Using the ISO/IEC 27034 as Reference to Develop an ASC Library

Alexssander Siqueira

Sheila Reinehr
Andreia Malucelli

Agenda

Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Agenda

Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Introduction

- Secure software development allows the development of solutions considering information security aspects in the project's scope, avoiding malicious users to attack system's vulnerabilities.

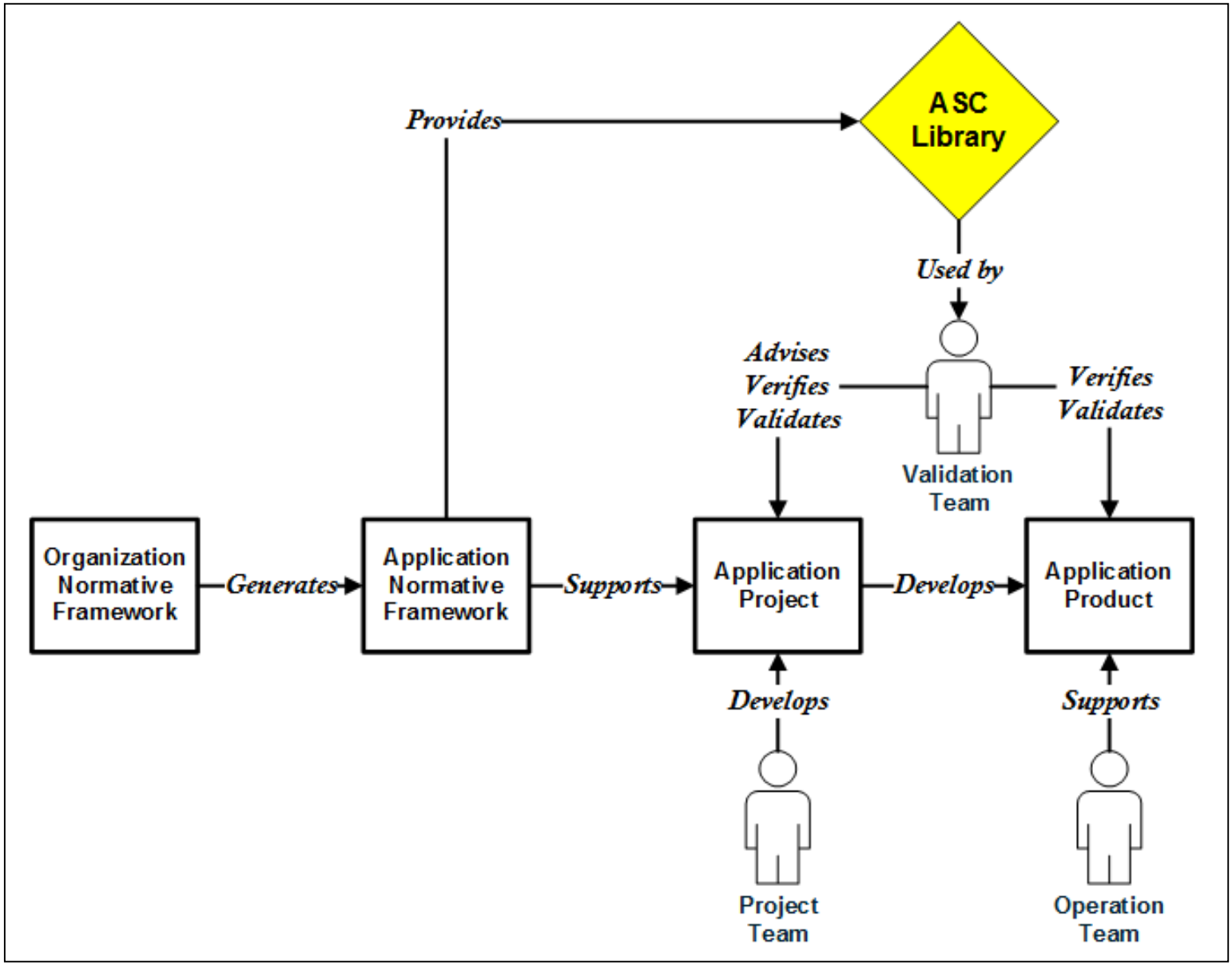
- In this case, security requirements must be integrated into the application's solution design, since its conception.

