Overview of the Risk-based Cyber Mission Assurance Process

Francois Rheaume
Defence Research and Development Canada - Valcartier
Building 24, 2459 de la Bravoure Road, Quebec, QC
G3J 1X
CANADA

francois.rheaume@drdc-rddc.gc.ca

ABSTRACT

The Risk-based Cyber Mission Assurance Process describes a series of activities on the cyber risk management of military platforms and systems throughout their whole life cycle in order to achieve cyber mission assurance. The process integrates cyber risk management into the Canadian Armed Forces missions, procurement, projects and engineering processes. The process is made of three main activities: Mission assurance requirements analysis, integrated risk assessment and security development. These activities are integrated into the Department of National Defence's Standard Project Framework and the Materiel Acquisition and Support process. This report presents the first activity of the Risk-based Cyber Mission Assurance Process: Mission assurance requirements analysis.

1.0 INTRODUCTION

To achieve their missions, military organizations are becoming increasingly dependent on electronic systems. To assure the success of their missions while achieving efficient resource allocation, military organizations must now focus on the cyber security of these systems in relation with military mission requirements. This need for Cyber Mission Assurance (CMA) is of concern to various military communities such as the acquisition, cyber force, Information Technology (IT), operational and security communities. Defence Research and Development Canada (DRDC) has developed the Risk-based Cyber Mission Assurance Process (RCMAP). Inspired from System Security Engineering (SSE) principles [1], the RCMAP integrates into the whole system lifecycle and in alignment with the Department of National Defense's procurement process [2]. Although it can be adapted to other military communities, it is therefore primarily developed for the acquisition community.

The RCMAP has three main activities:

1. Mission Assurance Requirements Analysis,

2. Integrated Risk Assessment, and

3. Security Development.

The concept behind RCMAP is illustrated in Figure 1. The process is made in such a way that allows decision makers to be aware of risks from assets up to missions and that allows each player to take risk decisions during the whole lifecycle, in a way that is aligned with the mission needs. Risks are first identified and assessed and then mitigated via decision-making applied to the scope, security requirements, risk appetite and overall

acquisition process management. The green arrows at the bottom of Figure 1 depict the Material Acquisition and Support process used by the Department of Defense in Canada.

RCMAP does not reinvent cyber risk management. Rather it is an evolutionary combination of different existing guidelines and frameworks that is axed toward cyber mission assurance. It is a process that adapts RTCA's airworthiness security process [3-5] to cyber mission assurance of military assets and considering all environments, e.g., land, air and navy. It is defined in alignment with the System Security Engineering (SSE) processes of the NIST SP 800-160 [6] and considering aspects of existing frameworks such as ITSG-33 [7] and NIST RMF [8]. It is a procedural approach tailored to military materiel acquisition needs. Like ITSG-33 and NIST RMF, it can be governed by organizational frameworks such as NIST CSF [9], where high-level security profiles can both orient the security decisions on the basis of RCMAP and communicate RCMAP achievements to high-level, senior management.

