Agility of Security Practices and Agile Process Models: An Evaluation of Cost for Incorporating Security in Agile Process Models

H. Maria Maqsood and Andrea Bondavalli
Department of Mathematics and Informatics, University of Florence, Morgagni, Florence, Italy

Keywords: Software and Systems Development Methodologies, Software Process Improvement, Empirical Software Engineering, Agile Methodologies, Agility, Process Models, XP, Scrum, Agile Process Models.

Abstract: Agile process models are widely used today for software development. There has been an immense increase in use of agile methodologies due to their major focus on delivering working software and accommodating changes in requirements. However, use of agile methodologies for developing secure systems still poses many challenges. This research, addresses the issue of observing the effect on agility of process models while security practices are applied in them. An approach is proposed which calculates level of agility of six agile process models (XP, Scrum, FDD, ASD, DSDM, and Crystal) and security practices against four fundamental parameters of agility. When security practices are applied to process models they lower the degree of agility. We propose a method to see this effect based on factor of agility and also that the degree of agility of process model can be adjusted at desired level by including or excluding security practices.

1 INTRODUCTION

Agile focuses on rapid development and follows the rule of delivering working software in short intervals.

One of the major advancement in the field of software is that from past decade developers and all stakeholders consider security as a proper issue (McGraw, Allen, Barnum, & Ellison, 2008). The current concern is we do not have very compact solutions to address the problem.

This paper is structured into five major sections. Section 1 gives introduction, section 2 gives brief overview of related work to understand the problem in hand, section 3 describes the methodology to calculate agility of process models and lists details of a research survey that we have performed to calculate the agility of security practices in process models. Section 4 gives the formula to calculate the agility of models after the application of selected security practices.Section 5 concludes the work done and Section 6 describes future work directions.

2 RELATED WORK

According to Jacobson (Jacobson, 2002), an agile team is very responsive to changes since adapting to change is what agile software development is all about. It is very important for an agile team to understand that software is developed by teamwork, and collaboration is the heart of success (Boström, Gustav, & et al., 2006).

Software engineers gathered forces and began to classify agile processes in early 2001 (K.Beck, 2001). Agile Alliance stated the agile manifesto as (K.Beck, 2001)

“Individuals and interactions over processes and tools, Working software over comprehensive documentation, Customer collaboration over contract negotiation; Responding to change over following a plan”

Security is an afterthought during software development, it is addressed either very late in development or even after it (Kravchenko, Elena, & E. W., 2017).

Now the question arises what will we call a secure product? According to Microsoft (Howard & Lipner, 2006), a secure product is the one that can handle the integrity, confidentiality and customer

Maqsood, H. and Bondavalli, A.
Agility of Security Practices and Agile Process Models: An Evaluation of Cost for Incorporating Security in Agile Process Models.
DOI: 10.5220/0009356403310338
In *Proceedings of the 15th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2020)*, pages 331-338
ISBN: 978-989-758-421-3

information along with the confidentiality of processing resources under administrator.

Many experts give advice on using agile methodologies for the development of secure systems (Moyon, Beckers, & Kleppe, 2018) as there are reported benefits of using agile for software development; however, security cycles are in contrast to agile approaches with the consequence of compromising the level of agility when incorporating security practices (Alnatheer, Ahmed, Gravell, Andrew and Argles, & David, 2010). There is no concrete method to monitor how agility will be affected. Security in its very own nature as a non-functional requirement is not easy to cater to. Still, it is the experience in this area that counts the most (K., S., & V., August, 2017) (Ashraf, S., & Aftab, & S., 2017).

3 METHODOLOGY

We provide a method to assess (numerically) agility of process models and security practices. There are two major contributions of this work, first is related to the degree of agility for six process models and second is about the degree of agility of twelve security practices in Scrum and XP. The agility of security practices varies from one process model to another; hence, there are dedicated tables to show values of security practices for both of our chosen process models.

The agility of a security activity or a process model refers to how an activity/process model behaves against basic parameters given by agile manifesto. The capacity of a security activity/process model to be flexible, lean, responsive and speedy defines how agile it is. If it possesses higher values of these attributes, it has a high degree of agility and vice versa. We have further assessed the agility of process models after including selected security practices by using a formula. The variation in the degree of agility of a process model before and after application of security practices shows how much agility is compromised to incorporate security.

