Managing Cyber-Risk: Contracts, Litigation, Acquisitions & Procurement

Riccardo C. Storti
Chief Engineer, Delta Group Engineering, Melbourne, Australia

Sunday, March 14, 2021

Abstract

An analysis of twenty (20) Commercial-Off-The-Shelf (COTS) Technologies was executed in order to investigate how they may be applied to minimise the Cyber-Threats associated with ‘undefined requirements’ pertaining to Contracts, Litigation, Acquisitions & Procurement (CLAP). However, our analysis concludes that only one (1) COTS Technology is capable of achieving this objective (Testimation Technology); as demonstrated utilising four (4) Simplified Examples. One (1) Simplified Example pertaining to Contracts, demonstrates Cyber-Threat minimisation by precisely & unambiguously specifying the minimum level of Cyber-Confidence to be delivered & the maximum level of Cyber-Risk to be tolerated. Three (3) Simplified Examples pertaining to Litigation, Acquisitions & Procurement respectively, demonstrate Cyber-Threat minimisation by the application of a Decision Assistance Table (DAT) generated by this COTS Technology. All four (4) Simplified Examples presented, demonstrate how it is possible to Manage Cyber-Risk utilising a scientifically formulated tool which has been experimentally verified to Predict & Measure all forms of Cyber-Risk to greater than 98.07% accuracy.

Key Words: Acquisitions, Contract Specification, Cyber-Confidence, Cyber-Risk, Decision Facilitation, Estimation, Litigation, Operations, Procurement, Quality Assurance, Risk Analysis, Software Testing

1 Delta Group Engineering; rstorti@gmail.com; ORCID-ID: 0000-0002-0152-3888
1 Introduction

1.1 Defining The Problem

To date, no institution *(globally)* possesses the capability to be aware of their Risk Exposure with respect to Undiscovered Defects *(i.e. their Cyber-Risk)* within Information Technology (IT) Systems. Undiscovered Defects can be a platform for exploitation as parties, of various motivation, seek to gain financial advantage for potential mischief; *e.g.* the North Korean government, terrorist groups, organized crime. However, beyond malicious intent exist more perilous Cyber-Threats; ‘undefined requirements’. Commonly, Business Sponsors expect Software Developers to ‘somehow know’ what these ‘undefined requirements’ are or should be. Conversely, the Software Development Team (SDT) responsible for building The Solution, expects that every requirement has already been captured and authorised such that all other aspects are deemed Out-of-Scope. From the perspective of the SDT, no ‘undefined requirements’ exist at the end of the Requirements Gathering Phase (RGP).

Irrespective of best intentions, it is neither practical nor feasible to capture all possible requirements unambiguously for an exact ‘meeting of the minds’ in any commercial IT engagement via narratives & documentation; *e.g.* a contract. People & corporations apply best endeavours to avoid ‘undefined requirements’, but it remains virtually impossible to completely close the gap. To circumvent this impasse, humanity has developed various statistical techniques to precisely quantify a necessary outcome; *e.g.* vaccine efficacy. By defining a necessary outcome with statistical precision, two *(or more)* parties may commercially engage whilst unanimously agreeing upon deliverables, but without the delivery path being relevant to all stakeholders. Because the delivery path becomes irrelevant to some of the parties involved *(e.g.* often the Business Sponsor), many of the consequences associated with ‘undefined requirements’ vanish; the net effect being to simplify the engagement.

One of the most significant requirements often remaining undefined is ‘the level of Cyber-Confidence to be delivered’; *i.e.* the level of Defect-free Confidence to be delivered. Alternatively, this may be described as ‘the maximum permissible level of Cyber-Risk’; *i.e.* the maximum level of Undiscovered Defects to be tolerated. Consequently, three *(3)* key commercial issues exist which require resolution & may be stated as follows:

1. How can we utilise statistical techniques to minimise the Cyber-Threats associated with ‘undefined requirements’?  
2. How can we utilise statistical techniques to define the required level of Cyber-Confidence to be delivered?  
3. How can we utilise statistical techniques to manage Cyber-Risk?  

