγωγή των δεδομένων που έχουν γίνει στο φύλλο «Interview».

Επιπρόσθετα στον ίδιο πίνακα στις στήλες I και J προστέθηκε ο πίνακας «Current GDPR-SAMM Maturity» που αποτυπώνει τις μετρήσεις ωριμότητας ανά κάθε επιχειρηματική λειτουργία από τις τέσσερις συνολικά που έχει το SAMM, πάντα σε σχέση και με το πρότυπο SAMM και το GDPR, και εμφανίζει τους σχετικούς δείκτες ωριμότητας για την τρέχουσα κατάσταση του οργανισμού.

Επιπλέον στον ίδιο πίνακα, «Current Maturity Score», όπως φαίνεται και στις εικόνες 23 και 24, έχουμε δημιουργήσει ένα νέο διάγραμμα που μας δείχνει γραφιστικά, ποσό κοντά είναι το υφιστάμενο «Current Maturity Score» επίπεδο ωριμότητας SAMM και GDPR, σε κάθε επιχειρηματική λειτουργία.



Current Maturity Score

Functions	Security Practices	Current	SAMM Maturity 1	2	3	GDPR
Governance	Strategy & Metrics	1.42	0.40	0.67	0.35	1.07
Governance	Policy & Compliance	0.90	0.35	0.35	0.20	0.90
Governance	Education & Guidance	1.05	0.50	0.35	0.20	1.05
Construction	Threat Assessment	1.10	0.20	0.30	0.60	0.80
Construction	Security Requirements	1.55	1.00	0.35	0.20	1.55
Construction	Secure Architecture	1.45	0.35	0.75	0.35	0.35
Verification	Design Analysis	1.85	0.75	0.50	0.60	0.75
Verification	Implementation Review	1.05	0.35	0.35	0.35	0.35
Verification	Security Testing	1.12	0.57	0.35	0.20	0.92
Operations	Issue Management	1.93	0.83	0.75	0.35	1.58
Operations	Environment Hardening	1.70	0.75	0.35	0.60	0.95
Operations	Operational Enablement	0.95	0.50	0.10	0.35	0.60

Current GDPR-SAMM Maturity

Business Functions	SAMM	GDPR
Governance	1.12	1.01
Construction	1.37	0.90
Verification	1.34	0.67
Operations	1.53	1.04

SAMM-GDPR Current Score

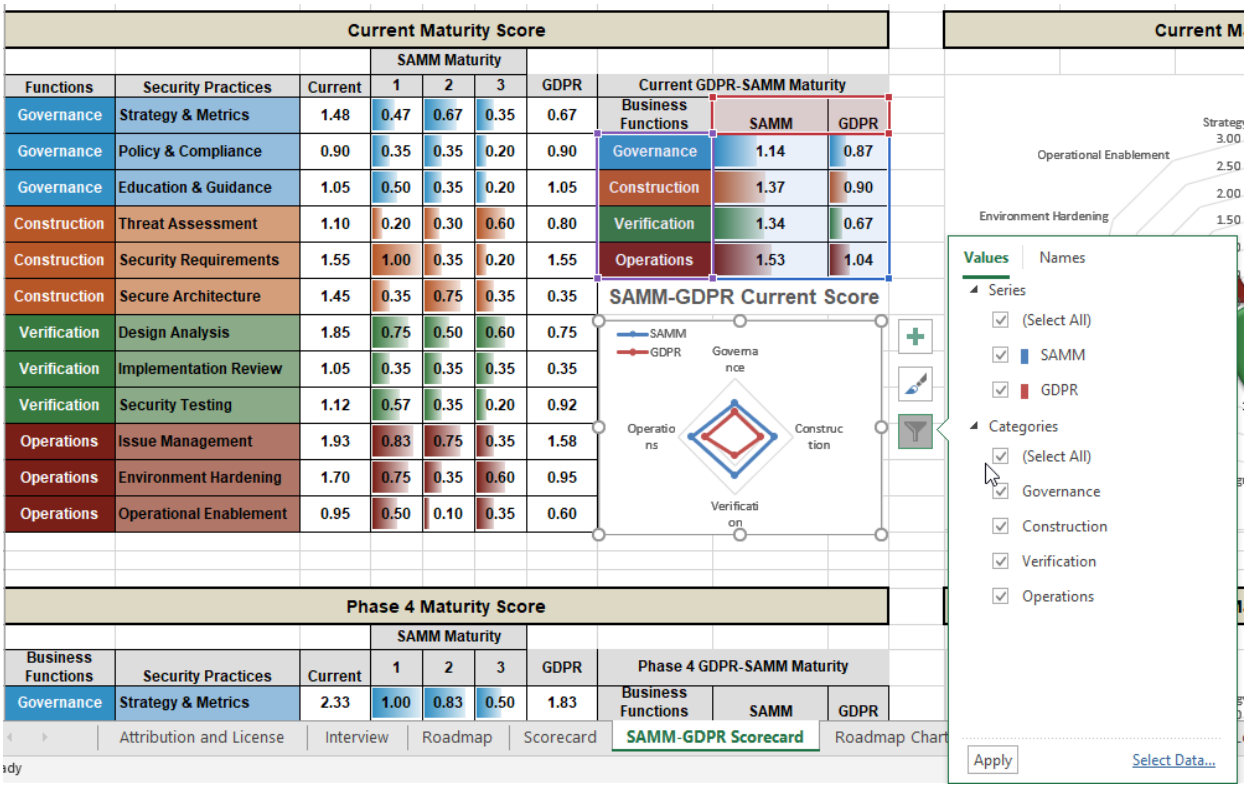
Phase 4 Maturity Score

Business Functions	Security Practices	Current	SAMM Maturity 1	2	3	GDPR
Governance	Strategy & Metrics	2.33	1.00	0.83	0.50	1.83

Phase 4 GDPR-SAMM Maturity

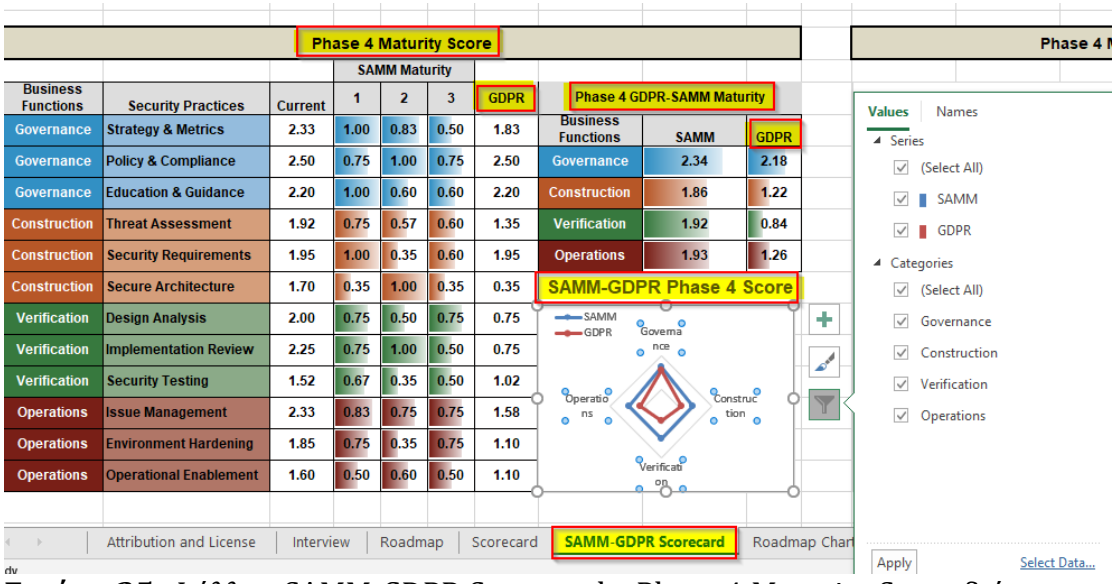
Business Functions	SAMM	GDPR

Εικόνα 23. Φύλλο «SAMM-GDPR Scorecard», Current Maturity Score πίνακας με GDPR.