The four parameters of agility that we have used in our work are defined by agile manifesto (K.Beck, 2001) as

- Flexibility

Ability to adapt to expected or unexpected changes at any time.

- Leanness

It refers to the improvement of products and services based on the feedback of customers in terms of what they value.

- Responsiveness

Responsiveness refers to appropriate reaction against expected or unexpected changes.

- Speed

Speed refers to rapid and iterative development for small releases.

It is important to understand that they are not ranked in any Order. A process must have all of these attributes to be called an agile process.

3.1 Agility of Process Models

We have evaluated the agility of six agile process models against four basic parameters of agility based on the work of (Qumer, A., Henderson-Sellers, & B., 2008). They proposed an approach to calculate the agility of process models in terms of their phases and practices however, We have taken both practices and phases into account and computed a single value that represents the degree of agility of certain model. Following are six process models that we have considered.

- XP(Extreme Programming),
- Scrum,
- ASD(Adaptive Software Development),
- DSDM(Dynamic System Development Method),
- FDD(Feature driven development) and
- Crystal.

However, we have used XP and Scrum only for further evaluations, since we were not able to have significant amount of responses for rest of the process models through our survey.

Extreme programming (XP) is an agile process model, which intends to improve responsiveness and software quality and cater to flexible requirements (Beck & Kent, 2004).There are four basic phases of XP

- Planning,
- Designing,
- Coding and
- Testing.

Scrum (Ken Schwaber & Beedle, 2002) has major focus on courage, respect, openness and commitment. Scrum has the following basic activities

- Product backlog,
- Building teams,
- Scheduled meetings,
- Sprint and
- Sprint review.

The calculation of agility of process models is based on the work of Qumer B.Henderson (Qumer, A., Henderson-Sellers, & B., 2008). They derived a formula to present the agility of each process model's phases and practices within the range 0 to 1 where 1 represents that the process model is highly agile. In this paper, we have calculated the agility of a process model as whole, including practices and phases.

We will use following equation to perform calculations,

Degree of agility of process model = Sum of agile factors / (no. of practices of process model * no. of agile attributes) (1)

For example, let us consider the process model XP.

Sum of agile factors in XP [flexibility + speed + leanness + responsiveness] = [15+13+6+15] =49
Number of practices + phases in XP = 18
Number of agile attributes = 4
By applying the formula (1) we get
*49÷ (18*4)=0.68*

Table 1: Process Models.

Agile Attributes / Process Models	Flexibility	Leanness	Speed	Responsiveness	Sum of agile factors	No. of practice + phases in a process model	Total Agility of process model
XP	15	6	13	15	49	18	0.68
Scrum	9	0	10	9	28	10	0.7
ASD	10	0	12	10	32	12	0.66
FDD	10	0	10	10	30	13	0.57
Crystal	9	0	11	11	32	11	0.70
DSDM	10	0	11	11	32	15	0.53

It is evident that some process models have higher agility as compared to others. As given in Table 1 Crystal and Scrum have highest degrees of agility and DSDM has lowest, which refers to the fact that Crystal and Scrum are more agile, and DSDM is least agile in this set of process models.

However, our focal point is not comparison between process models; our focus is to see how agility of any one-process model is affected after including security practices.

3.2 Agility of Security Activities in Process Models

We have considered the degree of agility of few of the most widely used security activities against four agile parameters (as we did for process models). This approach is based on the work of (Hossein keramati & Mirian-Hosseinabadi, 2008). The values of security attributes are based on survey from industry personnel. There was a need to perform this survey because as per our knowledge there is no numerical data available for such reasoning. We could only find theoretical reasoning through literature, hence we conducted a survey to provide grounds for empirical analysis.

3.2.1 Research Survey

We performed a questionnaire-based survey to observe the agility of 12 most common security practices against four agile parameters in six process models. The research survey serves as descriptive survey and it provides a descriptive analysis. As Oppenheim, (Oppenheim, 2000) describes a descriptive survey provides descriptive analysis only, which refers to frequencies and cross tabulation. According to Oppenheim, (Oppenheim, 2000) descriptive surveys are not meant to describe causal relationship of variables instead their focus is on describing what proportions of sample represent certain opinion or what is the frequency of occurrence of certain events/values.

While selecting the organizations for responses we used purposive sampling. Nardi (Nardi, 2014) describes this method as collecting samples from respondents based on some specific trait, which is important for the study. In this research survey, we have involved organizations that have experience of working with agile AND are using security techniques in agile methods.