Fortunately, these issues have already been resolved by Commercial-Off-The-Shelf (COTS) Technology built to Predict, Measure, Manage & Mitigate all forms of Cyber-Risk:  

- [https://testimation.com/](https://testimation.com/)

1.2 Shaping The Solution

In this article, we utilise Commercial-Off-The-Shelf (COTS) Technology to demonstrate how it may be applied to minimise the Cyber-Threats associated with ‘undefined
requirements’ pertaining to Contracts, Litigation, Acquisitions & Procurement (CLAP). Cyber-Threat minimisation is achieved by precisely & unambiguously specifying the minimum level of Cyber-Confidence to be delivered & the maximum level of Cyber-Risk to be tolerated. Although this COTS Technology was built for the purpose of Software Quality Assurance (QA), we provide Simplified Examples of how it may be applied as a key delivery & decision making tool with respect to CLAP.

1.3 COTS Technology

The Commercial-Off-The-Shelf (COTS) Technology utilised in this article was developed to Predict, Measure, Manage & Mitigate Cyber-Risk. It achieves this by determining the number of Test Cases required to Quality Assure (QA) Software & expresses the result in terms of a Probability Distribution denoting Cyber-Confidence. This COTS Technology has been experimentally validated to greater than 98.07% accuracy, & all experimental results are available for peer review [1], [2]. We apply this COTS Technology to generate a Decision Assistance Table (DAT) as shown in Tab. (1), & utilise the results in Simplified Examples; the Economically Optimal Solution (EOS) of 99% is emphasised by cell shading:

| Cyber-Confidence | Cyber-Risk | Test Cases | Cost ($) | Description of Tc’s |
|------------------|------------|------------|----------|---------------------|
| 80.22%           | 19.78%     | Tc’s       | $        | C                   |
| 93.15%           | 6.85%      | 2·Tc’s     | 2-$      | C + H               |
| 97.43%           | 2.57%      | 3·Tc’s     | 3-$      | C + H + M           |
| 99%              | 1%         | 4·Tc’s     | 4-$      | C + H + M + L       |
| 99.6%            | 0.4%       | 5·Tc’s     | 5-$      | C + H + M + L + 25%·SO |
| 99.84%           | 0.16%      | 6·Tc’s     | 6-$      | C + H + M + L + 50%·SO |
| 99.93%           | 0.07%      | 7·Tc’s     | 7-$      | C + H + M + L + 75%·SO |
| 99.97%           | 0.03%      | 8·Tc’s     | 8-$      | C + H + M + L + 100%·SO |

Tab. (1): Decision Assistance Table (DAT)

Where:
1. C = Critical Priority Test Cases
2. H = High Priority Test Cases
3. M = Moderate Priority Test Cases
4. L = Low Priority Test Cases
5. SO = Super-Optimal Test Cases

Nomenclature:
6. Cyber-Confidence = Defect-Free Confidence:
   • The Probability that an Application or Information Technology (IT) System is void of Defects
7. Cyber-Risk = The Testing Not Executed = Undiscovered Defects:
   • The Probability that an Application or IT-System contains Dormant Defects which have not yet been discovered
   • Cyber-Risk = 1 – Cyber-Confidence
8. Test Case:
   • A train of Function Points (FPT’s) or User Input Commands (UIC’s) following a Functional Process (FP) defined by the Business Sponsor:
     • UIC’s are also known as User Steps (US’s) or Test Steps (TS’s)

❖ Applied Definitions: refer to The Appendix for more information
2 Simplified Examples

An effective means by which to communicate the decision making power of the solution presented herein is to investigate four (4) Simplified Examples, as follows;

1. Contracts
2. Litigation
3. Acquisitions
4. Procurement

2.1 Contracts

Dilemma:
- The Martian Department of Defence (MDoD) is seeking to improve the functional reliability of the Software controlling its Combat Drones (CD’s) by introducing a strict Contractual Requirement (CR) for all 3rd party vendors. The CR is to be enforced by a Quality Assurance (QA) Specification generated by Commercial-Off-The-Shelf (COTS) Technology.