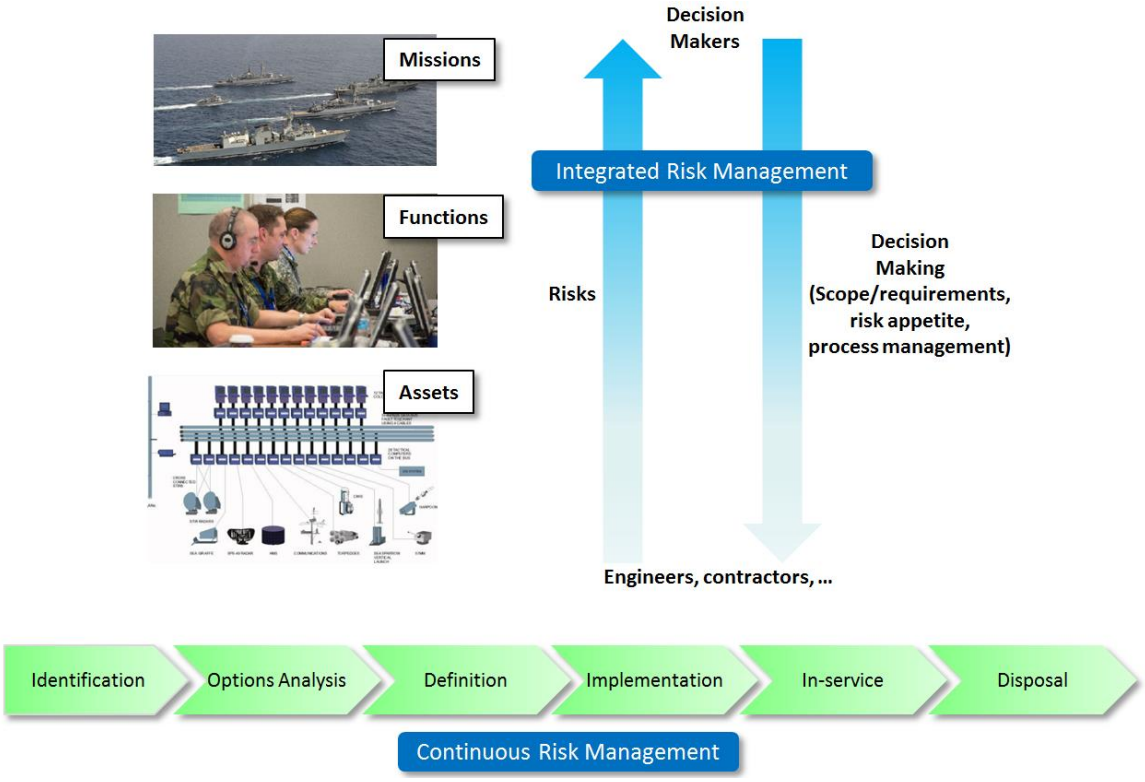

Figure 1: Conceptual overview of the Risk-based Cyber Mission Assurance Process (RCMAP).

Through the Mission Assurance Requirements Analysis (MARA) activity and its methods for determining security requirements, RCMAP allows for harmonization of the Information Technology (traditional enterprise applications) and Operational Technology (cyber-physical systems) types of systems, which are increasingly mingled in military systems. This is an extension to the IT-oriented frameworks like ITSG-33 and NIST RMF.

For the sake of readability, the terms 'cyber security' and 'security' are used interchangeably in this document.

2.0 ALIGNMENT WITH ENGINEERING PROCESSES

RCMAP is an adaptation of RTCA's airworthiness security process to cyber mission assurance. Like the latter, the RCMAP activities integrate into the ISO/IEC/IEEE 15288 system life-cycle process (System and Software Security Engineering) [10]. This is illustrated in Figure 2. This integration adds a systems security aspect to the ISO/IEC/IEEE 15288 system life-cycle process. It is also consistent with the security activities defined in the NIST SP 800-160 System and Software Engineering (SSE) process [10], which was defined after the System and Software Engineering process and based on the same activities. Note that Figure 2 shows the lifecycle up to the integration and verification phases, when the physical system is developed and ready to operate. For the remaining phases of the System and Software Engineering process that range from operation to disposal, no new RCMAP activity is mandated, except that the risk assessment may be updated as results of new threat notifications, system updates or after a certain period of time.

