International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFC

(06/2019)

ITU-T Focus Group Digital Currency including Digital Fiat Currency

Protection Assurance for Digital Currencies

Method for Achieving the Required Security Assurance Level for Protecting Digital Currency including Digital Fiat Currency with High Confidence

Security Working Group Deliverable

Focus Group Technical Report

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Currency Including Digital Fiat Currency (FG DFC) at its meeting in May 2017. TSAG is the parent group of FG DFC.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Protection Assurance for Digital Currencies:
Method for Achieving the Required Security Assurance Level for Protecting Digital Currency including Digital Fiat Currency with High Confidence

About this Report

This technical report was written by Jacques Francoeur, from the Security Working group of the ITU-T Focus Group Digital Currency including Digital Fiat Currency.

The author acknowledges the contributions and feedback received from members of the Security working group.

If you would like to provide any additional information, please contact Vijay Mauree at tsbfgdfc@itu.int

Table of Contents

List of Figures

1 Executive Summary

As per the terms of reference of the ITU-T Focus Group on Digital Currency including Digital Fiat Currency (FG DFC), the Focus Group would develop security models around which security requirements could be defined in consideration of current best practices and the critical security challenges faced by the industry today.

> What is so special about transitioning the traditions and precedents of physical money into its digital equivalent?

We have successfully transitioned from physical signatures to their digital and electronic equivalents. Almost everything today is digital. Can we apply current security best practices in the same way we protect current systems? Can we accept the typical financial industry fraud losses? It is a cost of doing business. Can we accept a breach once and a while?

The truth of the matter is that most Internet connected systems are not secure-by-design and are compromised or can be compromised with just intent and resources.

> *Does Digital Fiat Currency or a Central Bank Digital Currency warrant a higher level of security assurance than is typical of financial services today?*

What will it take to "protect" various forms of Digital Currency? What is the problem? Do we have the capability and resources? The simple answer, based on our track record, highly uncertain. What will it take to get to the required answer – with confidence?

The field of Cybersecurity - one cannot see it, touch it, smell it, hear it. For these ephemeral reasons, the field has been and continues to be avoided by most and mostly misunderstood. Even within the active security field, there is great variability in skill levels. This is becoming worse with the influx of new practitioners. The field could benefit from analytical skills since the level-of-complexity of the field is very high and growing rapidly.

The field of Internet and eCommerce was initially relegated "to the basement" within IT. A security chasm formed between Security and IT who spoke "technobabble" and used fear, uncertainty and doubt and the business who had a "technophobia" for the rapidly changing Internet. Initially, the separation of the two worlds worked. However, in the last decade, a security awakening has occurred. Fiduciary executives have awakened to the impact of decades long underinvestment in and lack of commitment to security. Excessive residual risk was taken.

Unlike other fields, Security is an art and not a science. It is not formed in the traditional "field-of-science" manner with formal university creation but rather through grass root, technical expertise as the information revolution exploded. With spreadsheets being the primary industry tool to manage security controls, most practitioners develop their own approach and method each time they need to measure, track and demonstrate compliance. This institutional security information is entombed in the spreadsheet and sometimes lost and/or reinterpreted by others. The cycle of loss repeats itself.

Secure-by-Design is most often not incorporated into the original design due to increased costs and complexities. In this case, security is relegated to a "bad IT" Band-Aid role with poor protection results.

Today, innovation is outpacing our ability to secure and protect with confidence. The impact of not having a formal security taxonomy and ontology, results in variability and subjectivity in the nature, form and prescriptiveness of security control descriptions for identical security control topics. This variability requires significant human reconciliation and interpretation efforts, resulting in significant time and costs allocated to understanding, managing and normalizing.

This paper outlines a security model and method that addresses two security challenges at the core of insufficient and ineffective protection[1] - funding driving amount-of-security and visibility driving quality-of-security.

- The **Unified Security Model** (USM) integrates into a single system level model the fiduciary cycle of risk acceptance which determines resource funding (amount-of-security).
- The **Unified Expression Model** (UEM) integrates expressions into the USM as a single system with high visibility of "*Risk to Value and its Protection*" down to the more specific "*Attack Exploit to Target Vulnerability and its Countermeasures*" enabling advanced visibility, measurability and analysis of state-of-security to ensure quality-of-security.

Given the criticality of currency to people, nations and society and the severity of damages that could result from a loss of currency trust and confidence, the level of security assurance for the Digital Fiat Currency use case will be deemed to be:

Security Assurance Level: 4-5 High to Very High
On a 1 to 5 scale of 1: Very Low | 2: Low | 3: Average | 4: High | 5: Very High

For general reference purposes, the assurance level proposed is similar to the security assurance expected of the following.

- NIST 800-54 r4: "Security and Privacy Controls for Federal Information Systems and Organizations" High Assurance on a 3-level scale of Low | Medium | **High**
- Common Criteria v3.1 r5 for supply chain hardware and software security: Common Criteria for IT Security Evaluation (ISO/IEC 15408)
- US FIPS high assurance standards like FIPS 140-3[2] "Security Requirements for Cryptographic Modules"

This paper recommends that for high to very high assurance use cases such as Digital Currency, an integrated, high precision, inheritance-based system and method be used to define, model and analyze all aspects of security required to provide reasonable protection.

[1] This paper makes a fundamental distinction that security "delivered" by security assets performing security functions is not the same as protection "received" by business assets performing business functions. The efficacy of the security in providing protection (mitigate exploit) is specific to the attack exploit.

[2] FIPS 140-3 "Security Requirements for Cryptographic Modules
https://csrc.nist.gov/publications/detail/fips/140/3/final

2 Overview

As indicated by the frequency and nature of compromises that are contained and breaches that trigger public disclosure, the protection of a complex end-to-end business, with confidence, is very difficult to achieve and maintain over time. The protection of a complex end-to-end ecosystem is a an even greater challenge.

How can the "challenge be met?" *What are the main challenges?*

How much will "meeting this challenge" cost? Is a new paradigm needed?

The central challenges are technical and non-technical. Protection is needed and that comes from an adequate "amount of security" driven by funding allocated by fiduciaries and the required "quality of security" in delivery. Protection can only be delivered "up to" the level of security funding. Failure to protect is often not a technical issue but a funding one.

The need for effective and persistent security in a high assurance use case of "Digital Currency including Digital Fiat Currency" ("Digital Currency") represents an even bigger challenge. To meet the challenge, a new approach is proposed that contains the necessary level of precision and control to adequately define and analyze the requirements in order to receive the funding to deploy, operate and maintain the required protection.