Contractual Requirement:
- 3rd party software development contractors shall deliver Military Combat System’s (MCS’s) to a functional reliability standard of no less than 99.97% Defect-Free Confidence; hence, the Probability of Undiscovered Defects (i.e. the Cyber-Risk) should not exceed 0.03%

Business Requirement:
- Ten (10) Functional Processes (FP’s) relating to the operation of Combat Drones (CD’s) are required to be validated to 99.97% Cyber-Confidence

Investigation:
- Measurements:
  - The average number of User Input Commands (UIC’s) per FP is five (5)

Resolution:
- QA Specification:
  - Critical Priority Test Cases = 67; see Fig. (1)
    - Refer to The Appendix for more information: Point 8
  - Positive Test Cases = 33.5 = 33 (rounded value)
  - Negative Test Cases = 33.5 = 33 (rounded value)
  - Contractual Requirement Test Cases = 531; see Fig. (2)
  - The Ratio of Contractual Requirement Test Cases to Critical Priority Test Cases [as shown in Tab. (1)] is given by:
    - 531 / 67 = 7.93:1 ≈ 8:1
  - The Ratio of Negative Test Cases to Positive Test Cases is given by:
    - Refer to The Appendix for more information: Point 7
    - (531 – 33) / 33 ≈ 15:1
2.2 **Litigation**

The following fictitious Dilemma is derived from real events:

- [https://thenewdaily.com.au/finance/finance-news/2017/08/07/cba-blames-software-glitch/](https://thenewdaily.com.au/finance/finance-news/2017/08/07/cba-blames-software-glitch/)

**Dilemma:**

- The National Bank of Mars (NBoM) is facing penalties of $1T (AUD) due to Software Defects associated with their Automatic Teller Machines (ATM’s). These Defects resulted in criminal organisations depositing funds & laundering money in defiance of Legislation & Regulated Banking Practices
Investigation:

- The NBoM utilises Commercial-Off-The-Shelf (COTS) Technology to conduct a Software Quality Audit (SQA) on the 3rd party software controlling their ATM’s. The SQA measures that the vendor deployed their solution into production with a Defect-Free Confidence (i.e. Cyber-Confidence) of only 90%, without informing the NBoM of the residual 10% Cyber-Risk

- By comparing the results of the SQA to Tab. (1), the NBoM concludes that the 3rd party vendor executed all Critical Priority Test Cases & approximately 62% of High Priority Test Cases. This meant that 38% of High Priority Test Cases & all Moderate & Low Priority Test Cases remained unexecuted

- NBoM analysis of Tab. (1) also reveals that the level of Quality Assurance (QA) deployed by the 3rd party vendor was Sub-Optimal [i.e. below 99% Cyber-Confidence]; possibly in an attempt to reduce project costs by prematurely terminating Testing

- The NBoM determined that the Defect exploited by the criminal organisation had been categorised as a Low Priority Test Case by the 3rd party vendor

- The NBoM concludes that if the 3rd party vendor had of tested to the Economically Optimal Solution (EOS) of 99% Cyber-Confidence, the Low Priority Test Case responsible for the exploited Defect would have been detected & corrected prior to deployment

Resolution:

- Since ATM’s are independent 3rd party ElectroMechanical devices, the NBoM could not have participated in the Software-Development-Life-Cycle (SDLC) or the Software-Testing-Life-Cycle (STLC) of the deployed product. Consequently, the NBoM could not have contributed to the Test Case prioritisation process which may have prevented the Defect from being exploited by criminal organisations via the ATM User Interface (UI)

- If the Low Priority Test Case at the centre of the scandal had of been categorised as a Critical Priority Test Case by the 3rd party vendor, then it is conceivable that the Defect would not have been exploited & the criminal organisation could not have laundered money

- The NBoM argues in court that the 3rd party vendor should absorb 10% of the penalty costs due to an oversight in their Test Case prioritisation process:
  - The court awards $100B (AUD) to the NBoM