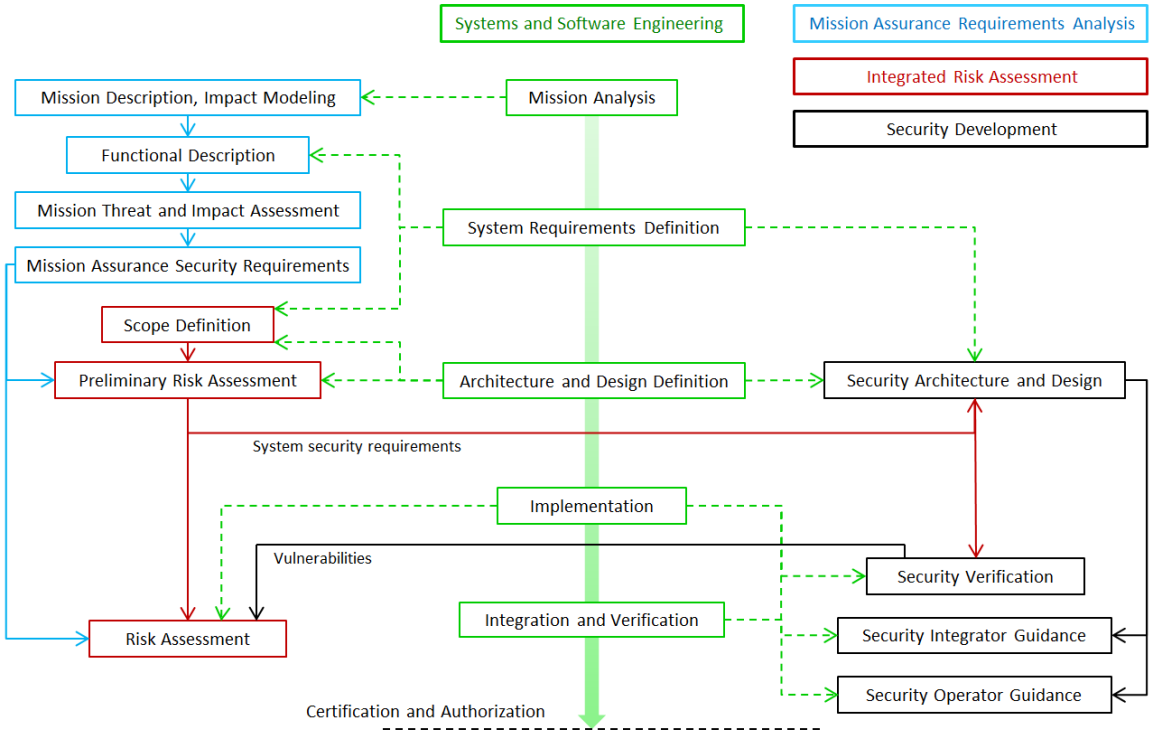

Figure 2: RCMAP as part of the Systems and Software Engineering process.

3.0 RISK-BASED CYBER MISSION ASSURANCE PROCESS

The three main activities to achieve risk-based cyber mission assurance are shown in Figure 3: 1) Mission Assurance Requirements Analysis, 2) Integrated Risk Assessment and 3) Security Development. Each activity is made of a number of sub-activities that are listed in the middle column of the diagram.