Εικόνα 24. Φύλλο «SAMM-GDPR Scorecard», Current Maturity Score διάγραμμα SAMM-GDPR.

Ανάλογες προσθήκες έχουν πραγματοποιηθεί στους πίνακες της «Phase 4 Maturity Score» όπως φαίνεται στην εικόνα 25.



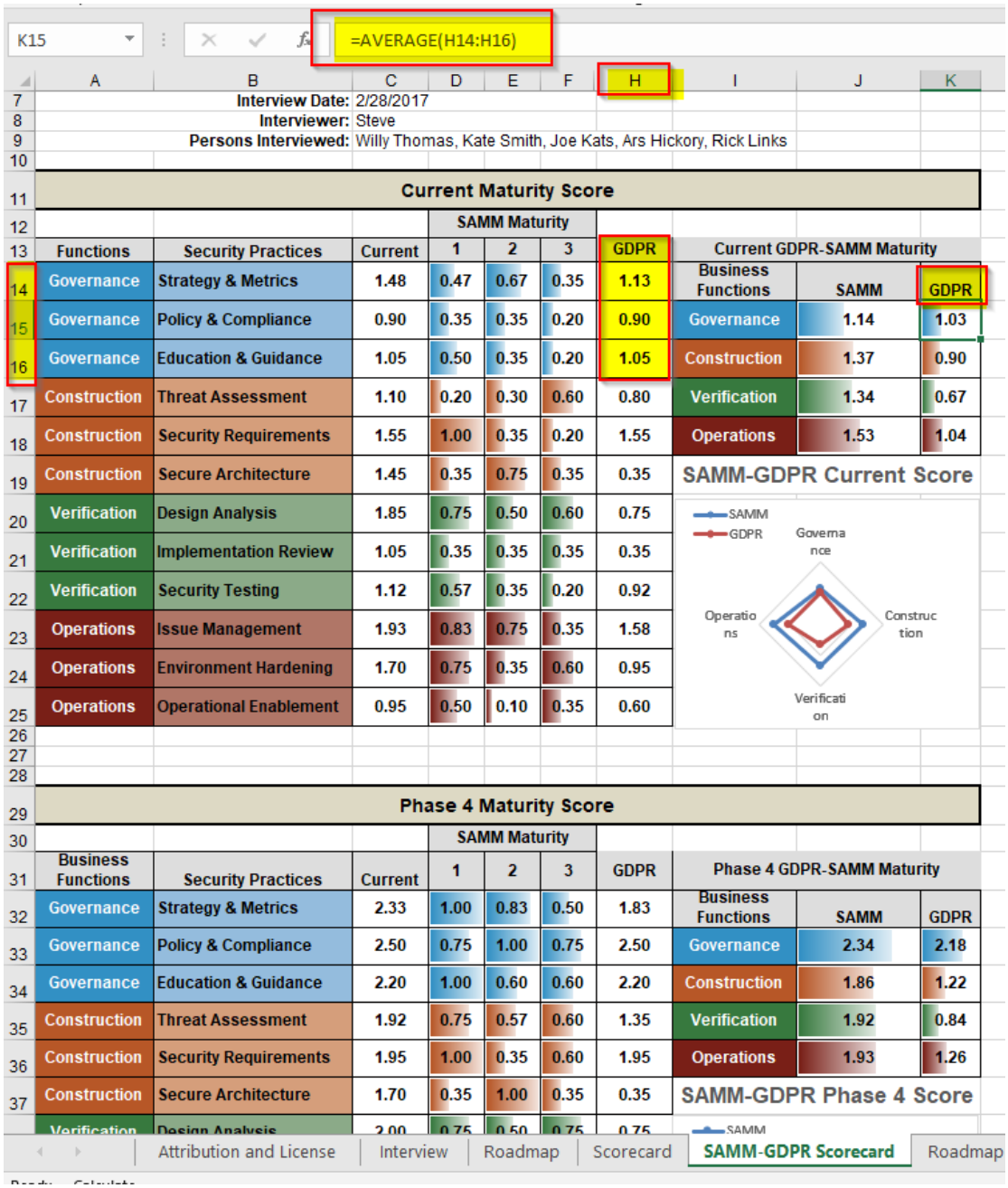
Εικόνα 25. Φύλλο «SAMM-GDPR Scorecard», Phase 4 Maturity Score διάγραμμα SAMM-GDPR

Ο αλγόριθμος που δημιουργήθηκε βασίζεται στην συνάρτηση AVERAGE και υπολογίζει το μέσο όρο.

Έτσι για τον πίνακα «Current Maturity Score» η συνάρτηση είναι η «=AVERAGE(H14:H16)». Υπολογίζει το μέσο όρο από τις περιοχές Η14 έως Η16 που σε αυτή την περίπτωση είναι ολόκληρη η επιχειρηματική λειτουργία «Διακυβέρνηση - Governance», που περιλαμβάνει και τις 3 πρακτικές ασφάλειας, που είναι η Στρατηγική & μετρήσεις (Strategy & Metrics), η Πολιτική και συμμόρφωση (Policy & Compliance) και η Εκπαίδευση & Καθοδήγηση (Education & Guidance).

Άρα 1,13+0,90+1,05 = 3,08. Και εν συνεχεία αποτυπώνει τον μέσο όρο στον πίνακα Current GDPR-SAMM Maturity, στην στήλη Κ. Και ο οποίος προκύπτει 1,03 καθώς είναι το αποτέλεσμα της διαίρεσης του 3,08 δια των τριών πρακτικών ασφάλειας.