2.3 Acquisitions

The following fictitious Dilemma is derived from real events:

- [https://www.abc.net.au/news/2020-09-04/bain-capital-new-owner-of-virgin-australia-creditors-vote-yes/12629528](https://www.abc.net.au/news/2020-09-04/bain-capital-new-owner-of-virgin-australia-creditors-vote-yes/12629528)

Dilemma:

- Martian Capital Investments (MCI) is seeking to acquire Virgin Interplanetary Airlines (VIA) following a downturn in travel due to a pandemic. MCI addresses its Due Diligence obligations by identifying key areas of scrutiny, one being ‘Cyber-Risk & Associated Remediation Costs’. MCI leadership is concerned about acquiring an Information Technology (IT) elephant & seeks to utilise the outcome of the Cyber-Risk investigation in its negotiations with VIA
Investigation:
- MCI utilises Commercial-Off-The-Shelf (COTS) Technology to conduct a Cyber-Risk Assessment (CRA) of VIA IT-Systems. The CRA measures that VIA is commercially trading with a Defect-Free Confidence (i.e. Cyber-Confidence) of only 80.22% & consequential Cyber-Risk of 19.78%; MCI leadership is concerned by the Risk Exposure associated with this result
- MCI analysis of Tab. (1) reveals that the level of Quality Assurance (QA) of existing VIA IT-Systems is Sub-Optimal [i.e. below 99% Cyber-Confidence]
- MCI determines that the cost of Cyber-Confidence Remediation to the Economically Optimal Solution (EOS) of 99% requires a Capital Expenditure (CapEx) investment of $100M (AUD)

Resolution:
- MCI utilises their Cyber-Due-Diligence as leverage in its negotiations with VIA

2.4 Procurement

Dilemma:
- The United States of Mars (USM) is seeking to procure Next Generation Strike-Fighters for their War against the Peoples Republic of Venus (PRV). They have attended prototype demonstrations conducted by two major 3rd party vendors & are considering their tender responses. Given that both vendors are offering similar capabilities, the USM is exploring Points-of-Difference to assist with their final determination of preferred vendor for the $50B (AUD) procurement contract

Investigation:
- The USM utilises Commercial-Off-The-Shelf (COTS) Technology to conduct a Cyber-Risk Assessment (CRA) of the Avionics Software aboard each Prototype Strike-Fighter (PSF). The CRA measures that the PSF associated with the Vendor-1 solution operates at 97.43% Cyber-Confidence, whilst the Vendor-2 solution operates at 99.97% Cyber-Confidence
- USM analysis of Tab. (1) reveals that the Quality Assurance (QA) level of the Vendor-1 solution is Sub-Optimal [i.e. below 99% Cyber-Confidence]. In contrast, it also reveals that the QA level of the Vendor-2 solution is Super-Optimal [i.e. above 99% Cyber-Confidence]
- The USM learns from Vendor-1 that to close the 2.54% Software Reliability gap between themselves & Vendor-2 would require a six (6) month delivery delay

Resolution:
- After careful consideration of many factors including similarities, maintenance & life-cycle requirements, the USM concludes that a decisive Point-of-Difference between vendors exists in relation to Software Reliability
- The USM awards the procurement contract to Vendor-2 based upon Cyber-Confidence
3 Discussion

3.1 Testimation COTS Technology

Risk is a measure of uncertainty & an inherent attribute of many virtual & physical systems. Indeed, even physical mechanisms at the quantum level of reality are governed by Heisenberg's Uncertainty Principle. Hence, the need to understand & accept the existence of Cyber-Risk is fundamental to minimizing the test effort required to Quality Assure complex information systems. It is simply impractical & inappropriate to deny the existence of Risk, as this undermines the physical nature of the Universe. Consequently, the best we can hope to achieve is to manage an agreed level of acceptable Cyber-Risk, & mitigate unacceptable Cyber-Risk by validating Software ‘smarter’ not ‘harder’. Thus, an element of Cyber-Risk Management must be incorporated into any pragmatic solution or tool.