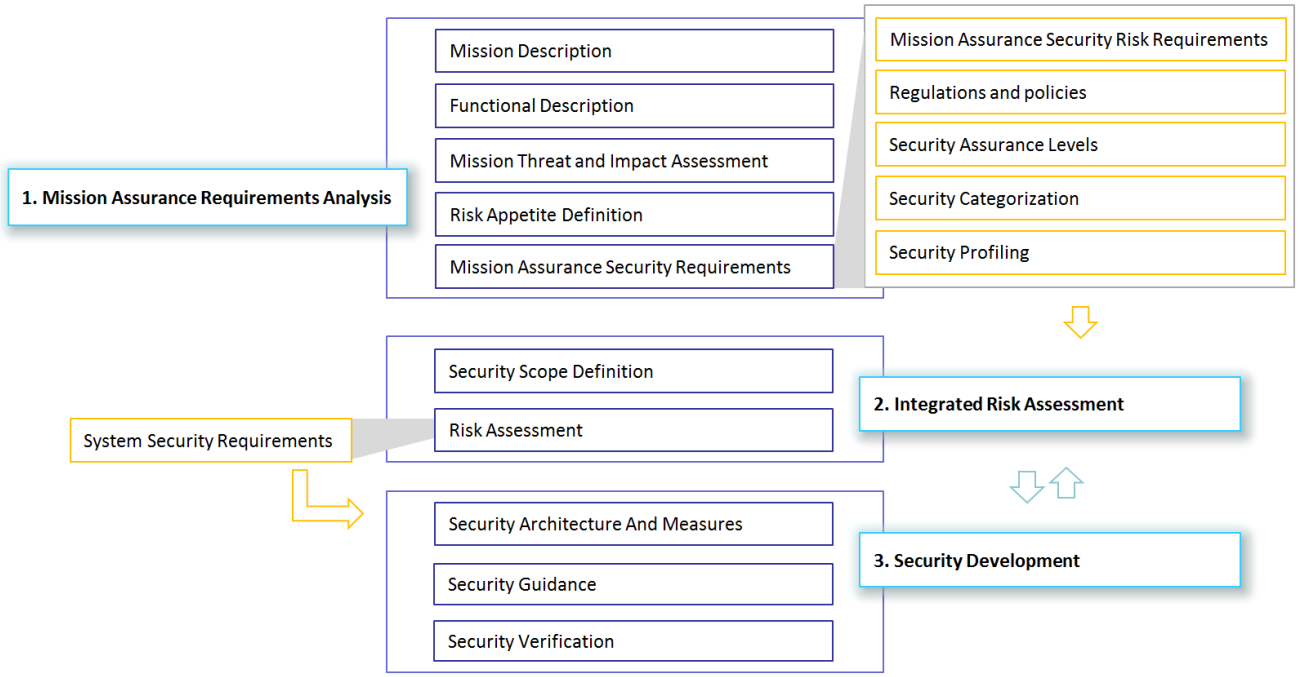

Figure 3: Activities under the Risk-based Cyber Mission Assurance Process with the list of outputs (shown in orange/top right) of the Mission Assurance Requirements Analysis activity.

The Mission Assurance Requirements Analysis activity mostly concerns the organization's management and operations. At this stage, no security expert is required to perform this activity. As shown in Figure 4, this compares to the departmental level in ITSG-33, to the Executive and Business/Process levels in NIST CSF and to the Organization and Mission/Business processes in NIST RMF. The outputs of the Mission Assurance Requirements Analysis activity are produced during the Mission Assurance Security Requirements sub-activity, based on the results of the other four sub-activities. They are grouped into five different categories shown in the orange boxes at the top right of Figure 3: Mission Assurance Security Risk Requirements, Regulations and policies, Security Assurance Levels, Security Categorization and Security Profiling. These outputs are used to guide the Integrated Risk Assessment and Security Development activities, which are involved with systems and where security experts/engineers/contractors come into play to define system security requirements. Note that the frontier between the departmental level and the system level is not totally closed, like in the case of Integrated Risk Assessment and Security Development that are performed at the departmental level but where most of the work is done at the system level.

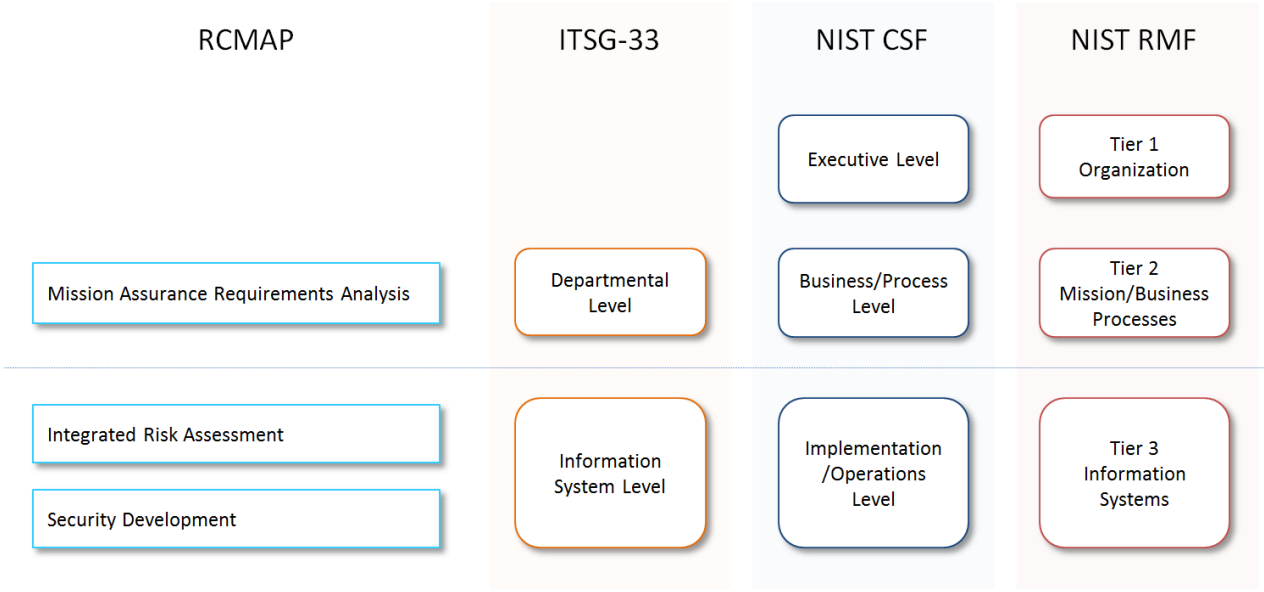

Figure 4: Mapping of the RCMAP main activities onto each of ITSG-33, NIST CSF and NIST RMF abstraction levels.