The research was designed to get responses of individuals', project managers or developers working with agile methodologies. One person can give response for more than one process model according to his experience in relevant model/models. All responses were collected through a web-based survey using Google forms. (Alreck, P.L., Settle, & R.B, 1995) Mentions three major methods for collecting data when performing questionnaire-based survey. First is Personal interviewing second is mail data collection and third is telephone interviewing. However, now days there is very popular method of conducting web based survey. There are many reasons for selecting web-based surveys. All the data you get through them is already in electronic form so it is easy and fast to access the data. In addition, it prevents the chances of errors during manual entries of data as Nardi (Nardi, 2014) suggests. This method is speedy and cost effective too when compared to mail based surveys. It also proves to have higher response rate, which is one of the major issues with other methods of surveys.

3.2.2 Design of Research Survey

We conducted a survey through questionnaire by using 5 point Likert scale (Likert, 1932) method. The responses were collected through web-based questionnaire. Sample is given in Appendix A. We asked industry experts to rank the security activities against four parameters of agility on the scale of (Alreck, P.L., Settle, & R.B, 1995) (Rea, L.M., & R.A., 1997)

5= Strongly Agree,
4=Agree,
3=Neutral,
2=Disagree and
1=Strongly Disagree.

Each expert has chosen the process model of his or her expertise and ranked security attributes for that particular process model (Jon A. Krosnick & Presser, 2010).

For example, an expert of XP ranks the security practice “attack identification” as 5 (strongly agree) against agile attribute “flexibility”, this represents that expert strongly agrees that attack identification is highly flexible in XP. OR in other case, if he assigns 1 (strongly disagree) this refers to not flexible at all in this case. Flexibility and other three agile parameters are defined in accordance to agile manifesto (described in detail in section 3). Figure 1 represents sample sources.

In our questionnaire, first two questions were dichotomous questions that represent an exclusive disjunction. Our first question, “I have experience of agile process models for more than 5 years”. Question 2 states, “I have more than 3 and less than 5 years of experience with agile process models and security practices”. The detail of responses is shown in Figure 2. In total, we received 56 responses.We received 18 responses for Scrum out of which 10 had experience with agile and security for less than 3 years, 6 had more than 5 years of experience in agile whereas 2 had more than 3 years of agile experience with security practices.

For XP we got 20 responses, 10 of them have worked with security practices in agile for less than 3 years, 8 had greater than 5 years of agile experience and 2 had more than 3 years of agile experience. For Feature Driven Development we encountered five responses, three of them had experience with security attributes and agile for less than 3 years whereas 1 had agile experience of more than 5 years and last respondent has experience of more than 3 years. For Adaptive Software Development we received 6 responses 3 of which have worked with security and agile processes for less than 3 years and 2 of them had experience of more than 5 years in agile development whereas 1 had experience of more than 3 years with agile and security practices. For DSDM (Dynamic System Development Method) we had 5 respondents, 3 of them had experience with agile process models and security attributes for less than 3 years, 1 had more than five years of agile experience and last one had more than three years of agile and security experience solely. For Crystal process model we received two responses 1 had experience with agile and security attributes for more than 3 years and 1 had experience with agile for less than 3 years.

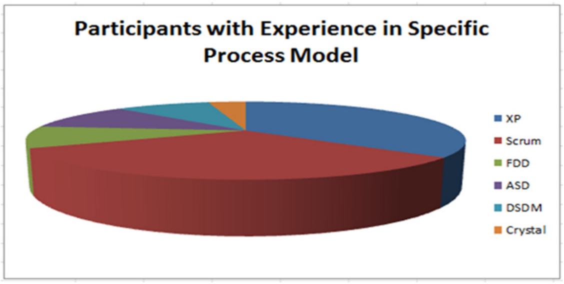

Figure 1: Participants with Experience in Specific Process Model.

Further evidence is required for process models, to deduce more reliable conclusions about their agility. However, in this paper we provide the application of our methodology on two process models namely Scrum and XP, since we have better number of responses against these models as compared to rest of the four process models. Furtherwork is required to verify and validate the results of process models with lower number of responses.

3.2.3 Results

The tables in this section represent the final values of security practices against agile parameters for Scrum and XP based on the expert’s opinions taken through a survey. We have processed the data of the survey by using a formula given in (2). First we have assigned weights to the responses.