Introduction

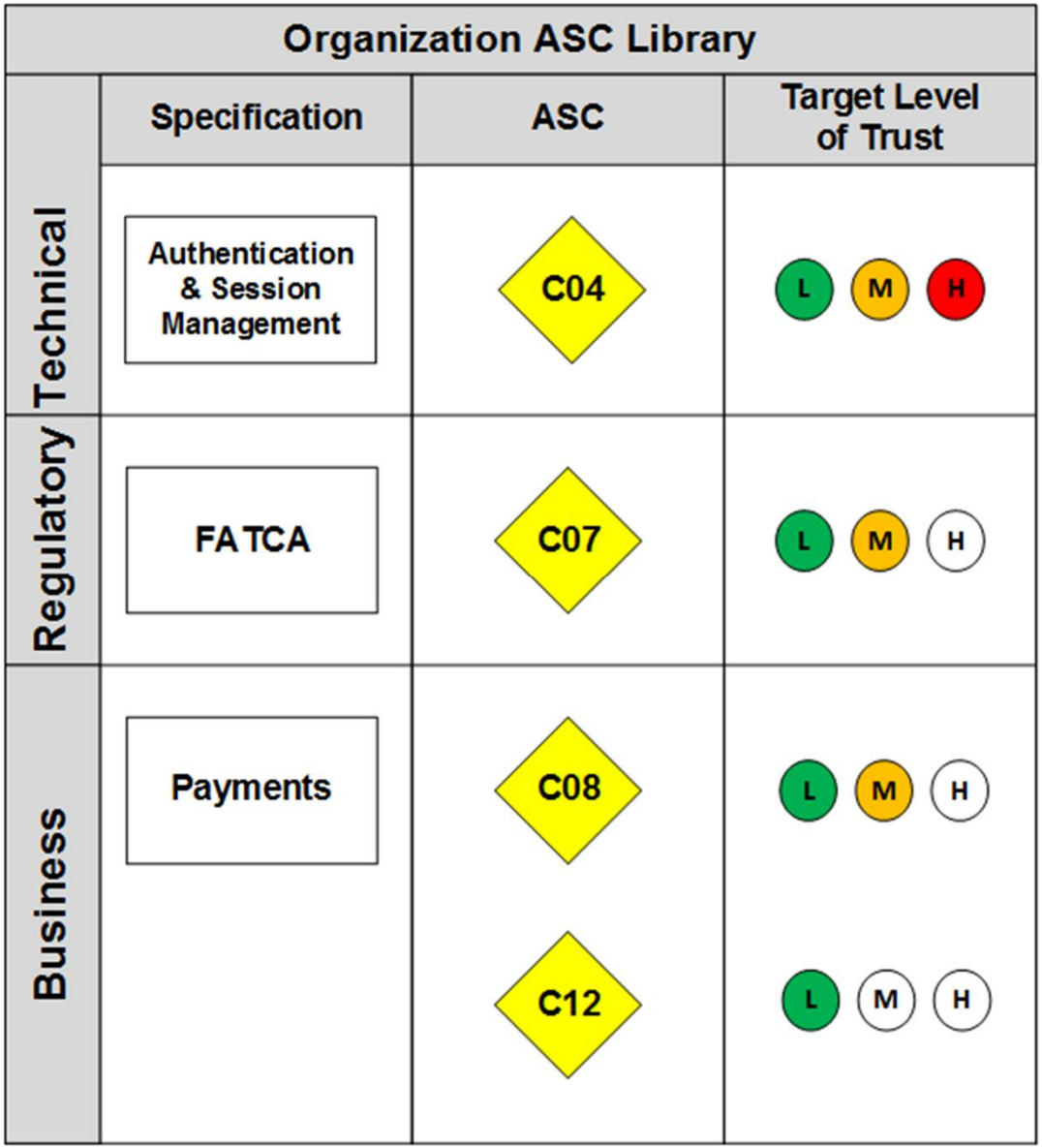
- The standard ISO/IEC 27034 provides the necessary guidance to the development of application security in any interested organization.

- An important standard's concept is the Application Security Control (ASC) Library that may provide a central repository of security controls specification and design.

Introduction



Introduction



Introduction

- This work reports an action-research developed in an international bank that adopted the ASC Library concept.
- After reviewing its previous applications security risk assessments and identifying several missing security controls.
- In this case, the ASC Library became an option.