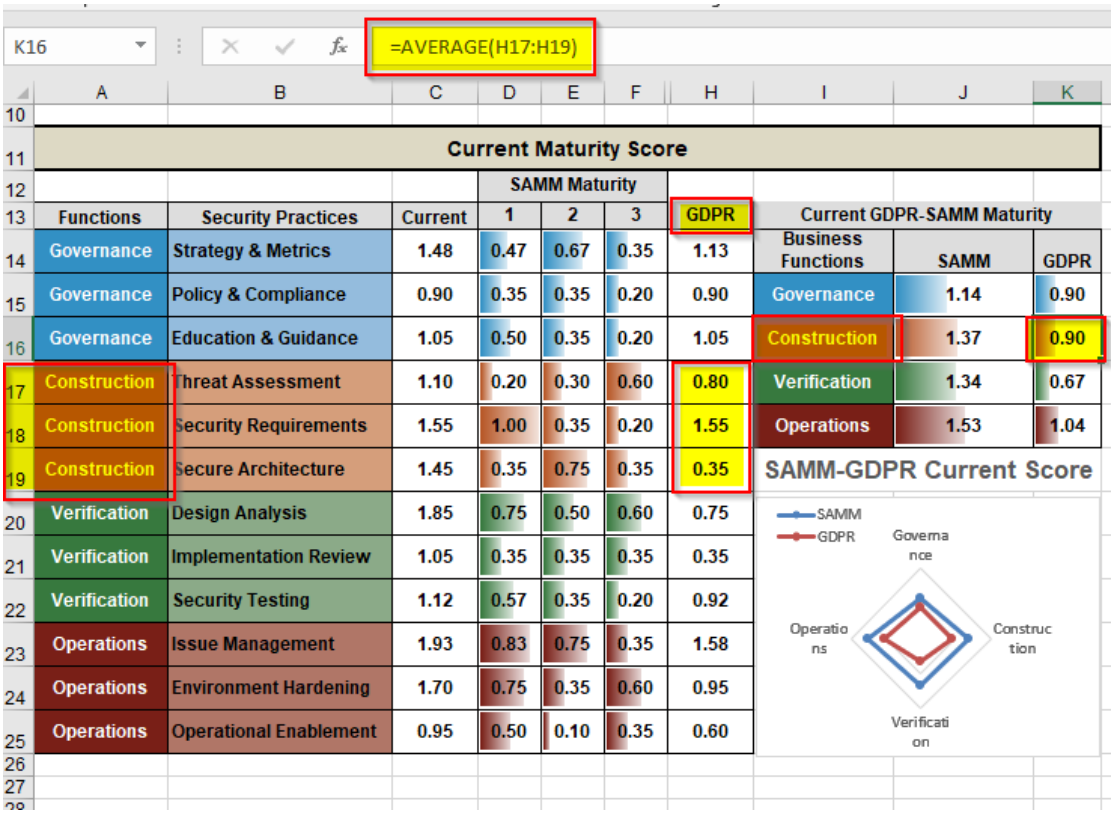
Η πραγματοποιηθείσα προσθήκη φαίνεται παρακάτω στην εικόνα 26 (Φύλλο «SAMM-GDPR Scorecard», συνάρτηση AVERAGE για Διακυβέρνηση).



Εικόνα 26. Φύλλο «SAMM-GDPR Scorecard», συνάρτηση AVERAGE για Διακυβέρνηση.

Ανάλογοι αλγόριθμοι βασισμένοι στον τύπο συνάρτησης Average έχουν δημιουργηθεί και για τις υπόλοιπες 3 επιχειρηματικές λειτουργίες με το εργαλείο να υπολογίζει τους αντίστοιχους μέσους όρους ωριμότητας ανά επιχειρηματικές λειτουργίες όπως φαίνεται και στην εικόνα 27 που παρουσιάζει την συνάρτηση SUMIF για την 3η επιχειρηματική λειτουργία «Κατασκευή – Construction».

Αυτό έχει πραγματοποιηθεί και για τον πίνακα Current Maturity Score και Phase 4 Maturity Score που είναι μέσα στο φύλλο «SAMM-GDPR Scorecard».



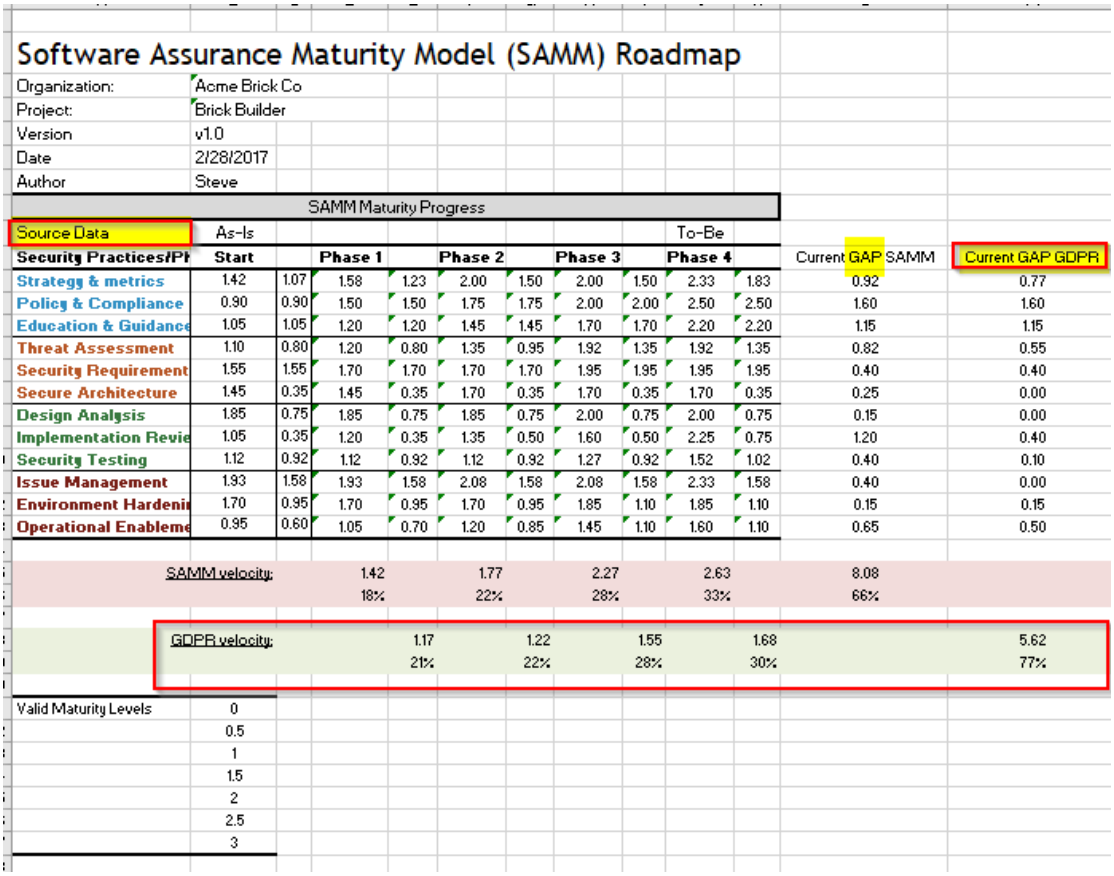
Εικόνα 27. Φύλλο «SAMM-GDPR Scorecard», συνάρτηση AVERAGE για Κατασκευή.

4.4 **Φύλλο «SAMM-GDPR Roadmap chart»**

Φύλλο «SAMM-GDPR Roadmap chart»

a. Προσθήκη στηλών στον πίνακα «Source Data» με τα δεδομένα που αφορούν το GDPR
b. Αντικατάσταση του διαγράμματος με τις φάσεις (πιο ευανάγνωστο) και overlay 2 διαγραμμάτων (SAMM και GDPR)

Στο φύλλο «SAMM-GDPR Roadmap chart» προστέθηκαν στήλες οι όποιες υποστηρίζουν τα δεδομένα που αφορούν το GDPR. Έτσι για αυτό το λόγο έγινε προσθήκη στηλών στον πίνακα «Source Data» που αποτυπώνει τα δεδομένα που αφορούν το GDPR και που φαίνεται στην εικόνα 28 παρακάτω.