The objective of this article is to utilise Commercial-Off-The-Shelf (COTS) Technology to demonstrate how it may be applied to minimise the Cyber-Threats associated with ‘undefined requirements’ pertaining to Contracts, Litigation, Acquisitions & Procurement (CLAP). Cyber-Threat minimisation is achieved by precisely & unambiguously specifying the minimum level of Cyber-Confidence to be delivered & the maximum level of Cyber-Risk to be tolerated. A key message this article conveys is that specific levels of Quality Assurance (QA) incur specific costs. That is, the greater the required level of Cyber-Confidence in the solution, the greater the associated cost of QA; see Tab. (1). The mathematics underlying the COTS Technology is commonplace in many fields of endeavor & widely understood. At a fundamental level, the scientifically based COTS solution utilised is not new, only its application in Cyber-Space. The creators of the COTS Technology presented herein have gone to great lengths to be transparent [1]. The author supplies verifiable evidence of the COTS creators claims such that [2], [3]:

- Their Test Effort Estimation (TEE) Model Construct has been experimentally verified to Predict & Measure Cyber-Risk to high precision & accuracy [>98.07%]
- They show that TEE quantifies Cyber-Confidence, which in turn quantifies Cyber-Risk. Hence, TEE is a Mission Critical Activity (MCA) when formulating Cyber-Risk Management Strategies & may be utilised prior to project commencement, in-flight or post facto as an assessment &/or auditing tool
- Their TEE Model Construct addresses & solves a number of significant fundamental issues with respect to estimating the test effort required on Software Projects in order to Predict & Measure Cyber-Risk

3.2 Other COTS Technology

As with any research endeavour, a thorough literature survey followed by a rigorous literature review is standard practice. However, at the time of writing this article & in the context of its objective, no useful &/or relevant literature was found or known to exist specifically dealing with the Cyber-Threats associated with ‘undefined requirements’; despite exhaustive searching. One may be inclined to conclude that an ‘undefined requirement’ is a synonym for Scope Creep, in which case an abundance of literature exists. However, this is not helpful in our objective because an ‘undefined requirement’ may or may not lead to Scope Creep. Even if literature is cited drawing a
connection between Scope Creep and ‘undefined requirements’, it never (to the knowledge of the author) explicitly relates Scope Creep to Cyber-Risk expressed as a statistical probability; e.g. Cyber-Risk = 1% probability of Undiscovered Defects:
  • A possible explanation for this being that the commercial nature of our article’s objective acts as a deterrent to publication. Corporations may be reluctant to reveal unfavourable information of a commercial nature, & independent authors may be concerned about infringing Intellectual-Property (IP) Laws by revealing Cyber-Risk information which may potentially lead to litigation.

To circumvent this obstruction, we executed a rigorous Commercial-Off-The-Shelf (COTS) Technology review of existing Cyber-Risk Management products available from the following firms:

1. RiskLens: https://www.risklens.com/
2. Interfacing: https://www.interfacing.com/risk-management-software
3. Tenable:
   • https://www.tenable.com/solutions/risk-based-vulnerability-management
4. MetricStream: https://www.metricstream.com/
5. Sphera: https://sphera.com/
6. Protecht: https://www.protechtgroup.com/
7. DoneSafe: https://www.donesafe.com/quality-management-software-qms/
8. RiskRecon: https://www.riskrecon.com/
9. LogicManager:
   • https://www.logicmanager.com/solution/it-security-risk-management/
10. NavexGlobal: https://www.navexglobal.com/en-us
11. AllGress: https://www.allgress.com/solutions
12. Riskonnect: https://riskonnect.com/
13. AdaptiveGRC: https://adaptivegrc.com/
14. Sword: https://www.sword-grc.com/
15. GBTec: https://www.gbtec.com/solutions/risk-management-software/
16. CammsRisk: https://cammsgroup.com/products/risk/
17. Resolver:
   • https://www.resolver.com/information-security-software/it-risk-management/
18. LogicGate: https://www.logicgate.com/
19. Norton | Symantec Insight: https://au.insight.com/en_AU/home.html