Weightage 3 is assigned to category A which has people with more than five years of experience, weightage 2 is assigned to category B which has people with more than 3 and less than 5 years of experience and finally category C has weightage 1 for responses from people with less than 3 years of experience.

The value of each agile attribute against each security practice is calculated by using the following formula,

$$\begin{array}{c}= (\text{sum of values by category A*3}) + (\text{sum} \\ \text{of values by category B*2}) + (\text{sum of values} \\ \text{by category C*1}) \div (\text{Total no. of responses of} \\ \text{category A*3}) + (\text{Total no. of responses of} \\ \text{category B*2}) + (\text{Total no. of responses of} \\ \text{category C*1})\end{array} \qquad (2)$$

For example, let us consider the process model Scrum. For calculating *flexibility* of Attack Identification (security practice), we have (data by experts through survey).

Responses in Category A = 6

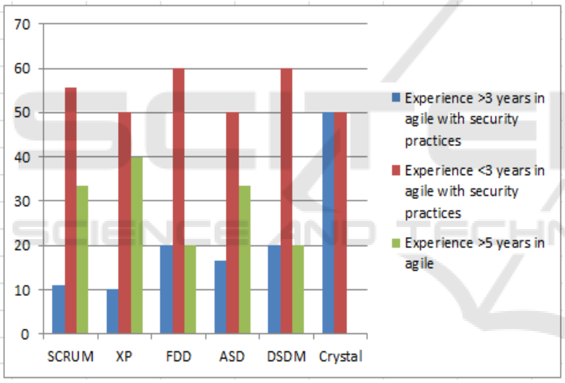

Figure 2: Detail in Terms of Percentage of Recorded Responses.

Responses in Category B = 2

Responses in Category C = 10

Sum of values (for 'flexibility' of 'attack identification') marked by experts in Category A=21

Sum of values marked by experts in Category B=9

Sum of values given by experts in Category C=36

By applying (2) we get,

*=(21 * 3) + (9 * 2) + (36 * 1) ÷ ((6 * 3) + (2 * 2) + (10 * 1))*

Flexibility of Attack Identification in Scrum is = 3.6 (Table 2)

(Since we want to find agility of each security practice)

Number of agile attributes = 4

Total agility of *Attack Identification* is sum of flexibility, speed, leanness, responsiveness.

= [3.6+3.5+3.2+3.7] = 14

Number of practices considered = 1

(Since we want to find agility of each security practice) Number of agile attributes = 4

Table 2: Agility of Security Practices in Scrum.

Agile Attributes Security Practices	Flexibility	Speed	Leanness	Responsiveness	Total Agility of a Security practice
Attack Identification	3.6	3.5	3.2	3.7	0.87
Threat Modelling	3.9	3.5	3.2	3.6	0.88
Security Requirement Analysis	3.8	3.1	3.1	3.3	0.83
Security Education and Awareness	3.4	2.9	2.8	3.0	0.75
Build Security Team	3.6	3.3	3.4	3.4	0.85
Resource Identification	3.6	3.4	3.5	3.2	0.85
Roles Identification	3.9	3.3	3.7	3.4	0.89
Review Design Security	3.7	3.3	3.0	3.8	0.86
Static Code Analysis	3.8	3.1	3.3	3.5	0.85
Penetration Testing	3.7	3.2	3.4	3.5	0.86
Incident Response Planning	3.5	3.5	2.7	3.6	0.81

Table 3: Agility of Security Practices in XP.

Agile Attributes Security Practices	Flexibility	Speed	Leanness	Responsiveness	Total Agility of a Security practice
Attack Identification	3.8	3.8	3.4	3.7	0.91
Threat Modelling	3.8	3.3	3.0	3.3	0.8
Security Requirement Analysis	3.6	3.1	2.8	3.6	0.81
Security Education and Awareness	3.4	3.0	2.6	3.2	0.76
Build Security Team	3.3	2.7	3.0	3.2	0.77
Resource Identification	3.5	3.2	2.9	3.1	0.79
Roles Identification	3.5	3.1	3.4	3.2	0.82
Review Design Security	3.7	3.1	2.8	3.6	0.85
Static Code Analysis	3.8	2.9	3	3.4	0.8
Penetration Testing	3.6	3.0	3.0	3.2	0.85
Incident Response Planning	3.4	3.5	2.7	3.3	0.80

By applying (1) we get, [14÷(1 x 4)]

Total agility of *Attack Identification* =3.5

Since we need to see the effect of this value on agility of any process model, we must have it between the ranges 0-1.