Software Assurance Maturity Model (SAMM) Roadmap

Organization:	Acme Brick Co
Project:	Brick Builder
Version	v1.0
Date	2/28/2017
Author	Steve

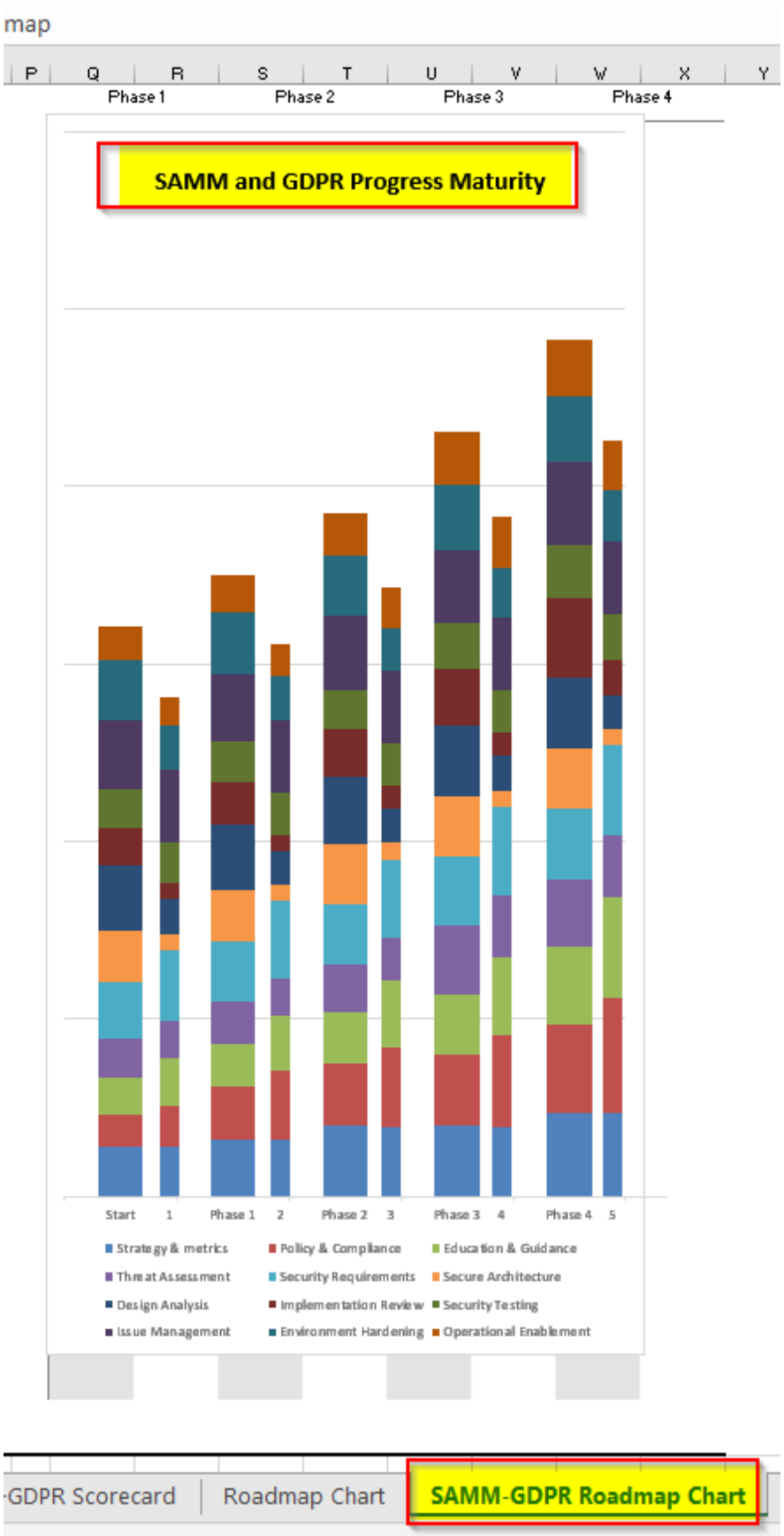
SAMM Maturity Progress

Source Data	As-Is								To-Be			
Security Practices/Ph	Start		Phase 1		Phase 2		Phase 3		Phase 4		Current GAP SAMM	Current GAP GDPR
Strategy & metrics	1.42	1.07	1.58	1.23	2.00	1.50	2.00	1.50	2.33	1.83	0.92	0.77
Policy & Compliance	0.90	0.90	1.50	1.50	1.75	1.75	2.00	2.00	2.50	2.50	1.60	1.60
Education & Guidance	1.05	1.05	1.20	1.20	1.45	1.45	1.70	1.70	2.20	2.20	1.15	1.15
Threat Assessment	1.10	0.80	1.20	0.80	1.35	0.95	1.92	1.35	1.92	1.35	0.82	0.55
Security Requirement	1.55	1.55	1.70	1.70	1.70	1.70	1.95	1.95	1.95	1.95	0.40	0.40
Secure Architecture	1.45	0.35	1.45	0.35	1.70	0.35	1.70	0.35	1.70	0.35	0.25	0.00
Design Analysis	1.85	0.75	1.85	0.75	1.85	0.75	2.00	0.75	2.00	0.75	0.15	0.00
Implementation Revie	1.05	0.35	1.20	0.35	1.35	0.50	1.60	0.50	2.25	0.75	1.20	0.40
Security Testing	1.12	0.92	1.12	0.92	1.12	0.92	1.27	0.92	1.52	1.02	0.40	0.10
Issue Management	1.93	1.58	1.93	1.58	2.08	1.58	2.08	1.58	2.33	1.58	0.40	0.00
Environment Hardeni	1.70	0.95	1.70	0.95	1.70	0.95	1.85	1.10	1.85	1.10	0.15	0.15
Operational Enableme	0.95	0.60	1.05	0.70	1.20	0.85	1.45	1.10	1.60	1.10	0.65	0.50
SAMM velocity:			1.42		1.77		2.27		2.63		8.08	
			18%		22%		28%		33%		66%	
GDPR velocity:				1.17		1.22		1.55		1.68		5.62
				21%		22%		28%		30%		77%

Valid Maturity Levels
0
0.5
1
1.5
2
2.5
3

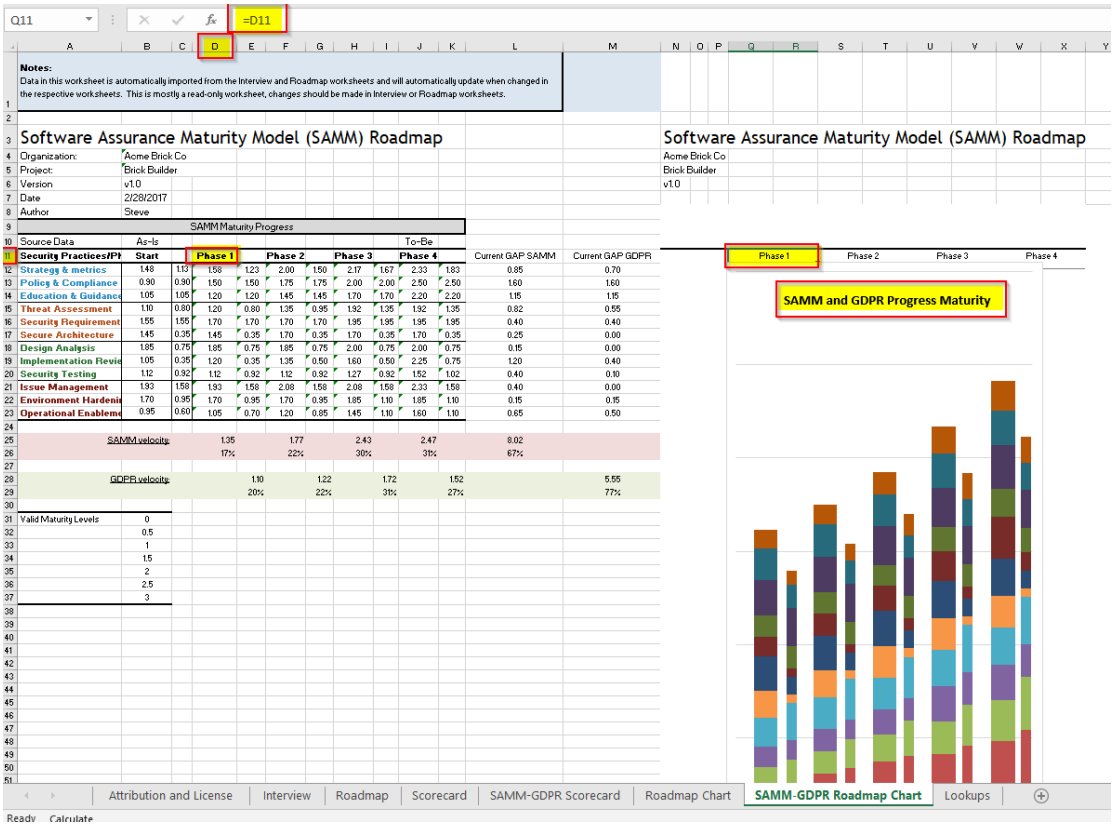
Εικόνα 28. Φύλλο «SAMM-GDPR Roadmap Chart», Source Data.