Effective protection cannot be achieved without a clear understanding of what is being protected – TARGET. Central to both the USM and UEM is a simple relationship of Threat | Target | Protection. This document defines a Digital Currency Ecosystem (DCE) Target model for centralized, hybrid and decentralized issuance. The DCE Target is defined in 5 Stages with a more detailed level 2 decomposition for each stage. The document outlines a residual risk model applied to the high level DCE Target.

In order to define specific security standards, the DCE Target must be further decomposed to identify specific vulnerabilities to specific threats that need to be addressed. A detailed breakdown of the Target enables a clear understanding of the relationships between DCE components.

2.1 Scope

The scope of this document is the full end-to-end life cycle management of a Digital Currency Ecosystem from procurement of DC technology, to DC issuance to DC value conversion.

2.2 Major objectives

The main objective is to provide a new more precise and integrated method to define, fund, deploy, operate and maintain sufficient security so as to reduce the residual risk to a reasonable level with confidence.

3 The Unified Security Model

The Unified Security Model (USM) illustrated in Figure 1 is a single integrated model derived from the only three fundamental elements of the problem: Threats to Value which becomes a Target that should be Protected.

Security engages cooperatively with the Target (blue arrow inside Target) while in all cases except one "the insider" the Threat does not have such a favorable relationship with the Target (red arrow outside target).

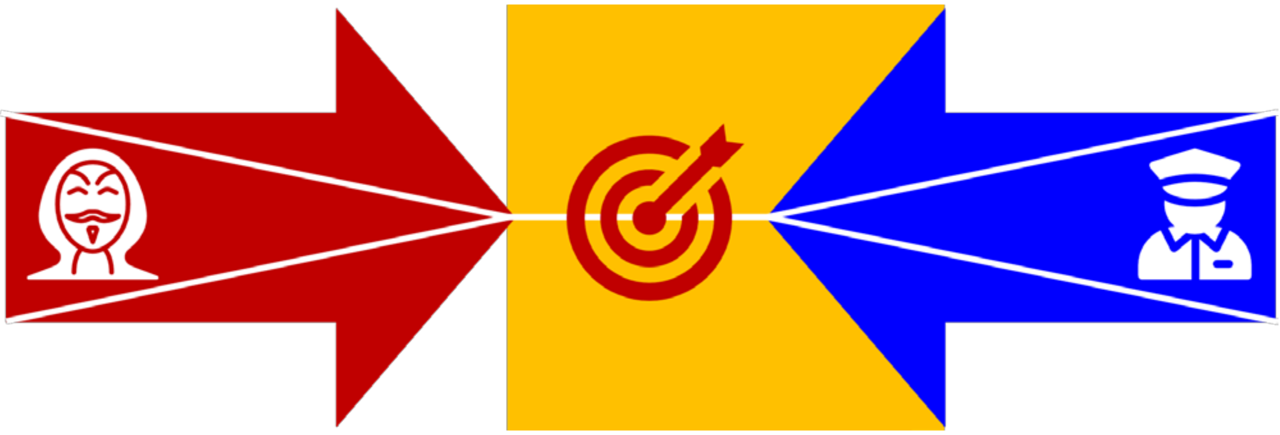


Figure 1: Unified Security Model: Threat | Target | Security

The high-level model of Figure 1 is extensible architecturally into a much more detailed Unified Expression Model of Figure 2. The expression is a much more detailed construct but still involving the same fundamental elements as the model. The expression can be used for attack vector analysis to a specific Target vulnerability to identify appropriate security countermeasures, all in a single integrated system, illustrated in Figure 1 as a high-level risk model and the lower construct Figure 2 as an "atomic expression" that can model an actual implemented control.

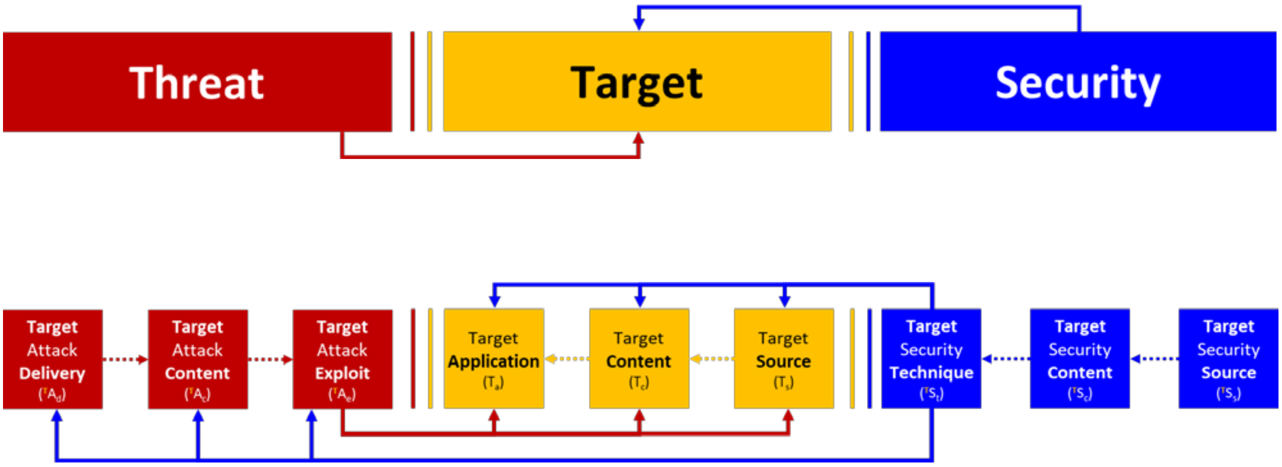

Threat
Target
Security
Target Attack Delivery ($^{T}A_d$)
Target Attack Content ($^{T}A_c$)
Target Attack Exploit ($^{T}A_e$)
Target Application (T_a)
Target Content (T_c)
Target Source (T_s)
Target Security Technique ($^{T}S_t$)
Target Security Content ($^{T}S_c$)
Target Security Source ($^{T}S_s$)

Figure 2: Unified Expression Model (top) & Threat | Target | Countermeasure Expression

A unique outcome of this integrated high and precise level model is the ability to measure in increasing detail while deriving higher level properties through hierarchical aggregation.

To understand the potential threats to a Target and what would be an effective control countermeasure design one first has to understand in detail what needs protection, as illustrated as the Target in Figure 1. In this case the Target is the full life cycle of "Digital Currency including Digital Fiat Currency," collectively referred to as the Digital Currency Ecosystem (DCE), illustrated in Figure 3.

The following will outline:

- A model of the Digital Currency Ecosystem as a business Target decomposed three levels.
- An assurance model to allow the nature and degree-of-security to be determined for different elements of the DCE Target model.
- Residual Risk Model to determine the acceptable residual exposure remaining after the application of a set of security controls and assurance level.