Hence, Total agility of *Attack Identification* =3.5÷4=0.87

There are different practices and phases in each model and so the agility of security activities differs for each model. For example, Build Security Team Roles has value of 0.85 in Scrum whereas in XP it is 0.77. This is explained by the fact that Scrum has an inherent process of building teams in terms of making Scrum teams thus making the activity more flexible, speedy, lean and responsive whereas, XP has no such inherent process. However, further study is required to understand the changing behaviour of security practices in different process models.

4 APPLYING SELECTED SECURITY PRACTICES TO PROCESS MODELS

The main purpose of calculating agility of process models and security practices is to see how security practices will affect the agility of process models. Here we will perform the calculations and analysis.

Few abbreviations will be used

AOM → *Actual Agility of Model (Calculated previously as Degree of Agility of Process Model) (Range 0-1).*

ART→ *Agility Reduction Tolerance (Calculated Previously as Degree of Agility of Security practices).*
(Range 0-1)

AAAS →*Agility after Applying Security practices (Calculated in this section). (Range 0 – AOM)*

Note we call agility of security practice, as "Agility Reduction Tolerance" because this value represents the cost a process model will bear for including a security practice. Hence, ART (Agility Reduction tolerance) is the factor responsible for reducing agility of process models.

4.1 Formula

$$\text{AAS}=[((\text{ART activity}_1 + \text{ART activity}_{2......}+\text{ART activity}_n) \div n) \text{ x AOM}] \qquad (3)$$

In this formula, we sum up the agility of selected security activities and divide it by total number of selected activities then multiply the obtained value by agility of selected process model. This would give us new agility of process model after taking out the cost of including security practices. Further explanation and application of this formula is provided with examples.

It is evident that some process models have higher agility as compared to others. As given in Table 1. Further we have applied the approach to Scrum and XP, keeping in view that their data is more unswerving with greater number of responses as compared to other process models.

4.1.1 Scrum

Let us see the effect of including following security practices in Scrum. Let us take the values for ARTof these activities from (Since we want to find agility of each security practice) Number of agile attributes = 4.

By applying (1) we get, [14÷(1 x 4)]

Total agility of Attack Identification =3.5. Since we need to see the effect of this value on agility of any process model, we must have it between the ranges 0-1.
Hence, Total agility of Attack Identification =3.5÷4=0.87 (Table 2)

ART of Attacks Identifications =0.87
ART of Review design security =0.86
ART of Static code analysis=0.85
Here,
n=3
AOM (Actual Agility of Model Table 1*) = 0.7*
By putting the values in (3) we get,
Agility After Application of Security (AAAS)
= [((0.87+0.86+0.85) ÷3) × 0.7]
AAAS=0.62

Here, the new agility of Scrum is 0.62 whereas. It is obvious that we will bear cost of including security in Scrum; this work provides an empirical way to see that cost. This can serve as one major factor, (there can be other factors like time (Ayalew, Kidane, & Carlsson, 2013)) for selection of security practices.

4.1.2 XP

Let us see the effect of including same security practices (Attacks Identifications, Review design security and Static code analysis) in XP. Let us take the values for ART of these activities from (Table 3)

ART of Attacks Identifications =0.91

ART of Review design security =0.85
ART of Static code analysis=0.8
Here,
n=3
AOM (Actual Agility of Model Table 1 *) = 0.68*
By putting the values in (3) we get,
Agility After Application of Security AAAS

$$= [((0.91+0.85+0.8) \div 3) \times 0.68]$$

AAAS=0.58

In this case the AAAS of XP becomes 0.58 which is lower than its original value (0.68). The effect of including selected security activities in XP is visible in terms of reduced degree of agility. This represents the cost that one has to bear in terms of agility for including security practices.

5 CONCLUSIONS

The effect of including selected security activities can be seen in both process models. This leads to two conclusions. Firstly you are firm to use certain security practices, let us say as your prime factor in this case you can perform the calculations to see the effect of your decision on agility of different process models. Secondly, you are firm to use certain process model and you are ready to adjust security practices keeping the degree of agility of process model as prime factor. Both of above-mentioned approaches can be handled by proposed method.