Ακόμα για να αποτυπωθεί σωστά σε γράφημα πραγματοποιήθηκε αντικατάσταση του αρχικού διαγράμματος με τις φάσεις, για να είναι πιο ευανάγνωστο, και δημιουργήσαμε overlay 2 διαγραμμάτων (SAMM και GDPR) με την χρήση stick bar charts όπως φαίνεται και στην παρακάτω εικόνα, εικόνα 29.



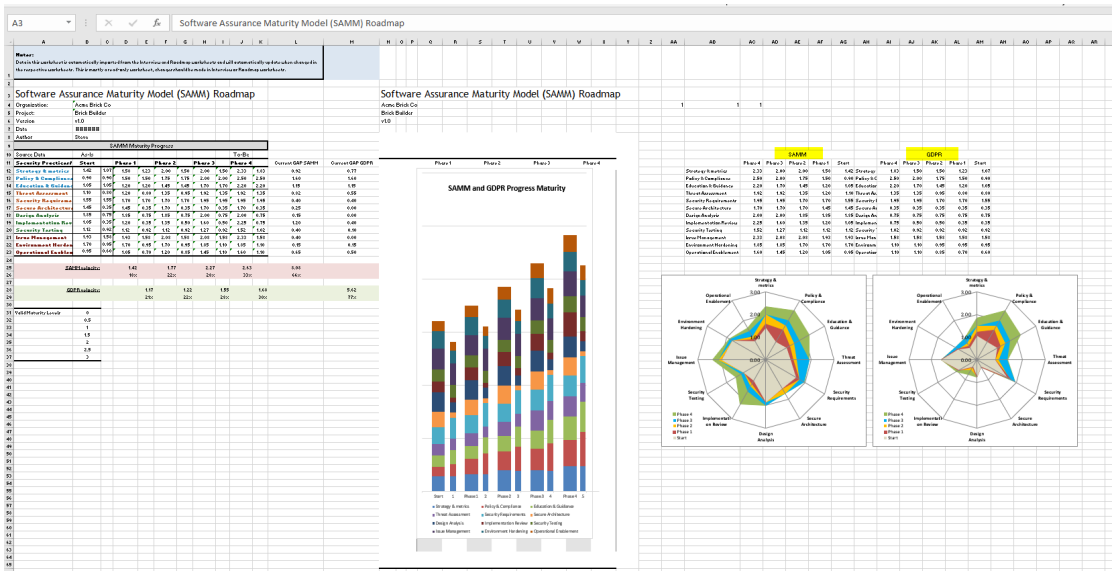
Εικόνα 29. Φύλλο «SAMM-GDPR Roadmap Chart», Διάγραμμα.

Τα δεδομένα που διαβάζει το διάγραμμα τα αντλεί από το ίδιο φύλλο, από τον πίνακα «SAMM Maturity Progress». Στην παρακάτω εικόνα, εικόνα 30 βλέπουμε πως δουλεύει το διάγραμμα, ενδεικτικά για την φάση ωριμότητας 1 (Phase 1).



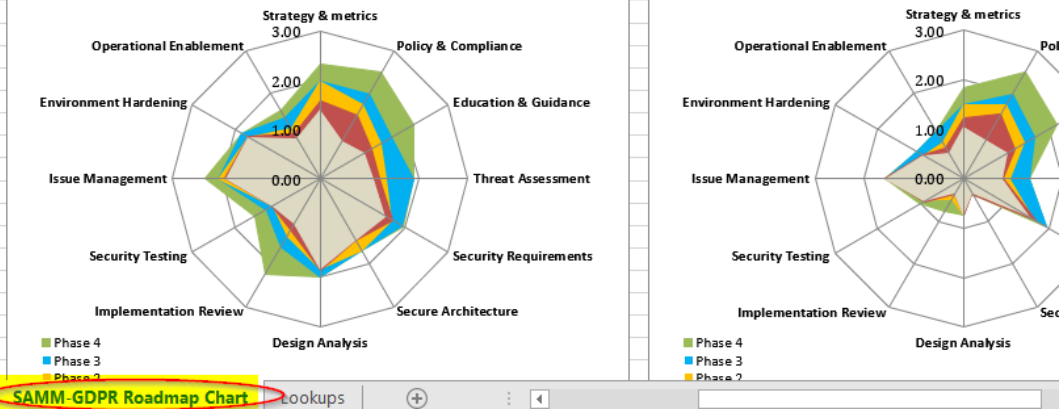
Εικόνα 30. Φύλλο «SAMM-GDPR Roadmap Chart», highlight phase 1.

Τέλος, στο φύλλο «SAMM-GDPR Roadmap Chart», στην πάνω δεξιά πλευρά του φύλλου, υπάρχει ένας συγκεντρωτικός πίνακας που αποτυπώνει όλες τις φάσεις, όπως την τρέχουσα αλλά και τις υπόλοιπες τρεις φάσεις ωριμότητας, δηλαδή το που είναι ο οργανισμός και το που θέλει να φτάσει. Η αξία εδώ έγκειται ότι βάσει των αλλαγών και των προσθηκών που κάναμε στο εργαλείο, αποτυπώνεται η κάθε φάση ξεχωριστά, για καθεμιά από τις 12 πρακτικές ασφάλειας, τόσο για το SAMM όσο και για το GDPR και αυτό μπορούμε να το δούμε αποτυπωμένο στις παρακάτω εικόνες 31 και 32.



Εικόνα 31. Φύλλο «SAMM-GDPR Roadmap Chart», Συγκεντρωτικός Πίνακας για SAMM και GDPR.