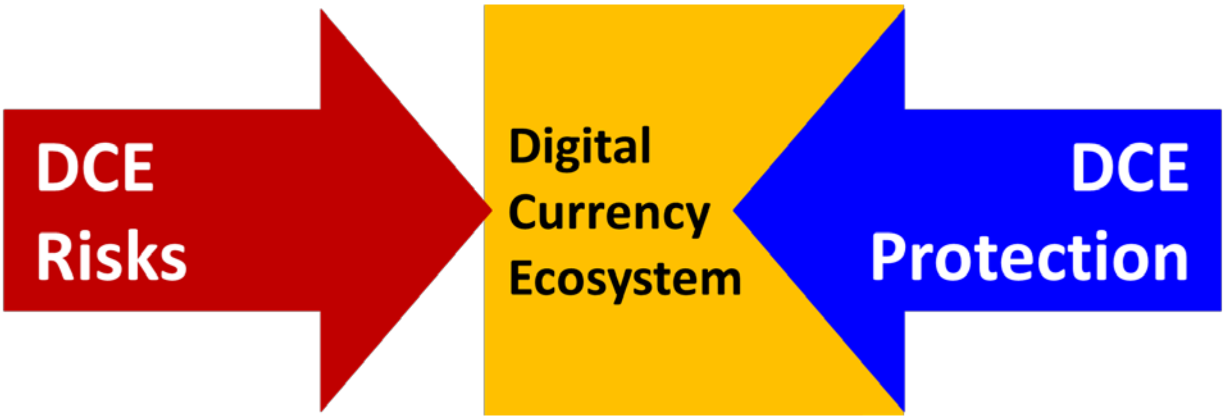


Figure 3: Digital Currency Ecosystem as USM Target

A "Payment Pattern" use case applying this model is published in a Liaison Statement. The Payment Pattern is illustrated in the target zone of Figure 4. The pattern involves the Stage 4 and 5 to both centrally and de-centrally issued Digital Currency. It decomposes Stage 4 and 5 Level 2 further into level 3 and so on.

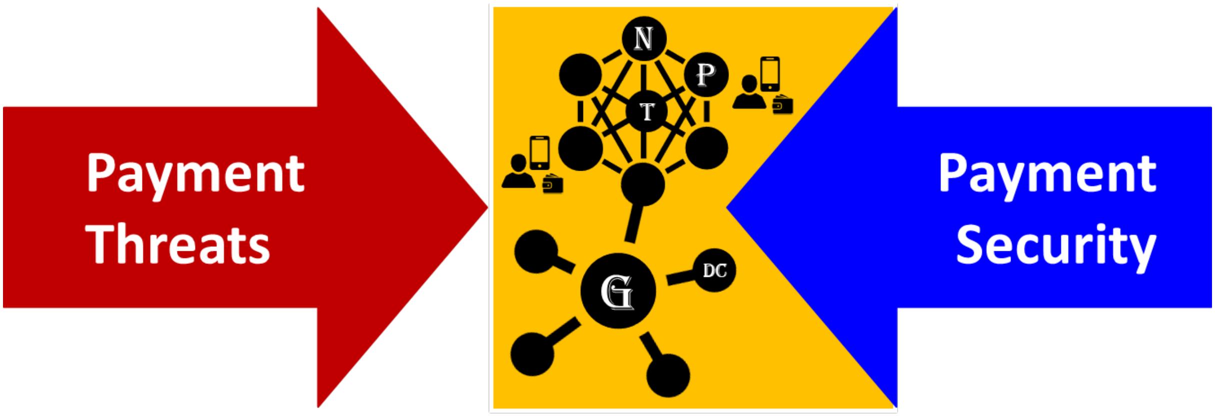
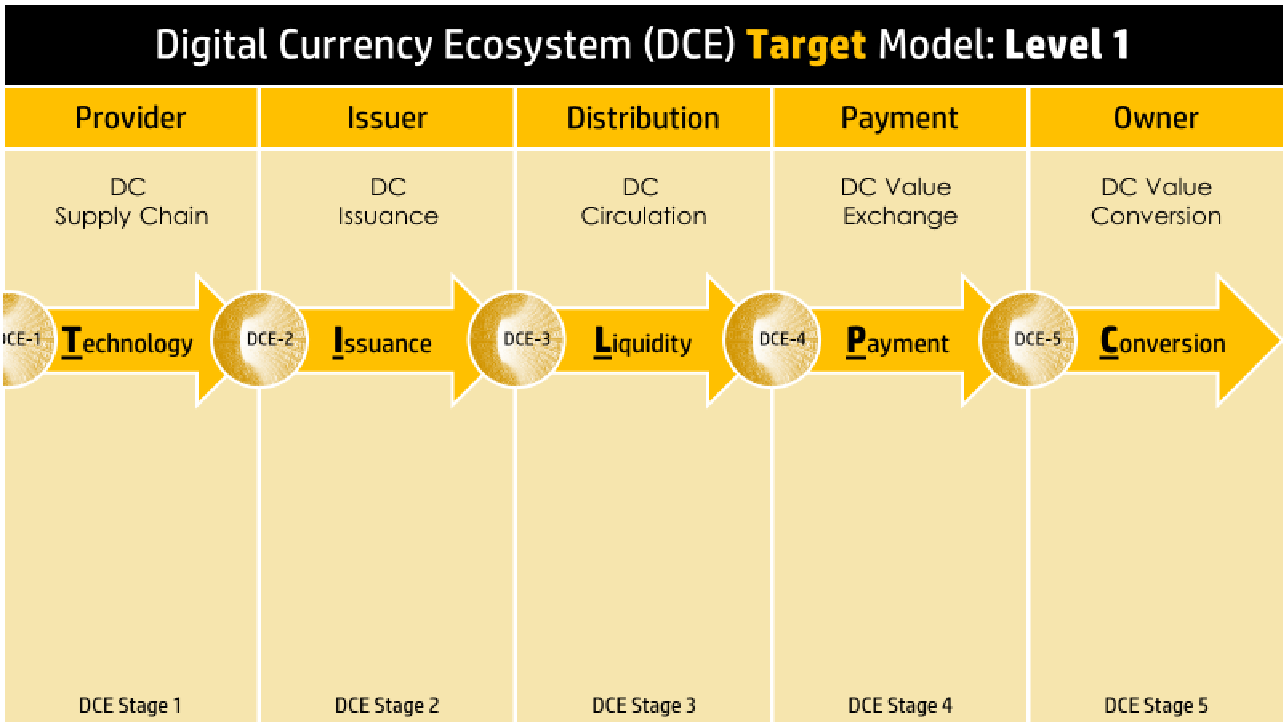


Figure 4: Payment Pattern Threat | Target | Protection Use Case in liaison statement

3.1 DCE Target Model

The Digital Currency Ecosystem (DCE) Target model is achieved through a series of decompositions, each intended to define the core structure that exists within each decomposition. The first level of decomposition is linear and sequential and seeks to divide along natural boundaries. It segments the DCE into five stages, illustrated in Figure 5.