Analysis of the COTS products associated with the firms listed above, yielded three (3) key observations:

1. The logic & methodology associated with the operation of their algorithms is hidden information; i.e. how they actually work to fulfil their claims cannot be independently replicated or validated

2. None of the products are capable of determining the probability of Undiscovered Defects (i.e. Cyber-Risk) within Information Technology (IT) Systems

3. None of the products are capable of quantifiably demonstrating resultant Cyber-Confidence if Business Owners were to precisely follow & act upon the advice generated by them; that is, they do not assert statements (or equivalent) such as:
   • “Following the corrective action advised by our product, your Cyber-Confidence will be 99.97%”
Consequently, no like-for-like comparison is possible between Testimation COTS Technology & the products from the firms listed above. Moreover, no comparable alternative is known to exist.

3.3 Contractual Mechanisms

Thus far, we have demonstrated via Tab. (1) & the use of Simplified Examples, the power & usefulness of Cyber-Risk measurement as a decision making tool. It is often chanted by Continuous Improvement Process (CIP) Engineers that, ‘we cannot improve that which is not measured’. Nor can we easily, precisely, clearly &/or unambiguously define success in the absence of numerical targets. Of course, it is not always possible to numerically define objectives, but where possible, it should be attempted & is always preferred. However, in situations where documented narratives seem to be the only option, a contractual agreement is required. The inherent weakness with narratives is that it is extremely difficult, if not impossible, to precisely & unambiguously articulate all possible clauses required to ensure a ‘meeting of the minds’ resulting in zero potential for disputes or litigation between parties.

To address this, Axelrod et. Al. outline a procedural framework to introduce more stringent Cyber-Security requirements (i.e. Cyber-Confidence requirements) into Software Development Agreements (SDA’s) [4]. In doing so, the client pushes more responsibility back on to Contractors for the Quality & Reliability of the Solution they have been engaged to deliver. Nevertheless, despite best intentions & Axelrod’s Framework, some ‘undefined requirements’ are likely to remain; irrespective of the care taken by all parties. Axelrod’s Framework for developing and enforcing software Cyber-Security clauses in Contracts is constructed as follows:

1. Identify Cyber-Risks
2. Assess Cyber-Risks
3. Suggest Cyber-Risk Mitigation Strategies
4. Propose Contractual Requirements
5. Determine & Analyse Costs & Benefits of Contractual Requirements
6. Prioritise Cyber-Risks Based on Net Value
7. Draft Contractual Terms & Conditions
8. Negotiate Terms & Conditions
9. Enforce Terms & Conditions

By inspection, it is clearly evident that Cyber-Risk Prediction & Measurement Technology is an ideal companion to Axelrod’s Framework across multiple stages.

The Cyber-Risk associated with exponential technological growth is a global concern & deeply troubling to Law Makers & lawyers. The U.S. Government Accountability Office (GAO) stated in 2016 that the Software aboard a Modern Luxury Vehicle is substantially more logically complex than the F-22 USAF Jet Fighter [5]; as displayed in Tab. (2):

| Technology                  | Millions of Lines-of-Code |
|-----------------------------|---------------------------|
| F-22 USAF Jet Fighter       | 1.7                       |
| Boeing 787 Dreamliner       | 6.5                       |
| Modern Luxury Vehicle       | 100                       |

Tab. (2): Software Complexity
Moreover, an ever broadening spectrum of Law Firms advocate the perils & pitfalls surrounding the Cyber-Risk associated with contractual ambiguity & 'undefined requirements'. Consequently, Law Firms are emphasising the need to mitigate this Cyber-Risk via improved Contractual Specification, in concert with management tools such as Control Objectives for Information Related Technologies (COBIT-5) [6], [7], [8]:

- Hence, Cyber-Risk Prediction & Measurement Technology is an ideal companion to the development of Contractual Specifications