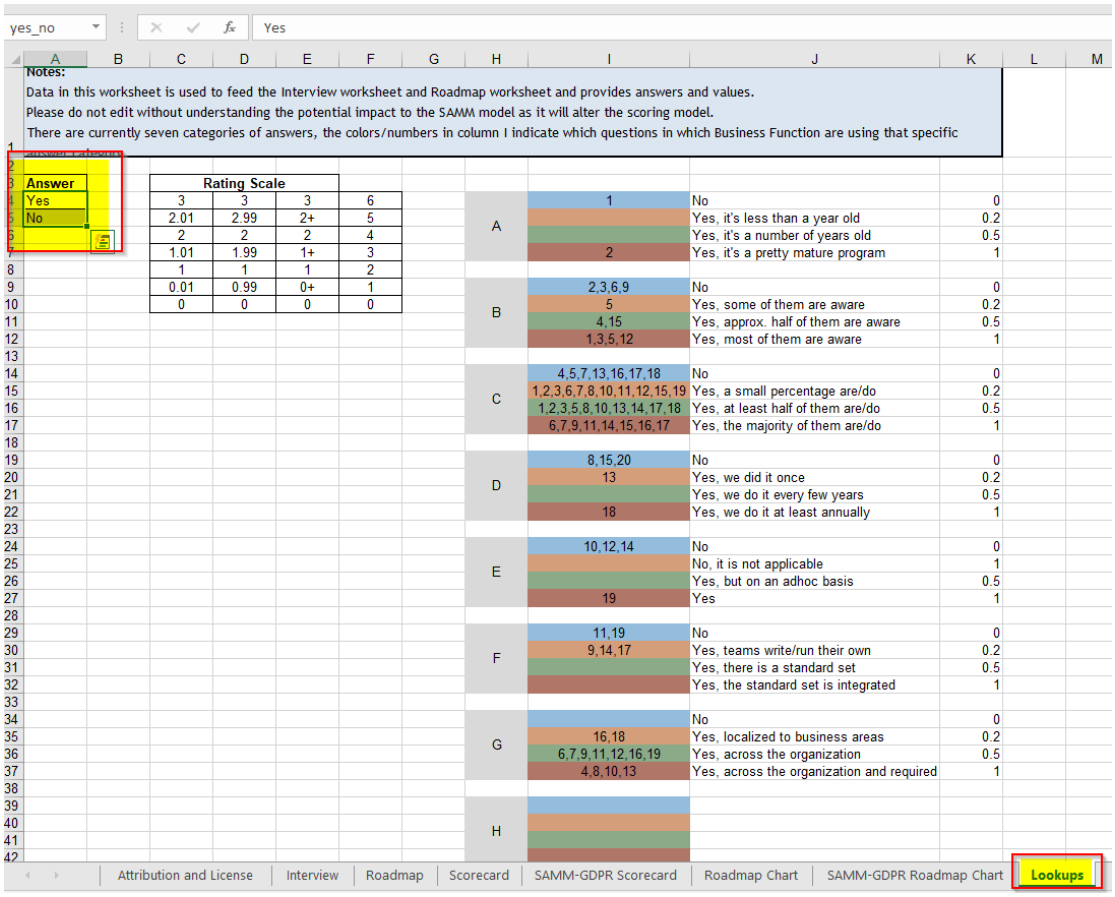
	SAMM					GDPR				
	Phase 4	Phase 3	Phase 2	Phase 1	Start	Phase 4	Phase 3	Phase 2	Phase 1	Start
Strategy & metrics	2.33	2.00	2.00	1.58	1.42	1.83	1.50	1.50	1.23	1.07
Policy & Compliance	2.50	2.00	1.75	1.50	0.90	2.50	2.00	1.75	1.50	0.90
Education & Guidance	2.20	1.70	1.45	1.20	1.05	2.20	1.70	1.45	1.20	1.05
Threat Assessment	1.92	1.92	1.35	1.20	1.10	1.35	1.35	0.95	0.80	0.80
Security Requirements	1.95	1.95	1.70	1.70	1.55	1.95	1.95	1.70	1.70	1.55
Secure Architecture	1.70	1.70	1.70	1.45	1.45	0.35	0.35	0.35	0.35	0.35
Design Analysis	2.00	2.00	1.85	1.85	1.85	0.75	0.75	0.75	0.75	0.75
Implementation Review	2.25	1.60	1.35	1.20	1.05	0.75	0.50	0.50	0.35	0.35
Security Testing	1.52	1.27	1.12	1.12	1.12	1.02	0.92	0.92	0.92	0.92
Issue Management	2.33	2.08	2.08	1.93	1.93	1.58	1.58	1.58	1.58	1.58
Environment Hardening	1.85	1.85	1.70	1.70	1.70	1.10	1.10	0.95	0.95	0.95
Operational Enablement	1.60	1.45	1.20	1.05	0.95	1.10	1.10	0.85	0.70	0.60



Εικόνα 32. Φύλλο «SAMM-GDPR Roadmap Chart», Συγκεντρωτικός Πίνακας για SAMM και GDPR #2.

4.5 **Φύλλο «Lookups»**

Το φύλλο «Lookups» ήταν κρυφό μέσα στο εργαλείο και το εμφανίσαμε. Η προσθήκη που έγινε ήταν η δημιουργία λίστας «Yes_No» στις περιοχές $A$4:$A$5, όπως φαίνεται και στην εικόνα 33.



Εικόνα 33. Φύλλο «Lookup», δημιουργία λίστας.

Κεφάλαιο 5

5 Αποτελέσματα

Τα αποτελέσματα του εργαλείου αποτυπώνονται στον παρακάτω συγκεντρωτικό πίνακα, πίνακας 5 – Συγκεντρωτικός πίνακας συσχέτισης SAMM Domains και άρθρων του κανονισμού GDPR.

SAMM Domains		GDPR Articles Related
SM	Strategy & Metrics	Yes
PC	Policy & Compliance	Yes
EG	Education & Guidance	Yes
TA	Threat Assessment	Yes
SR	Security Requirements	Yes
SA	Secure Architecture	Yes
DR	Design Review	Yes
IR	Implementation Review	Yes
ST	Security Testing	Yes
IM	Issue Management	Yes
EH	Environment Hardening	No
OE	Operational Enablement	No

Πίνακας 5. Συγκεντρωτικός πίνακας συσχέτισης SAMM Domains και άρθρων του κανονισμού GDPR.

Κεφάλαιο 6

6 Ανάλυση Αποτελεσμάτων

Ο σχεδιασμός και η ανάπτυξη του εμπλουτισμού του εργαλείου με γνώμονα να καλύπτει τον νέο Γενικό Κανονισμό των Προσωπικών Δεδομένων, οδηγεί σε ένα ικανοποιητικό αποτέλεσμα, με αποτέλεσμα ο χρήστης να αποκομίζει την ολιστική εικόνα σε σχέση με την συμμόρφωση που έχει ο οργανισμός του στο GDPR, και ο οποίος κανονισμός είναι ενσωματωμένος μέσα στις τυπικές δραστηριότητες ενός κύκλου SAMM.

Χάρη στο εργαλείο αποτυπώνονται γρήγορα τις οι όποιες αποκλίσεις μεταξύ των επιχειρηματικών φάσεων και δίνεται η δυνατότητα στον χρήστη να προβαίνει σε ενδεχόμενες διορθωτικές κινήσεις για την επίτευξη μεγαλύτερης ωριμότητας και κατ’ επέκταση συμμόρφωσης του GDPR μέσα στον κύκλο SAMM.

Επίσης βάση της επεξεργασίας που κάναμε για να μπορέσουμε να απαντήσουμε τις ερωτήσεις στις 12 πρακτικές ασφάλειας (SAMM Domains) και στα επιμέρους SAMM Maturity Levels για το αν τα πεδία αυτά έχουν συσχέτιση με το GDPR ή όχι, δημιουργήσαμε τον παρακάτω πίνακα σε excel.