Digital Currency Ecosystem (DCE) Target Model: Level 1

Provider	Issuer	Distribution	Payment	Owner
DC Supply Chain	DC Issuance	DC Circulation	DC Value Exchange	DC Value Conversion
DCE-1 Technology	DCE-2 Issuance	DCE-3 Liquidity	DCE-4 Payment	DCE-5 Conversion
DCE Stage 1	DCE Stage 2	DCE Stage 3	DCE Stage 4	DCE Stage 5

Figure 5: Digital Currency Ecosystem Level 1 as USM Target

- DCE Stage 1: **Technology**: this stage focuses on the Providers and the people, process and technology practices that were involved in the design, manufacture and delivery of the Digital Currency issuance and management technology.

- DCE Stage 2: **Issuance**: Once there are trusted Provider sources, the Issuance Party procures the DC issuance technology and then goes through a process to activate the technology and conduct the DC issuance event(s).
    - **Central Issuance**: Issuance may be centralized by a single authority as in the case of the issuance of Digital Fiat Currency or Central Bank Digital Currency (CBDC).
    - **Decentralized Issuance**: DC issuance by Participants in a P2P Network.
    - **Hybrid Issuance**: DC issued by a mixture of both.
- DCE Stage 3: **Liquidity**: This stage involves the availability of DC in the central issuance model of Stage 2.
- DCE Stage 4: **Transaction**: This stage involves payment - executing and completing the transaction initiated by a Source Owner and a Destination Owner.
- DCE Stage 5: **Conversion**: This stage involves the transfer, conversion and transaction involving DC between Owners either directly via a P2P blockchain or indirectly via a payment gateway. Owners via an internet device and a local software Wallet application that manages the current DSs, transact.

Within each stage of the DCE there are questions of data flows within and between stages; data sensitivity in terms of Privacy and business criticality and access controls; governance and legal requirements.

3.2 DCE Threat-to-Target Analysis

The Threat-to-Target analysis follows the defining the target including core business functions and data types involves understanding the inherent risks in the processes involved within each stage.

The key question becomes what is the level-of-security and assurance required to reduce the residual risk and exposure of each stage to a reasonable and acceptable level? It is important not to over secure undervalued assets with respect to the under protection of valuable assets. Security is a scares resource and impacts the business and customer experience. It should be carefully applied to minimize the impact on users.

Figure 6 illustrates the same DCE of Figure 5 but now set against a background of threats to each stage. The nature and frequency of threats is driven be perceived attacker value and degree-of-difficulty. The threats that apply in each stage vary as each stage is fundamentally different.

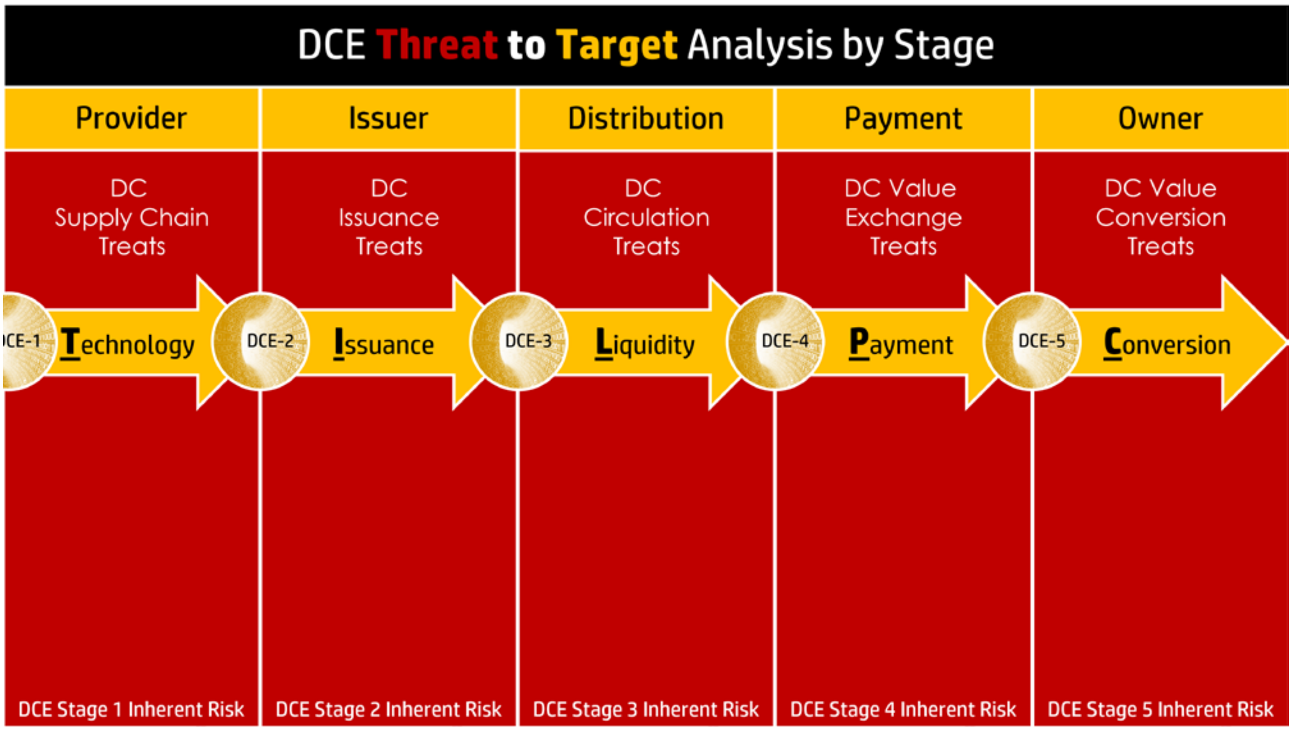


Figure 6 DFC Ecosystem Threat & Inherent Risk Analysis by Stage

- Supply Chain Threats: This stage would involve threats to hardware and systems, People and software involved in Stage 2.
- Issuance Threats: This stage would involve threats that are unique to the method of issuance of DC.
- Circulation Threats: This stage would involve threats to the circulation of DC.
- Exchange Threats: This stage would involve threats to the payments and transactions involving DC.
- Conversion Threats: This stage would involve threats to the transfer and conversion of DC.