Cyber Mission Assurance (CMA) is about the management of risks to the missions caused by cyber events. A risk to the mission is defined as the product of the likelihood of a mission threat event happening and the impact on the mission of the threat event:

$$Mission\ Risk = Likelihood(Mission\ Threat) \times Mission\ Impact$$

Mission impacts and mission threats are analyzed and dealt with during the Mission Assurance Requirements Analysis activity, while the likelihoods of mission threats are assessed as part of the Integrated Risk Assessment activity. Thus, the Mission Assurance Requirements Analysis activity is not about determining mission risks but only mission threats and impacts, which are the main contributors in the risk equation. Their determination does not necessitate security expertise at the system level. Complete risk evaluation is performed when working at the system level and therefore requires cyber security experts to evaluate likelihoods from experience and trends. The Mission Assurance Requirements Analysis activity produces requirements on mission risks and not an evaluation of the mission risks, since only mission impact levels are determined and not the likelihoods of the corresponding mission threats. The evaluation of mission risks is completed during the Integrated Risk Assessment activity where system-level risks are assessed.

The following sections describe each of the three RCMAP main activities.

3.1 Mission Assurance Requirements Analysis activity

Mission Assurance Requirements Analysis should start at the Identification phase and continue up to the Definition phase of the procurement (MA&S) process. The goal of the Mission Assurance Requirements Analysis activity is to develop Mission Assurance Security Requirements, including Mission Assurance Security Risk Requirements, Security Assurance Requirements, as well as the determination of Security

Category(ies) and Profile(s) and considering applicable regulations and policies.

This activity divides into five sub-activities:

1. Mission Description,
2. Functional Description,
3. Mission Threat and Impact Assessment,
4. Risk Appetite Definition, and
5. Mission Assurance Security Requirements Determination.

The Mission Description and Functional Description activities lay the building blocks onto which impact relationships and dependencies are defined. Those relationships and dependencies are defined into a mission impact model. Using the mission impact model and the functional description, threats are defined and impacts are determined during the Mission Threat and Impact Assessment activity. Given a level of risk appetite, the mission threats and the mission impacts are then used to establish Mission Assurance Security Risk Requirements. The requirements serve as inputs into Statement of Operational Requirements (SORs), Statement of Work (SOW) or Project Implementation Plan (PIP). They will be used throughout the remaining phases of a project, starting with the project implementation phase, as they will instruct on the mitigation of cyber security risks evaluated throughout the project.

The mission assurance models developed during this activity will also provide managers with a way to communicate mission risks.

3.2 Integrated Risk Assessment

Integrated Risk Assessment starts during the Implementation phase of the MA&S process shown in Figure 1 and after Mission Assurance Security Requirements have been determined. This activity evaluates the cyber risks at the system level. Using the mission threats and the mission impact model defined previously during the Mission Assurance Requirements Analysis activity, the risks evaluated at the system level can be translated into risks at the mission level.

The Implementation phase of the MA&S process is where the system architecture and design is developed, including the security aspect. As the system architecture and design is being developed, it informs risk assessment activities from which new system security requirements are determined. Risk assessment continues during In-service as new threats and vulnerabilities can be discovered and considered.

Integrated Risk Assessment has two sub-activities:

1. Scope Definition and
2. Risk Assessment.

The scope definition has to do with the description of the assets and their attack surface, as well as the

identification existing security measures when the assessment involves existing systems. An asset can be either physical or virtual, including data and protocols, and may also be described as a function or process, depending on the stage of development of the system. It is during the scope definition that will be determined whether risk assessment is performed on the new/upgraded system only or on the whole platform or weapon system, depending on the connectivity between the new/upgraded system and the platform or weapon system. Asset interconnections are described during the asset description activity.