4 Conclusion

An analysis of twenty (20) Commercial-Off-The-Shelf (COTS) Technologies was executed in order to investigate how they may be applied to minimise the Cyber-Threats associated with ‘undefined requirements’ pertaining to Contracts, Litigation, Acquisitions & Procurement (CLAP). However, our analysis concludes that only one (1) COTS Technology is capable of achieving this objective (Testimation Technology); as demonstrated utilising four (4) Simplified Examples. One (1) Simplified Example pertaining to Contracts, demonstrates Cyber-Threat minimisation by precisely & unambiguously specifying the minimum level of Cyber-Confidence to be delivered & the maximum level of Cyber-Risk to be tolerated. Three (3) Simplified Examples pertaining to Litigation, Acquisitions & Procurement respectively, demonstrate Cyber-Threat minimisation by the application of a Decision Assistance Table (DAT) generated by this COTS Technology. All four (4) Simplified Examples presented, demonstrate how it is possible to Manage Cyber-Risk utilising a scientifically formulated tool which has been experimentally verified to Predict & Measure all forms of Cyber-Risk to greater than 98.07% accuracy.

Previously published research into the COTS Technology which satisfies our objective, confirms that it yields an experimentally validated solution demonstrating ‘How to Predict & Measure Cyber-Risk’ for any Internet Connected Information System (ICIS) to greater than 98.07% accuracy. Their technology utilises a statistical based methodology whereby the evaluations/decisions made, result in the contraction or expansion of the ‘z-Score’ associated with an infinite population of database records. Moreover, the COTS Technology creators show that their solution holds for all scales of ICIS, from an Application level to an Enterprise level. They also show that Test Effort Estimation (TEE) quantifies Cyber-Confidence, which in turn quantifies Cyber-Risk; subsequently, TEE is a Mission Critical Activity (MCA) when formulating Cyber-Risk Management Strategies & may be utilised prior to project commencement, in-flight or post facto as an assessment &/or auditing tool:

- Therefore, based upon previously published research, the COTS Technology utilised in our article may be considered to be authoritative, reliable & Fit-for-Purpose (F4P) with respect to our objective; i.e. minimising the Cyber-Threats associated with ‘undefined requirements’ pertaining to Contracts, Litigation, Acquisitions & Procurement (CLAP)
5 Bibliography

[1] An Experimentally Verified Method to Predict & Measure All Forms of Cyber-Risk:  
https://www.researchgate.net/publication/344085524_AnExperimentallyVerifiedMethodtoPredictMeasureAllFormsofCyber-Risk

[2] Supplementary File: Experimental Evidence:  
https://www.researchgate.net/publication/344084557_How_to_Predict_Measure_Cyber-Risk_PoC

[3] Supplementary File: Engineering Model:  
https://www.researchgate.net/publication/344085430_The_TEE_Test_Effort_Estim ation_Model

[4] W. Axelrod, CrossTalk, Journal of Defense Software Engineering, Model-Based Testing, Issue: 201707 (July/August 2017), pg. 22-30:  
https://community.apan.org/wg/crosstalk/m/documents/258360  
https://www.researchgate.net/publication/320536868_Using_contracts_to_reduce _cybersecurity_risks

[5] U.S. Government Accountability Office (GAO). (March 2016.) “Vehicle Cybersecurity: DOT and Industry Have Efforts Under Way, but DOT Needs to Define Its Role in Responding to a Real-world Attack.” GAO-16-350:  
https://www.gao.gov/assets/gao-16-350.pdf

[6] Law Firm: Norton-Rose-Fulbright: Cyber-Risk & Project Contracts (2019):  
https://www.nortonrosefulbright.com/en-au/knowledge/publications/b6ab5887/cyber-risk-and-project-contracts

[7] Law Firm: Covington: Managing Risk Associated with 3rd Party Outsourcing (2015):  
https://www.cov.com/-/media/files/corporate/publications/2015/10/managing_risk_associated_with_thir d_party_outsourcing.pdf

[8] ISACA | Reviewed by Sunil Bakshi, CISA, CRISC, CISM, CGEIT, ABCI, AMIIB, BS 25999 LI, CEH, CISSP, ISO 27001 LA, MCA, PMP: Book Review: Vendor Management Using COBIT-5 (2016):  
https://www.isaca.org/resources/isaca-journal/issues/2016/volume-6/vendor-management-using-cobit-5
Appendix

Applied Definitions:

1. **Function Point (FPT):**
   - A Function Point is a software feature which accepts **User Input Commands (UI/C’s)**; examples of FPT’s Include:
     - Buttons, Check-Boxes, Drop-Down Menus, Text Fields, Joysticks, Aircraft Control Pedals, Microphones etc.