3.3 DCE Impact-to-Target Analysis

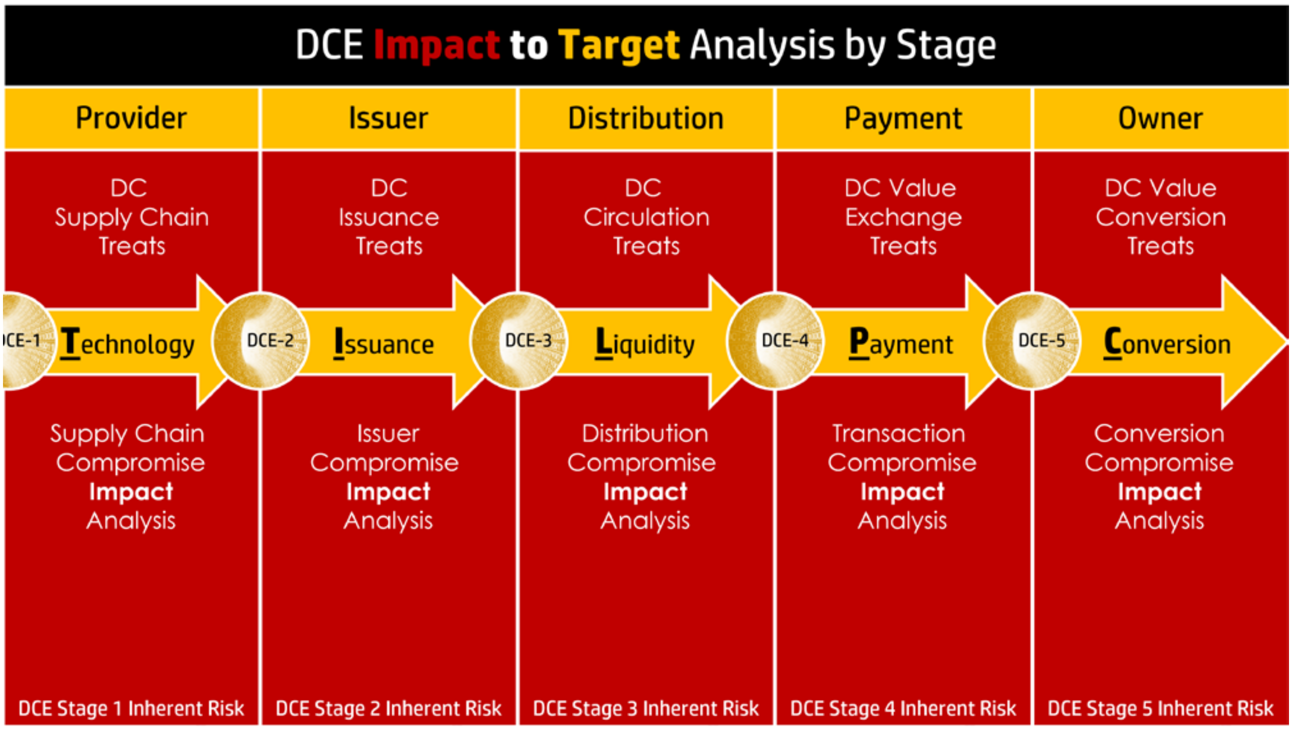
The Impact-to-Target analysis involves taking a step further from the Threat-To-Target analysis to consider the nature and severity of the impact. Given that resources are scarce, allocation of resources should be based on greatest risk and impact reduction.

Previously we established a method to define the target, what needs to be protected at a level 1. This decomposition process must continue to level 2 and so one to the point of defining the function of all IT device classes, data types and applications.

The DCE model allows for a focused risk-based protection approach to be applied to each component involved in each stage of the DCE. Security Assurance means not only nature or type of security but also levels of security and verification. With knowledge of potential impact of a compromise at each stage, appropriate controls can be designed, and assurance measures applied for the desired confidence level.

Techniques of security applied to network devices, data and software remain mostly common across all roles and uses cases of these assets. IT devices, data and software have no contextual notion of use case. Based on context, the classes involved, their role at any given time, the potential impact levels of protection are articulated by policy.

Figure 7 illustrates the impact analysis applied to the DCE level 1 decomposition. For each stage, the level 1 impact analysis seeks to understand the severity of the consequences of a stage being compromised. From this, a standard of security and assurance can be articulated.



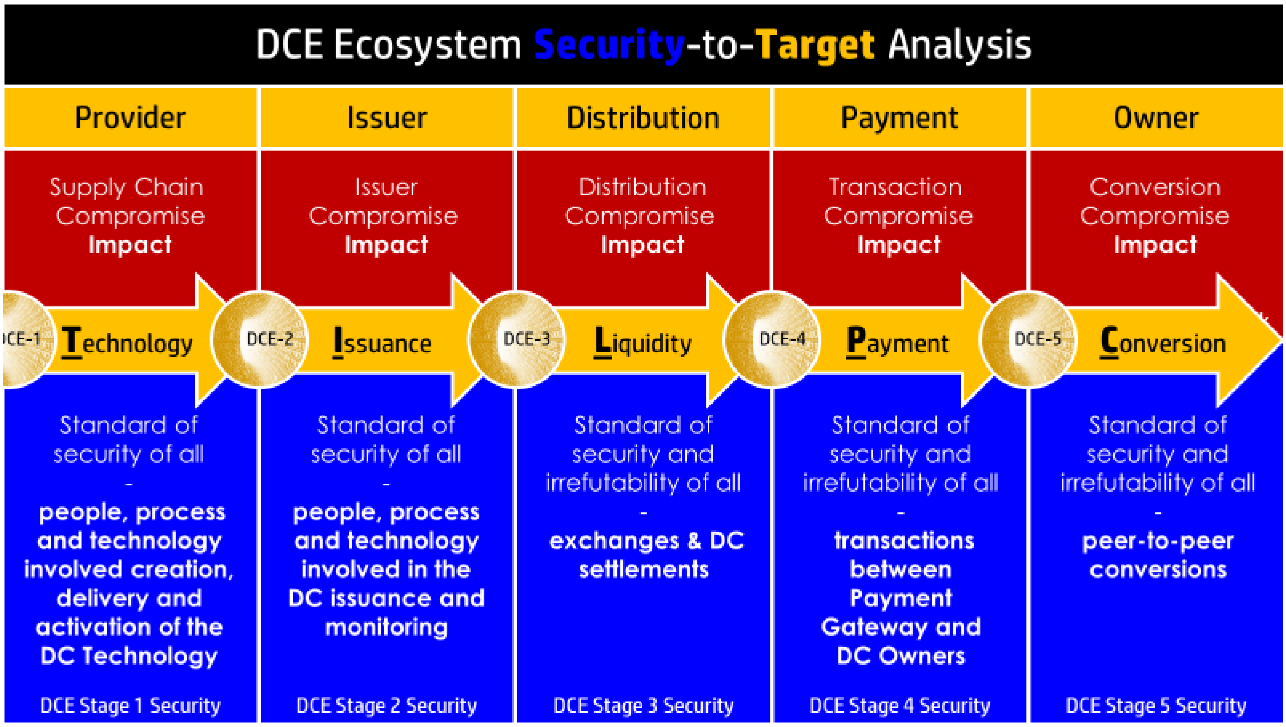
DCE **Impact** to **Target** Analysis by Stage

