		Misuse Activities				
Actor	Action	#	Security Attributes CO/IN/AV/AC	Source of the threat AIn/UIn/Out	Description	Asset
Customer	Create order	T1	AC	AIn	Disavows having created an order	Order
		T2	AV	Out	Tried to create many orders	N/A
		T3	AV	Out	Create an order in the name of a customer	Order
Broker	Process order	T4	IN	AIn/UIn	Change the information on a legitime order	Order
		T5	CO	UIn/Out	Verify the order process in the system	Order
Broker	Fulfill order	T6	CO	UIn/Out	Verify the information of the order processed (know the purchaser information)	Order
Customer	Notification	T7	AC	AIn	Disavows having accepted an order	Order
		T8	AC	Out	Accept an order in the name of a customer	Order
Broker	Close order & Update account	T9	IN	AIn/UIn/Out	Transfer money between accounts illegay	Account
		T10	CO	UIn/Out	Read information about orders closed	Order
		T11	CO	AIn/UIn/Out	Collects order information to disseminate illegally	Order

#	Security Policy	Description
P1	Open/closed systems	In a closed system, nothin is accesible unless explicitly authorized, in an open system or institution everything is accesible unless explicitly denied.
P2	Least privilege (need to know)	People or any active entity that needs to access computational resources should be authorized only to access the resources they need to perform their functions.
P3	Authorization	Explicit rules must be used to define who can use what resources and how. Authorizations may allow or deny access and may impose conditions for access.
P4	Obligation	Access to a resources is given only if some further action is executed before of after the access.
P5	Separation of duty	Critical functions should be assigned to more than one person or system.
P6	Auditing	An audit tail should record every that was done at some time. This is important for accountability purposes and in case of an attack it could help preventing future attacks.
P7	Authenticated transactions	Any exchange of information should be authenticated at both ends.
P8	Centralized/decentralized control	In a decentralized system its units or divisions have their own administrators and authority to define their won policies of enforcement mechanisms as far as they do not violate global policies.
P9	Ownership and administration	An administrative policy separates the administration of the data from its use
P10	Individual accountability	People or processes must be uniquely identified and their actions recorded an reviewed.
P11	Roles	In each role role different rights are needed to perform the corresponding functions.
P12	Name- or item-dependent access control	We control access to named data items or classes including all their instances.
P13	Content-dependent access control	Access to data depends on the specific records requested.
P14	Context-dependent access control	Access to data depends on what other information is also requested.
P15	History-dependent access control	We consider all or a subset of past requests to decide access.
P16	Discretionary delegation/garanting	A user who has a right may be allowed to delegate or grant this right at his discretion(keeping or losing the right).
P17	Mandatory rights	User receive rights from the system but cannot grant them to others.
P18	Multilevel rights	User are classified in levels and their access rights depend on their levels.