6 FUTURE WORK

This research can serve as one major parameter for selection of security practices. However, further study is required to learn about different values of same security activities in different process models. Second area of further work on this topic is to investigate other dimensions (for example time and monetary factors) that can help in selection of security activities. We will be looking into these dimensions along with Agility Reduction Tolerance of security activities in future in perspective of agile process models.

REFERENCES

Alnatheer, Ahmed, Gravell, Andrew and Argles, & David. (2010). Agile Secuirty Issues. *International Symposium on Empirical Software Engineeringl and Measurement.* Italy: ACM/IEEE.

Alreck, P.L., Settle, & R.B. (1995). *The survey research handbook:guidelines and strategies for conducting a survey.* IRWIN Professional Publishing.

Ashraf, S., & Aftab, & S. (2017). IScrum: An improved scrum process model. *Ashraf, S., & Aftab, S. (2017). IScrum: A International Journal of Modern Education and Computer Science (IJMECS)*, Ashraf, S., & Aftab, S. (2017). IScrum: An improved scrum process model. 9(8), 16-24.

Ayalew, T., Kidane, T., & Carlsson, B. (2013). Identification and Evaluation of Security Activities In Agile Projects. *Springer-Verlag Berlin Heidelberg* (pp. 139-153). Springer.

Beck, & Kent. (2004). *Extreme Programming Explained, Embrace Change.* Addison-Wesley.

Boström, Gustav, & et al. (2006). Extending XP practices to support security requirements engineering. *International workshop on Software engineering for secure systems.* ACM.

Hossein keramati, & Mirian-Hosseinabadi, S.-H. (2008). Integrating Software development Security Activities with Agile Methodologies. *International Conference on Computer Systems and Applications.* Doha, Qatar: IEEE.

Howard, M., & L. S. (2006). *The Security Development Lifecycle - SDL: A Process for Developing Demonstrably More Secure Software.* Microsoft Press.

Jacobson. (2002). A resounding 'Yes' to agile processes - But also more. *Cutter IT Journal, 15.*

Jon A. Krosnick, & Presser, S. (2010). Handbook of Survey Research. Emerald Group Publishing Limited.

K., R., S., H., & V., L. (August, 2017). Busting a myth: Review of agile security engineering methods. *In Proceedings of the 12th International Conference on Availability, Reliability and Security.*, 1-10.

K.Beck, M. A. (2001). *The Agile Manifesto.* Retrieved from www.agie.alliance.org.

Ken Schwaber, & Beedle, M. (2002). *Agile Software Development with Scrum* (Vol. 1). Upper Saddle River: Prentice Hall.

Kravchenko, Elena, & E. W. (2017). *Integrating Security in Agile projects.* Belfast: OWASP.

L. R. (1932). A Technique for the Measurement of Attitudes. *Archives of Psychology*, *Vol. 22, No. 140*, pp. 1-55.

McGraw, G., Allen, J. H., Barnum, S., & Ellison, R. J. (2008). *Why Is Security a Software Issue?, Software Security Engineering: A Guide for Project Managers.* The Addison-Wesley Software Security Series.

Moyon, F., Beckers, K., & Kleppe, S. (2018). Towards Continuous Security Compliance in Agile Software Development at Scale. *International Workshop on Rapid Continuous Software Engineering.* Gothenburg, Sweden: ACM/IEEE.

Nardi, P. M. (2014). *Doing survey research : a guide to quantitative methods.* London: Paradigm Publishers.

Oppenheim, A. N. (2000). Questionnaire design, interviewing and attitude measurement. Bloomsbury Publishing.

Qumer, A., Henderson-Sellers, & B. (2008). An Evaluation of the Degree of Agility in Six Agile Methods and its Applicability for Method Engineering. *Information and Software Technology, 50*(4), 280-295.

Rea, L.M., & R.A., P. (1997). *Designing and conducting survey research: a comprehensive guide* (2nd ed.). Jossey-Bass, Inc.

APPENDIX

Matrix Marked by Experts for Each Process Model

Agile Attributes Security Practices	Flexibility	Speed	Leanness	Responsiveness
Attacks identification	[1,2,3,4,5]	[1,2,3,4,5]	[1,2,3,4,5]	[1,2,3,4,5]
Threat Modelling				
Security requirement Analysis				
Security Education and Awareness				
Build Security Team				
Resource Identification				
Roles Identification				
Review Design Security				
Static Code Analysis				
Penetration Testing				
Incident Response Planning				