Provider	Issuer	Distribution	Payment	Owner
DC Supply Chain Treats	DC Issuance Treats	DC Circulation Treats	DC Value Exchange Treats	DC Value Conversion Treats
ICE-1 Technology	DCE-2 Issuance	DCE-3 Liquidity	DCE-4 Payment	DCE-5 Conversion
Supply Chain Compromise **Impact** Analysis	Issuer Compromise **Impact** Analysis	Distribution Compromise **Impact** Analysis	Transaction Compromise **Impact** Analysis	Conversion Compromise **Impact** Analysis
DCE Stage 1 Inherent Risk	DCE Stage 2 Inherent Risk	DCE Stage 3 Inherent Risk	DCE Stage 4 Inherent Risk	DCE Stage 5 Inherent Risk

Figure 7: DCE Level 1 Compromise Impact & Reasonable Assurance Model

3.4 DCE Security-to-Target Analysis

The Security-to-Target analysis illustrated in Figure 8 takes the outcome of the Impact-to-Target analysis of Figure 7 and defines appropriate security control that could to be applied at each stage based on the nature of the impact.



DCE Ecosystem Security-to-Target Analysis

Provider	Issuer	Distribution	Payment	Owner
Supply Chain Compromise **Impact**	Issuer Compromise **Impact**	Distribution Compromise **Impact**	Transaction Compromise **Impact**	Conversion Compromise **Impact**
CE-1 Technology	DCE-2 Issuance	DCE-3 Liquidity	DCE-4 Payment	DCE-5 Conversion
Standard of security of all - **people, process and technology involved creation, delivery and activation of the DC Technology**	Standard of security of all - **people, process and technology involved in the DC issuance and monitoring**	Standard of security and irrefutability of all - **exchanges & DC settlements**	Standard of security and irrefutability of all - **transactions between Payment Gateway and DC Owners**	Standard of security and irrefutability of all - **peer-to-peer conversions**
DCE Stage 1 Security	DCE Stage 2 Security	DCE Stage 3 Security	DCE Stage 4 Security	DCE Stage 5 Security

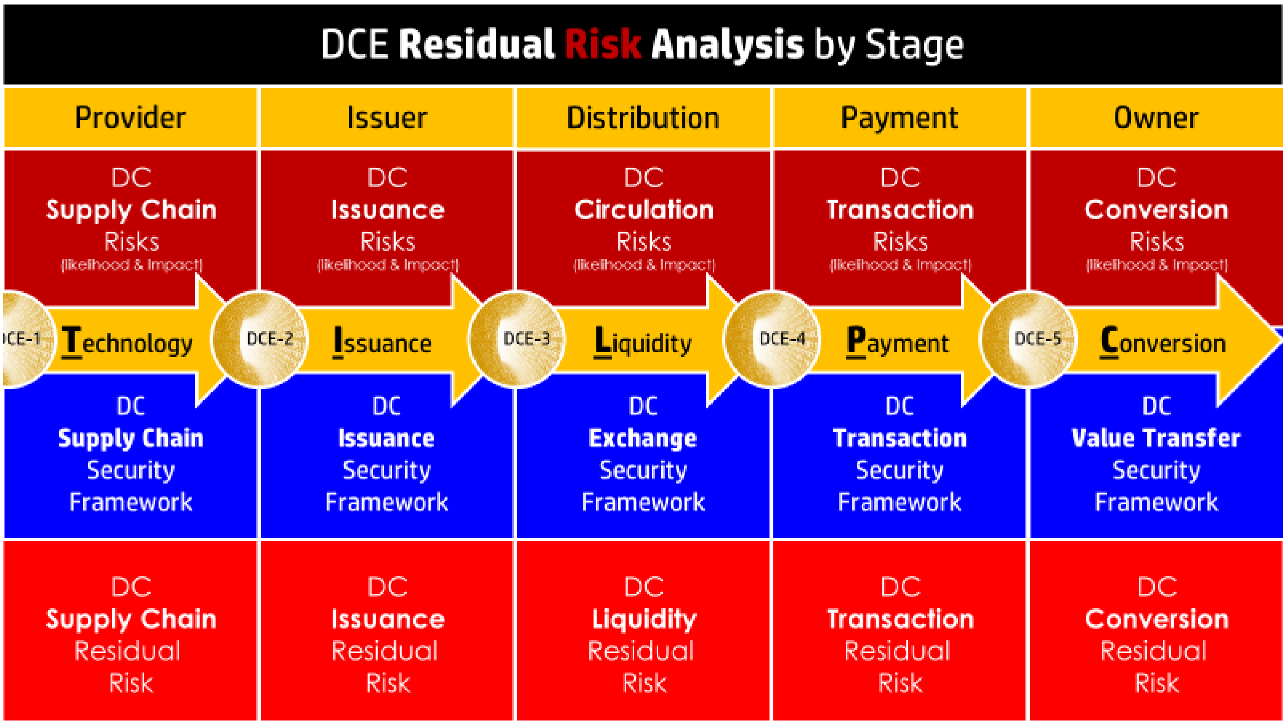
Figure 8: DCE Level 1 Stage: Security Assurance by Stage

This Target decomposition process should continue each level for each stage. The result is an ever-increasing target precision that ultimately leads to the identification of specific Asset Classes and specific assets that can be protected by specific controls.

3.5 DCE Residual Risk Analysis

Residual Risk Analysis involves estimating whether the risk remaining after applying available protection is acceptable by relevant stakeholders. Acceptability means whether the damages and losses in the event of realization of the risk are acceptable by the impacted stakeholders. If it is deemed unacceptable, the same impacted stakeholders must invest in risk reduction.

The ultimate policy and standard decision rests with what governing stakeholders deem acceptable residual risk by stage. Figure 9 illustrates the residual risk DCE model. It integrates the Target model with the threat and security assurance models. The residual risk and exposure of any stage is the inherent risks created by the threats reduces by the security and assurance standard.