Λόγω του ότι δεν ήταν δυνατόν να χωρέσει ευκρινέστατα λόγω του μεγέθους του, προβήκαμε σε στιγμιότυπο οθόνης και το εισαγάγαμε σαν εικόνα, εικόνα .

	A	B	C	D	E
1	SAMM Domains		SAMM Maturity Levels		GDPR Articles Related
2					
3	SM	Strategy & Metrics	SM1	Establish Unified strategic roadmap for software security within organization	Yes
4			SM2	Measure relative value of data and assets and choose risk tolerance	Yes
5			SM3	Align Security Expenditure with relevant Business indicators and asset value	No
6	PC	Policy & Compliance	PC1	Understand relevant governance & compliance drivers	Yes
7			PC2	Establish Security & Compliance Baseline + understand project risks	Yes
8			PC3	Require Compliance and measure projects against organization wide standards	Yes
9	EG	Education& Guidance	EG1	Offer Development staff access to resources around the topics of secure development	Yes
10			EG2	Educate all personnel in the software lifecycle with role specific guidance on secure development	Yes
11			EG3	Mandate extensive security training and certify personnel for baseline knowledge	Yes
12	TA	Threat Assessment	TA1	Identify and understand high-level threats to the organization and individual projects	Yes
13			TA2	Increase accuracy of threat assessment and improve granularity of per project understanding	No
14			TA3	Completely tie compensating controls to each threat against internal and third-party software	Yes
15	SR	Security Requirement	SR1	Consider security explicitly during the software requirements process	Yes
16			SR2	Increase granulairty of security requirements based on business logic and known risks	Yes
17			SR3	mandate security requirements process for all software projects and 3rd-parties interdependencies	Yes
18	SA	Secure Architecture	SA1	Insert consideration of proactive security guidance into the software design process	Yes
19			SA2	Drect the software design process towards know secure services and secure-by default designs	No
20			SA3	Formally control the software design process and validate utilization of secure components	No
21	DR	Design Review	DR1	Support adhoc reviews of software design to ensure baseline mitigations for known risks	Yes
22			DR2	Offer assessment services to review software design against comprehensive best practices for security	No
23			DR3	Require assessments and validate artifacts to develop detailed understandingof protection mechanisms	No
24	IR	Implementation Review	IR1	opportunistically find basic code-level vulnerabilities and other high-risk security issues	Yes
25			IR2	Make code review during development more accurate and efficient through automation	No
26			IR3	Mandate comprehensive code review process to discover language-level and application-specific risks	No
27	ST	Security Testing	ST1	Establish process to perform basic security tests based on implementation and software requirements	Yes
28			ST2	Make security testing during development more complete and efficient through automation	Yes
29			ST3	Require application specific security testing to ensure baseline security before deployment	No
30	IM	Issue Management	IM1	Understand high-level plan for responding to vulnerability reports or incidents	Yes
31			IM2	Elaborate expectations for response process to improve consistency and communications	Yes
32			IM3	Improve analysis and data gathering within response process for feedback into proactive planning	No
33	EH	Environment Hardening	EH1	Understand baseline operationel environment for applications and software components	No
34			EH2	Improve confidence in application operations by hardening the operating environment	Yes
35			EH3	Validate application health and status of operational environment against known best practices	Yes
36	OE	Operational Enablement	OE1	Enable communications between development teams and operators for critical security-relevant data	Yes
37			OE2	Improve expectations for continuous secure operations through provision of detailed procedures	Yes
38			OE3	Mandate communication of security information and validate artifacts for completeness	No

Εικόνα 34. Συγκεντρωτικός πίνακας συσχέτισης SAMM domains, Maturity Levels and GDPR.

Κεφάλαιο 7

7 Συμπεράσματα

Αναφορικά με την αξιολόγηση της συμμόρφωσης με τις απαιτήσεις του GDPR, η προστασία των προσωπικών δεδομένων αποτελεί ένα από τα σημαντικότερα ζητήματα κατά την ανάπτυξη νέων εφαρμογών. Η μεθοδολογία του μοντέλου SAMM (Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού - Software Assurance Maturity Model του οργανισμού OWASP μπορεί να:

- Αξιολογήσει τις υπάρχουσες πρακτικές ασφάλειας ανάπτυξης ασφαλούς λογισμικού.
- Αναπτύξει ένα σταθερό πρόγραμμα ανάπτυξης ασφαλούς λογισμικού.
- Επιδείξει με αξιόπιστο και μετρήσιμο τρόπο την εξέλιξη και τη βελτίωση του επιπέδου ασφάλειας λογισμικού.
- Ορίσει δραστηριότητες και πρακτικές που σχετίζονται με την ασφάλεια λογισμικού και να μετρήσει την αποδοτικότητά τους, τόσο για την ίδια τη λειτουργία της εφαρμογής όσο και για το σύνολο της εταιρείας ή του οργανισμού που αξιοποιεί το λογισμικό.

Η προτεινόμενη μεθοδολογία συνεπάγεται και μια σειρά από πλεονεκτήματα για τον οργανισμό, το έργο ή το προϊόν λογισμικού που θα επιχειρήσει να ενσωματώσει τον κανονισμό GDPR σε ένα κύκλο SDLC όπως το SAMM. Αυτά περιλαμβάνουν:

- Τη μείωση της προσπάθειας για τη διαχείριση επιπλέον κανονιστικών απαιτήσεων όπως το GDPR. Οι εργασίες που εφαρμόζονται για το SAMM χρησιμοποιούνται και για την κάλυψη των απαιτήσεων του GPDR.
- Την αύξηση της παραγόμενης αξίας από τη χρήση του toolkit του SAMM. Το εργαλείο του SAMM θα αποτελέσει εργαλείο και για την καταγραφή της κάλυψης των απαιτήσεων του GPDR.

- Την αύξηση του ρυθμού παραγόμενης αξίας από τη χρήση του SAMM. Το ποσοστό κάλυψης των απαιτήσεων του GPDR θα είναι πλέον μετρήσιμο και καταγεγραμμένο από το πρώτα στάδια ανάπτυξης λογισμικού σύμφωνα με το SAMM.
- Την υιοθέτηση της αρχής «Ιδιωτικότητας από το Σχεδιασμό» (Privacy by Design – PbD). Το SAMM, άρα και οι αρχές τις Ιδιωτικότητας που απαιτεί το GPDR, εφαρμόζεται σε όλες τις φάσεις ανάπτυξης του λογισμικού (Σχεδιασμός – Υλοποίηση – Δοκιμές – Παραγωγή).

Επιπλέον των παραπάνω, και για την πληρότητα της αξιολόγησης της προτεινόμενης μεθοδολογίας, θα πρέπει να σημειωθεί ότι η χρήση της συγκεκριμένης μεθοδολογίας ενδέχεται να εμφανίσει και κάποιες αδυναμίες.