2. **Functional Process (FP):**
   - The sequence of steps by which a User interacts with software in order to achieve an objective; some examples of FP’s are:
     - Create User Account, Delete User Account, Generate Monthly Sales Report, Transfer Funds, Verify Account Balance, Pay Bill etc.

3. **Business Process (BP):**
   - One or more Functional Processes (FP’s) delivering a Business objective. For example, the following BP combines three (3) FP’s:
     - BP = On-Boarding a New Employee = FP₁ + FP₂ + FP₃:
       - FP₁ = Create Employee ID
       - FP₂ = Create E-Mail Account
       - FP₃ = Authorise Wi-Fi Access

4. **Critical, High, Moderate & Low Priority Test Cases:**
   - C, H, M, L: Refers to the Priority-Grading (PG) for Executable Test Cases
   - Each Executable Test Case is assigned a Priority by the Business Sponsor
   - The Quad (4) Priority-Grading-Scale is widely utilised commercially
   - Each Executable Test Case seeks ‘Status = Passed’

5. **Super-Optimal Test Cases:**
   - Tests which are designed, written & executed, beyond the Economically Optimal Solution (EOS) of 99% Cyber-Confidence:
     - Typically, these take the form of Negative Test Cases

6. **Negative Test Case:**
   - Negative Testing is commonly described as ‘Error Path Testing’ or ‘Failure Testing’; seeking to identify User Pathways & Test Conditions resulting in failure rather than success. It is an essential strategy in determining the robustness of software, particularly in complex integration environments. For highly robust Quality Assurance (QA) Solutions, the number of Negative Test Cases should substantially exceed the number of Positive Test Cases
   - The contrast between Positive & Negative Test Cases may be demonstrated by the following Simplified Example:
     - **Test Scenario:**
       - Verify that the User Login Function accepts only English characters
     - **Positive Test Case:**
       - The User Login Function accepts English characters
• Negative Test Case:
  • The User Login Function rejects Non-English characters

7. Idealised (Theoretical) Positive & Negative Test Case Population Distribution:
   • For Cyber-Confidence outcomes less than or equal to the Economically Optimal Solution (EOS) of 99%, approximately half of the total population of Test Cases should be Positive & the remainder should be Negative; i.e. each Positive Test Case requires at least one counterpart Negative Test Case
   • For Cyber-Confidence outcomes greater than 99%, all Super-Optimal Test Cases should be Negative

8. Quality Assurance:
   • Numerous interpretations of Quality Assurance (QA) exist in the literature & software development communities; on the surface, it seems to mean different things to different people. However, within the forum of this article, we shall define QA utilising a contrasting paradigm as follows:
     • Testing = the validation associated with a single unit (i.e. one test)
     • QA = the validation associated with a population of units (i.e. many tests):
       • A single test is insufficient to Quality Assure any software solution; a population of tests is always required for the meaningful execution of the QA function

9. Economically Optimal Solution (EOS) of 99% Cyber-Confidence:
   • The minimum level of Cyber-Confidence spanning all four (4) grades of Test Case Priority; Critical, High, Moderate & Low (C, H, M, L)

10. Cyber-Threat:
    • Any threat to an Information Technology (IT) System which may interrupt Business Processes, undermine public interest or negatively impact commercial confidence; examples are:
      • Undiscovered Defects, External Actors (Penetration), Viruses, Phishing, poor Software Development Processes, poor Software Testing Processes, poor Project Management, poor Cyber-Governance etc.
      • A pseudonym for Cyber-Risk

11. Cyber-Security:
    • A pseudonym for Cyber-Confidence