DCE Residual Risk Analysis by Stage

Provider	Issuer	Distribution	Payment	Owner
DC Supply Chain Risks (likelihood & Impact)	DC Issuance Risks (likelihood & Impact)	DC Circulation Risks (likelihood & Impact)	DC Transaction Risks (likelihood & Impact)	DC Conversion Risks (likelihood & Impact)
ICE-1 Technology	DCE-2 Issuance	DCE-3 Liquidity	DCE-4 Payment	DCE-5 Conversion
DC Supply Chain Security Framework	DC Issuance Security Framework	DC Exchange Security Framework	DC Transaction Security Framework	DC Value Transfer Security Framework
DC Supply Chain Residual Risk	DC Issuance Residual Risk	DC Liquidity Residual Risk	DC Transaction Residual Risk	DC Conversion Residual Risk

Figure 9: DCE Residual Risk Analysis by Stage

3.6 DCE Risk Acceptance Decision

The Risk Acceptance Decision is a fiduciary decision directly tied to risks and investment. Less risk requires more investment. As illustrated in Figure 10, for each stage a Risk Assessment is conducted and based on the residual risks results and the risk acceptance appetite, funding is allocated to maintain or reduce the residual exposure. In some cases, is risk appetite is limited by regulation.

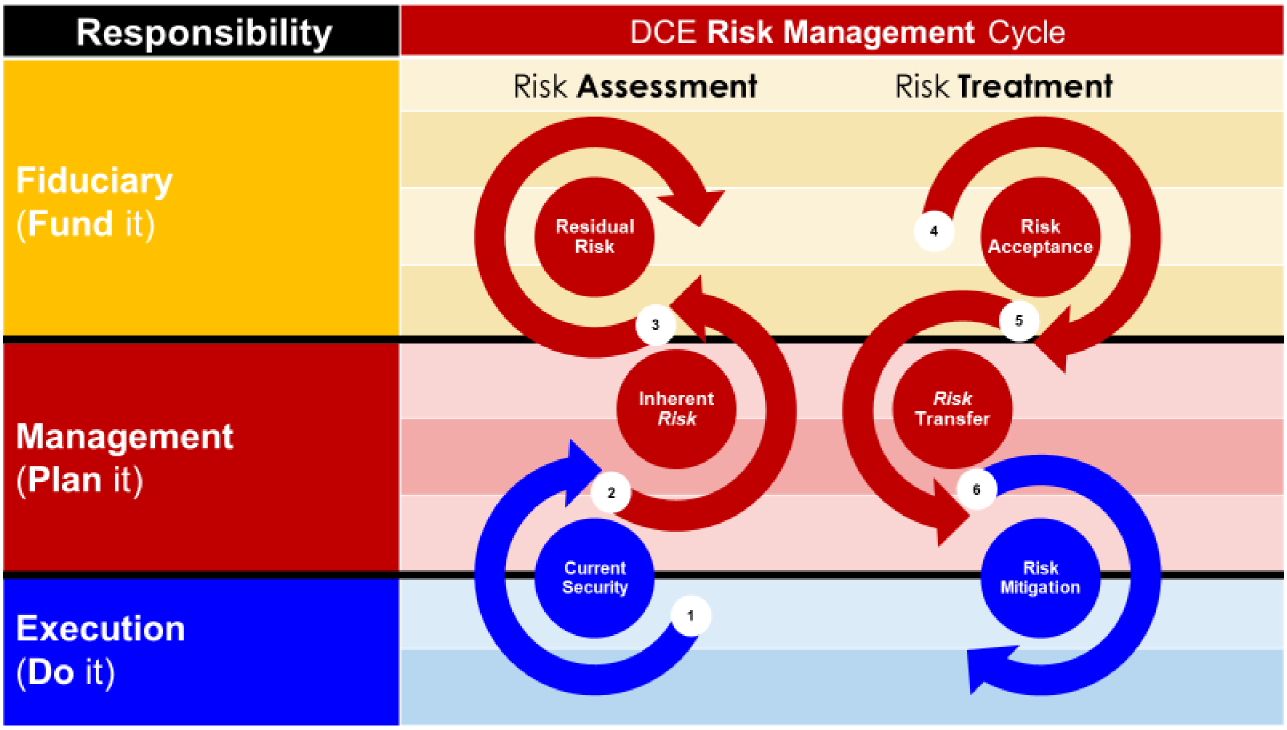


Figure 10: Stage Residual Risk Analysis Cycle

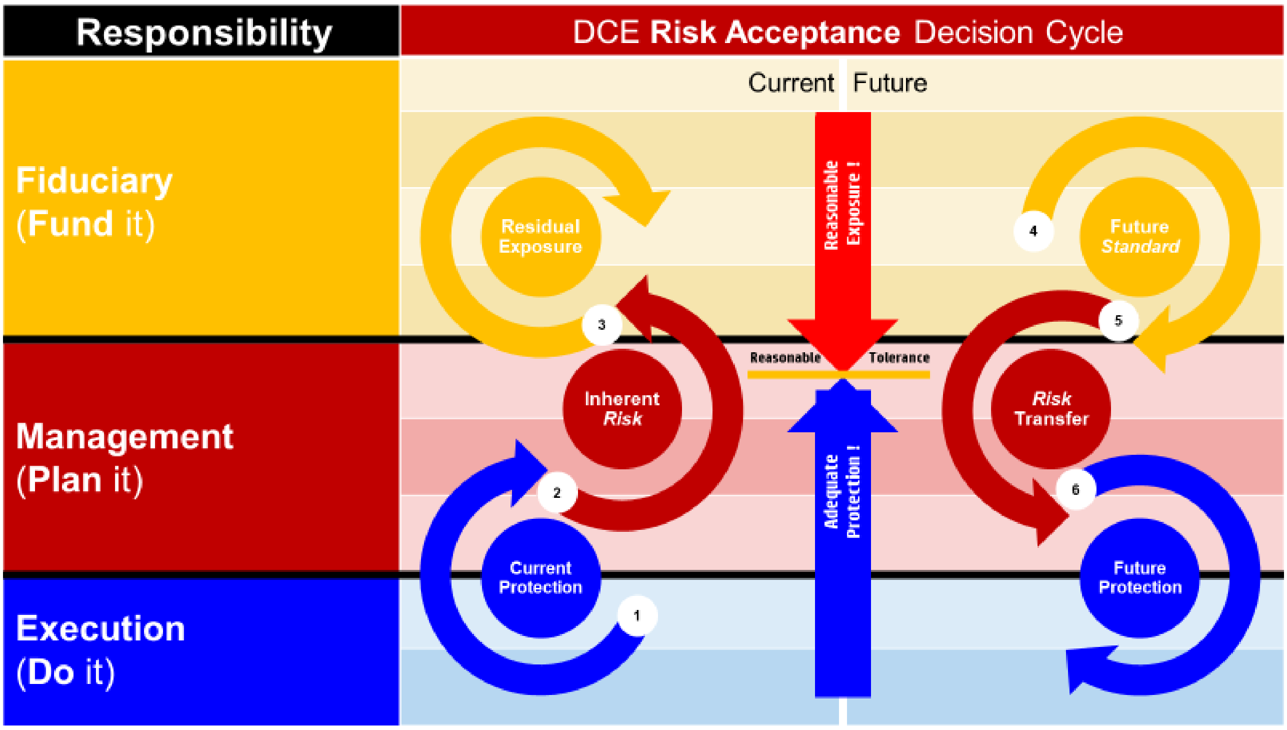


Figure 11: Reaching a Reasonable Risk Tolerance Level

4 Digital Currency Ecosystem Level 2 Target Model

DCE Level 2 Decomposition

Each of the 5 stages of the DCE Level 1 Decomposition illustrated in Figure # is further decomposed into Level 2. The objective of the decomposition is to identify and define the role of People, Process and Technology in each stage of the DCE, in both a centralized and decentralized issuance model.