Agenda

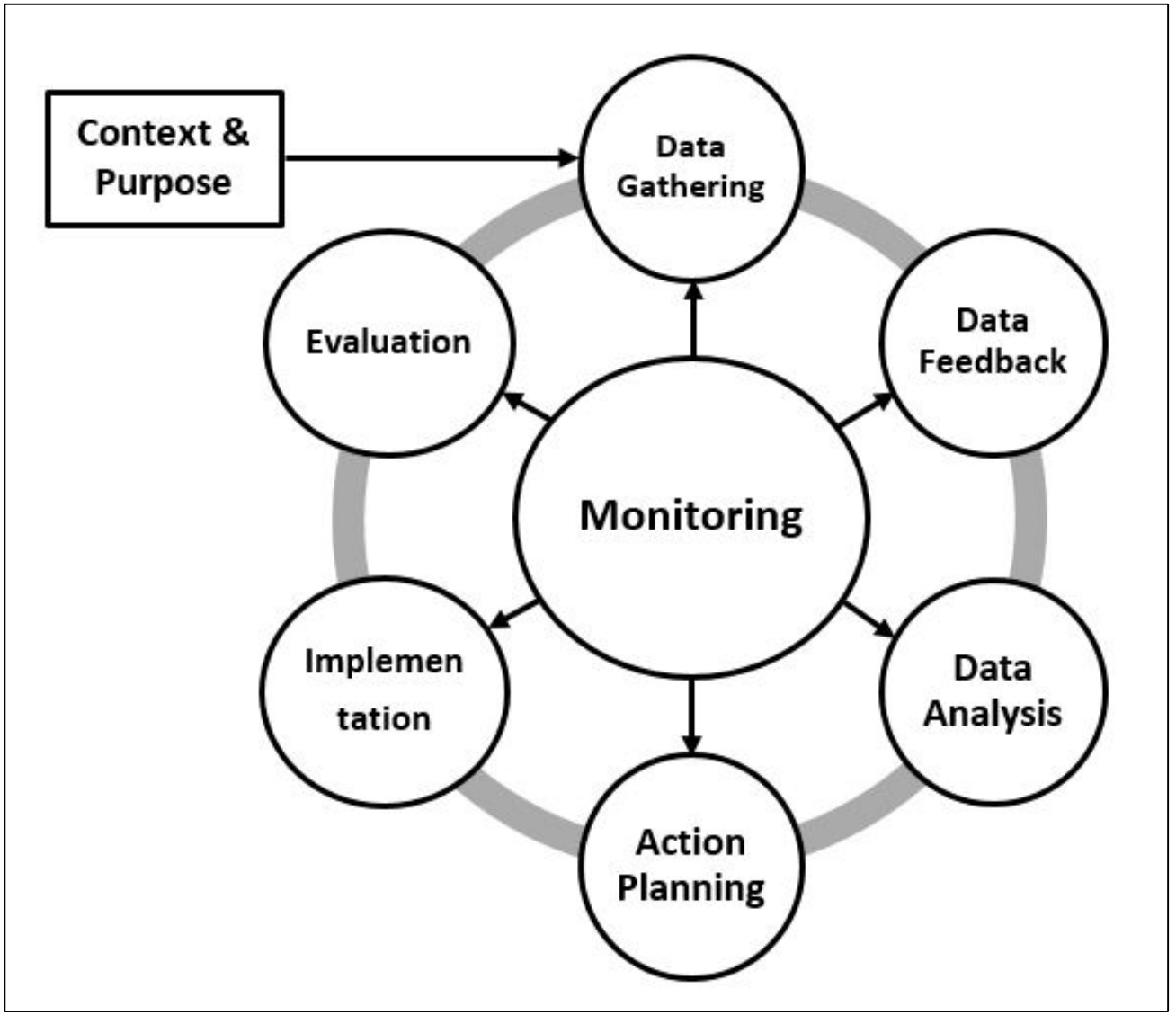
Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Research Method

- The reported experience was developed in an international banking company with a branch office in Brazil.
- A research group was composed by 3 employees (company's internal application security specialists).
- In this case, the suitable research method was the Action-Research, once the researcher was part of company's group.