Αυτές περιλαμβάνουν:

- Την αύξηση του χρόνου προετοιμασίας ενός έργου ανάπτυξης λογισμικού – κυρίως ως προς την ανάλυσή του.
- Την αύξηση του πλήθους των εμπλεκόμενων μερών στην εφαρμογή του SAMM. Εφόσον το SAMM toolkit αποτελέσει εργαλείο και για την συμμόρφωση με το GDPR, θα πρέπει να εμπλακεί στην εφαρμογή και την παρακολούθησή του και ο ρόλος του Data Protection Officer (DPO), απαίτηση που μπορεί να είναι αυξημένης δυσκολίας για κάποιους οργανισμούς.
- Την αύξηση των γνώσεων που θα πρέπει να φέρει η ομάδα για την εξυπηρέτηση και των αναγκών του GDPR. Η συγκεκριμένη απαίτηση μπορεί να εξισορροπηθεί με την εμπλοκή του Data Protection Officer (DPO).
- Η μεθοδολογία δεν αφορά το σύνολο των άρθρων του GDPR αλλά εστιάζει σε εκείνα που σχετίζονται με την ανάπτυξη λογισμικού. Εντούτοις αποτελεί μια γρηγορότερη μέθοδο αξιολόγησης διότι βασίζεται σε ήδη υπάρχουσα πρακτική.

7.1 **Μελλοντικές Επεκτάσεις**

Η παρούσα εργασία παρουσίασε την αξιοποίηση και επέκταση ενός τυποποιημένου εργαλείου αποτύπωσης του επιπέδου ωριμότητας μιας εφαρμογής ή ενός οργανισμού σε σχέση με το Μοντέλο Ωρίμανσης Εξασφάλισης Λογισμικού SAMM, ώστε να συμπεριλάβει, να ποσοτικοποιήσει και να αποτυπώσει ταυτόχρονα και το επίπεδο συμμόρφωσης με το GDPR.

Το συγκεκριμένο εργαλείο «SAMM Assessment Toolkit v1.5» βοηθά στην αποτύπωση της τρέχουσας ωριμότητας ενός οργανισμού σε σχέση με το επίπεδο συμμόρφωσης SDLC του αλλά και την παραγωγή ενός οδικού χάρτη (roadmap) για τη σταδιακή αύξησή του.

Το υπόψη εργαλείο έχει σχεδιαστεί με τρόπο, ούτως ώστε να επιδέχεται επεκτάσεις και προσθήκες και έχουν προβλεφθεί διάφορα επιμέρους στοιχεία και δεδομένα τα οποία δεν αναλύθηκαν λόγω περιορισμένου χρόνου.

Λαμβάνοντας υπόψιν ότι από τον οργανισμό OWASP έχει δημιουργηθεί μια ενημερωμένη έκδοση του SAMM, η SAMM v2.0, η οποία βρίσκεται ακόμα σε δοκιμαστικό στάδιο, το υπόψη εργαλείο θα μπορεί να προσαρμοστεί ευέλικτα και να χρησιμοποιηθεί με την ενημερωμένη έκδοση.

Παράλληλα, άλλη μία μελλοντική επέκταση, λαμβάνοντας υπόψη και την πολυπλοκότητα άλλων πρακτικών, μοντέλων και προτύπων, είναι η επέκταση του εργαλείου και σε άλλες πρακτικές, πρότυπα και κανονιστικές διατάξεις (π.χ. PCI-DSS).

Επίσης, καθώς οι κύκλοι ζωής ανάπτυξης λογισμικού διαφέρουν ανά μοντέλο SDLC, θα μπορούσε να παραμετροποιηθεί το εργαλείο για την αλλαγή του αριθμού των φάσεων ωριμότητας.

Τέλος, μια μελλοντική επέκταση και εξέλιξη είναι η πρόσθεση ειδικού βάρους ανά ερώτημα του μοντέλου SAMM, ως προς τη σημαντικότητα με το GDPR που θα έχει και αντίκτυπο στα αποτελέσματα που επιστρέφονται στο χρήστη μέσω της

διεπαφής του βάσει των απαντημένων ερωτήσεων και αυτό θα αποτυπώνεται ειδικότερα στο κομμάτι της βαθμολογίας (scoring).

Βιβλιογραφία

[1] N. S. a. P. Souras, «Economic Models and Approaches in Information,» *International Journal of Network Securit,* τόμ. 2, αρ. 1, p. 14–20, 2006.

[2] N. S. A. N. Bikos, «Architecture Design of an Area Efficient High Speed Crypto Processor for 4G LTE,» *IEEE Transactions on Dependable and Secure Computing,* τόμ. 15, αρ. 5, pp. 729-741, 2018.

[3] A. K. D. N. S. S. Zeadally, «Cryptographic Technologies and Protocol Standards for Internet of Things,» *Elsevier Science Press,* αρ. Internet of Things: Engineering Cyber Physical Human Systems, 2019.

[4] H. Li, L. Yu και W. He, «The Impact of GDPR on Global Technology Development,» *Journal of Global Information Technology Management,* τόμ. 22, αρ. 1, pp. 1-6, 2019.

[5] C. Gauthier , «The impact of the EU general data protection regulation on scientific research,» Université Paul Sabatier, Toulouse, 2017.

[6] O. Thomas και D. Christian , «Software Assurance Using Structured Assurance Case Models,» σε *Engineering and Managing Software Requirements*, Berlin, Springer, 2005, pp. 163-185.

[7] Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, «Access to European Union law,» 27 Απριλίου 2016. [Ηλεκτρονικό]. Available: http://eur-lex.europa.eu. [Πρόσβαση Ιούνιος 2017].

[8] «ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) 2016/679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ,» 2016.

[9] B. Curtis, M. C. Paulk, M. B. Chrissis και C. Weber, «Capability maturity model, version 1.1,» *IEEE Software,* τόμ. 10, αρ. 4, pp. 18-27, 1993.

[10] M. I. Daud, «Secure Software Development Model: A Guide for Secure Software Life Cycle,» σε *International MultiConference of Engineers and Computer Scienists*, Hong Kong, 2010.

[11] OWASP, «SAMM Project,» OWASP, 10 May 2019. [Ηλεκτρονικό]. Available: https://www.owasp.org/index.php/OWASP_SAMM_Project.

[12] D. Geer, «Are Companies Actually Using Secure Development Life Cycles?,» *Computer,* τόμ. 43, αρ. 6, pp. 12-16, 2010.

[13] R. Abhinav και J. Russell, «Secure Coding: Building Security into the Software Development Life Cycle,» *Information Systems Security,* τόμ. 13, αρ. 5, pp. 29-39, 2006.

[14] P. H. Meland και J. Jensen, «Secure Software Design in Practice,» σε *Third International Conference on Availability, Reliability and Security*, Barcelona, 2008.

[15] V. Paul και A. Bussche, The EU General Data Protection Regulation (GDPR), Springer, 2017.

[16] ΑΠΔΠΧ, «http://www.dpa.gr,» [Ηλεκτρονικό]. Available: http://www.dpa.gr/portal/page?_pageid=33,18990&_dad=portal&_schema=PORTAL. [Πρόσβαση Ιούλιος 2017].

[17] D. Sebastien, «Adding Privacy by Design in Secure Application Development,» OWASP.

[18] M. Mina, F. H. Foomany και M. Nathanael, «Complying With GDPR: An Agile Case Study,» *ISACA Journal,* τόμ. 2, 2018.

[19] M. Brecht και T. Nowey, «A Closer Look at Information Security Costs,» University of Regensburg, Germany.

[20] C. Watson, «OWASP SAMM Project,» [Ηλεκτρονικό]. Available: https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads.

[21] OWASP, «OWASP SAMM,» [Ηλεκτρονικό]. Available: https://owaspsamm.org/v1-5/downloads/.

[22] TOREON, "https://www.toreon.com/," [Online]. Available: https://www.toreon.com/application-security/embedding-gdpr-in-the-secure-development-lifecycle-sdlc/. [Accessed May 2019].