When the scope is established, risk assessment can start. Risk assessment consists in determining threat scenarios at the system levels, i.e., series of Tactics, Techniques and Procedures (TTPs) with some impacts in terms of loss of Confidentiality, Integrity or Availability of the assets under assessment. To better organize threat scenarios, the sequence of TTPs can be aligned onto the adversary life cycle, common known as cyber kill chain. The threat scenarios and their evaluated risks are used to determine system security requirements that drive the mitigation of risks.

3.3 Security Development

Security Development is performed in synchrony with the Risk Assessment activity during the implementation of a project. At this stage, the system security requirements that are determined during the risk assessment activity are translated into security measures. Security Development begins as soon as system architecture and design definition begins. This normally happens during the Implementation phase of the MA&S process. Security Development is also continued during the In-service phase, as new threats may arise or new vulnerabilities discovered.

Security Development has three sub-activities:

1. Development of the Security Architecture,
2. Development of Security Guidance and
3. Security Verification.

The development of the security architecture should follow the system and software engineering process, where the system security requirements are translated into a security architecture and design.

In addition to the development of a security architecture and its implementation, the security aspects on how to securely integrate, install and operate the system in deployment must be addressed. This is what Security Guidance is concerned with. Development of Security Guidance should describe all the required activities and procedures when integrating, installing or operating the new or upgraded system, as well as the constraints and conditions to follow. In DND's investment projects, if the project is an acquisition or the development of an entire platform (aircraft, ship or vehicle), then security guidance for the whole platform should be produced, as more to separate guidance for its individual systems. If the project involves a particular system to be upgraded or added to an existing platform, then security guidance for the system is required, and the security guidance for the platform must be updated to specify the security considerations of the new system applicable to the platform operators.

It should be demonstrated, through test procedures, that the security requirements are met. This is what Security

Verification is concerned with. During this activity, the test procedures should be clearly defined. They should be traceable and in line with the security requirements.

Vulnerability assessment is the principal activity under Security Verification. Depending on the stage of the lifecycle, vulnerabilities can be identified in the design of a system (e.g. missing functionalities, weak protocols, algorithms), in its technical (software/hardware) implementation, in its configuration or in the operation and maintenance procedures. Vulnerability assessment may also cover organizational practices, for example how the supply chain is managed.

Basically, vulnerability assessment takes place at three different times during the lifecycle:

1. Design: During this phase the vulnerabilities are assessed during the definition of threat scenarios. In this phase, vulnerabilities may rather be expressed as security requirements, where the vulnerability represents the lack of a security measure.

2. Installation/Integration: During this phase, tests are conducted on the platform/system to verify that it behaves as intended. This must include vulnerability assessment through scan, inspection and test. In the event that new vulnerabilities are discovered, this may trigger new threat scenarios. The threat scenarios should be updated as a result of that.

3. Operation/Maintenance: As new cyber threats and new vulnerabilities come out each day, it is important to assess whether the platform/system is affected. Also the configuration of the platform/system may change overtime which may expose new vulnerabilities.

During the Installation/Integration and Operation/Maintenance phases, the discovery of new vulnerabilities may prompt new threat scenarios or modification of the existing ones. The threat scenarios should be updated as a result of that along with system security requirements.

REFERENCES

[1] National Institute of Standards and Technology (NIST), Special Publication 800-160, Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2016.

[2] Project Approval Directive 2015, Vice-Chief of Defence Staff, Department of National Defense, Canada, March 2015.

[3] RTCA Inc, Airworthiness Security Process Specification, RTCA DO-326A, 2014.

[4] RTCA Inc, Information Security Guidance for Continued Airworthiness, RTCA DO-355, 2014.

[5] RTCA Inc, Airworthiness Security Methods and Considerations, RTCA DO-356, 2014.

[6] National Institute of Standards and Technology (NIST), Special Publication 800-160, Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, 2016.

[7] Communications Security Establishment Canada, Information Technology Security Guidance, IT Security Risk Management: A Lifecycle Approach, ITSG-33, 2012.

[8] National Institute of Standards and Technology (NIST), Special Publication 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 2010.

[9] National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity, 2014.

[10] Systems and Software Engineering – System Lifecycle processes, ISO/IEC/IEEE 15288, 2015.