Research Method



Agenda

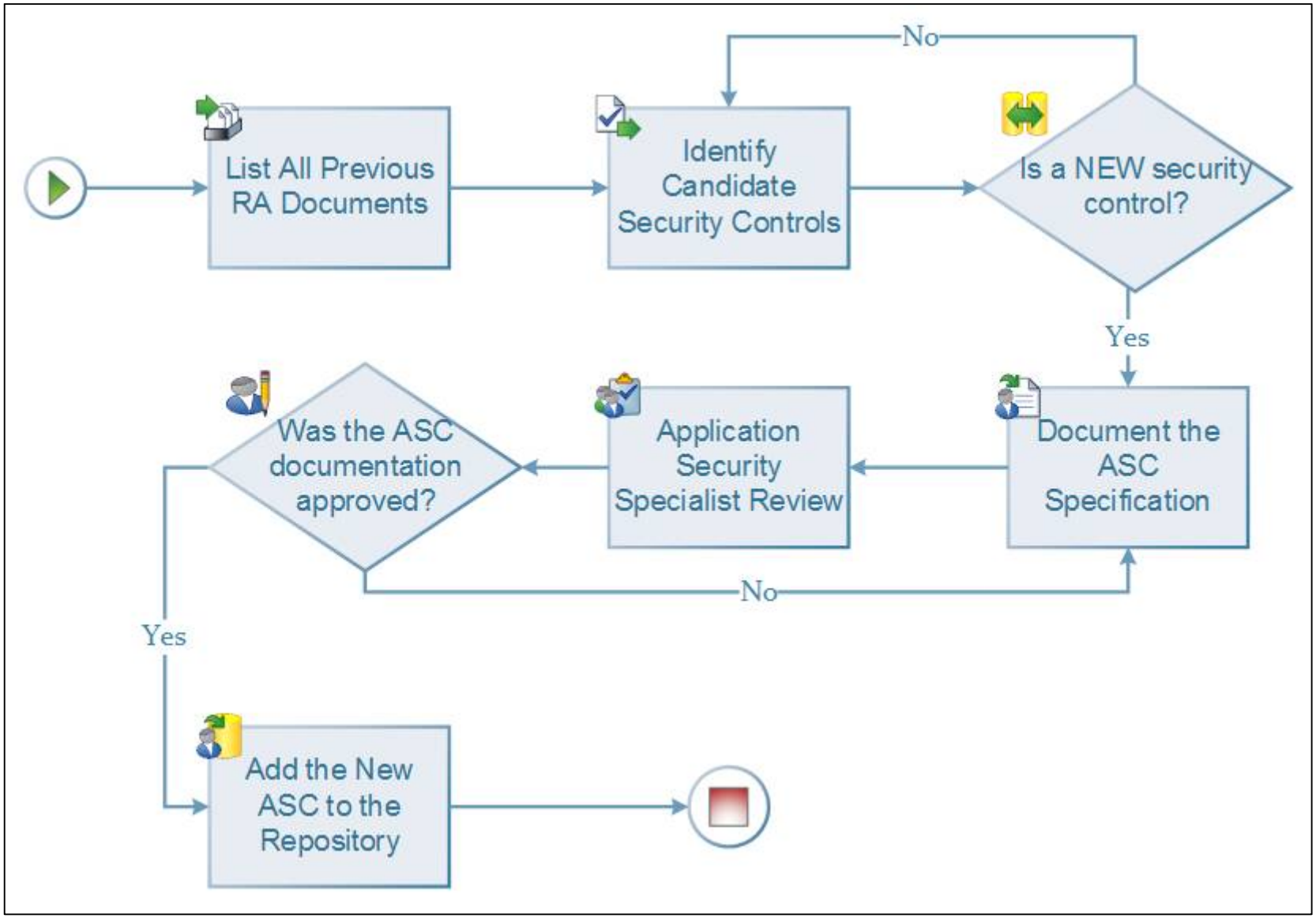
Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Research Development

- An initial set of basic controls was necessary to support the projects development.
- In this case, the main contribution of this work is a process to identify, specify and document the necessary security controls that would be applied in real projects in an international bank company.

Research Development



Research Development

- The current organization secure development process received a punctual change that consisted in the use of the ASC Library during the project's RA document elaboration.

	Security Controls																				
TLT	C01	C02	C03	C04	C05	C06	C07	C08	C09	C10	C11	C12	C13	C14	C15	C16	C17	C18	C19	C20	C21	Total
Low	x			x	x	x						x	x		x		x				x	9
Medium	x			x	x	x	x	x			x	x	x		x		x				x	12
High	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	21

Research Development

- In this case, for each project a list of recommended security controls will be obtained from the ASC Library.

- Instead of searching in previous documentation, the security specialists have to use the library as reference.

	Projects											
	P01	P02	P03	P04	P05	P06	P07	P08	P09	P10	P11	P12
As Is	12	15	21	16	11	21	12	21	21	16	16	21
Should Be	21	21	21	21	21	21	21	21	21	21	21	21
Difference	9	6	0	5	10	0	9	0	0	5	5	0

Agenda

Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Results Analysis

- It was possible to identify a set of security controls before the projects kick-off.
- During the risk assessment new controls could be requested and after the project delivery new threats could be identified by the production support area, demanding in this case a new security control request.

Results Analysis

- The difference calculated (Should Be x As Is), it is an important warning about RA documents quality that must be hold by the organization application security team.

- It was not possible to affirm that the applications were not protected.

Agenda

Using the ISO/IEC 27034 as Reference to Develop an Application Security Control Library

- Introduction
- Research Method
- Research Development
- Results Analysis
- Conclusion

Conclusion

- The ASC Library adoption is an important concept to the secure development process.
- Due to a lack of similar researches, this experience report can be a contribution to support other organizations to aggregate a similar library to their secure development process.

Conclusion

- Further work will report an entire ISO/IEC 27034 standard implementation that will contribute to provide more details about the challenges of adopting the ONF and ANF structures and the necessary changes in the organization environment, culture and work to produce secure applications.

Questions???

Alexssander Siqueira (alexssanderas@gmail.com)