The following sections discuss the logic behind how each stage was decomposed and the identification of who or what does what when to whom or what and why?

4.1 DCE Stage 1: Technology Level 2 Decomposition

The design and manufacture of DC issuance technology involves a complex supply chain comprised of People, Process, Technology and knowledge in individual streams. Figure 12 outlines a supply chain model based on the convergence and interaction of people performing processes to design and manufacture technology as follows:

- People Supply Chain: People involved in all stages of the design, manufacture and delivery of a Trusted Digital Currency Issuance System ("DC Technology"). This includes system design, manufacture of hardware, development of software and component integration and testing.
- Process Supply Chain: People design and execute processes and procedures necessary for the creation of DC Technology and its subsequent use to ensure trust as follows:
  - DC Technology Manufacturing Processes: Manufacture of hardware components, development of software and APIs and integration of all system components.
  - DC Technology Use Processes Activation, issuance and management of the DC. This is covered in stage 2.
- Technology Supply Chain: the DC Technology will involve the integration of many technologies embodied in hardware, firmware, that is mass produced for multiple uses. It is important to ensure all the components that comprise the trusted system are trustworthy.

This stage would not exhibit any "security technique" distinction whether used in the issuance of Centralized Digital Currency (CDC) or Decentralized Digital Currency (DDC). However, these issuance models may call for security assurance distinctions, that is CDCs as in the case of DFC should have a higher standard of security.

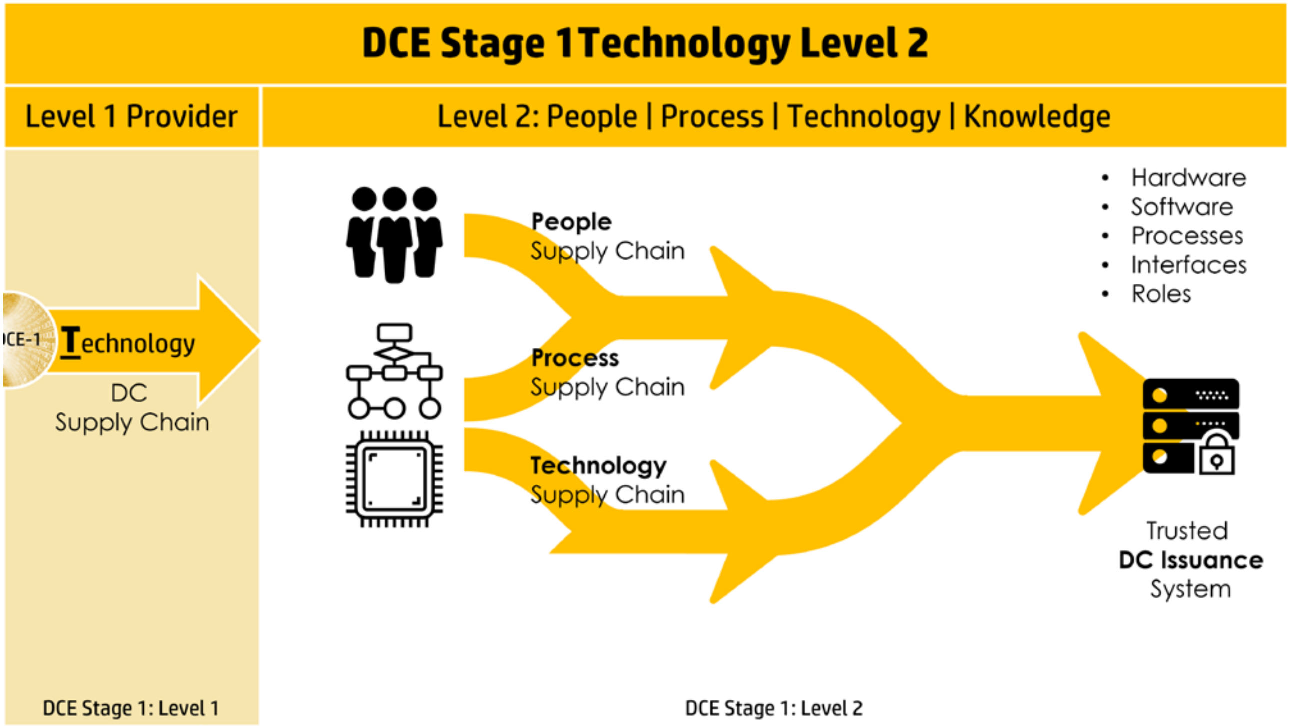


Figure 12: DCE Stage 1 Technology Level 2 Decomposition

Supply chain security best practices exist as a specialization for example, the supply of hardware and software to the government. Such a required certification includes Common Criteria v3.1 r5 for supply chain hardware and software security: Common Criteria for IT Security Evaluation (ISO/IEC 15408).

4.2 DCE Stage 2: Issuance Level 2 Decomposition

The issuance of DCs can take on two possible models;

- Centralized Issuance is where a single entity controls all aspects of the issuance of DC process, referred to as Centralized Digital Currency (CDC). Two uses cases within this category are: Digital Fiat Currency and Central Bank Digital Currency.”
- Decentralized Issuance is where participants each individually can issue DC under identical conditions, referred to as Decentralized Digital Currency (DDC).

Issuance models for both issuance cases are as follows:

4.2.1 DCE Stage 2: Centralized DC Issuance

The stage 2 decomposition of Issuance following a centralized Issuance Authority modifies the DCE model into a Centralized Digital Currency (CDC) model, as illustrated in Figure13. Digital Fiat Currency (DFC) falls into this category. The level 2 CDC issuance involves:

- CDC Stage 2.1: Procure involves the identification, procurement and delivery of the certified DFC Technology
- CDC Stage 2.2: Activate involves the setup and activation of the DFC Technology to yield a trusted state ready for issuance.

- CDC Stage 2.3: Issue involves the actual creation of the volume of DFC involved in the intended issuance.
- CDC Stage 2.4: Monitor involves monitoring the activity (velocity) of the DFC

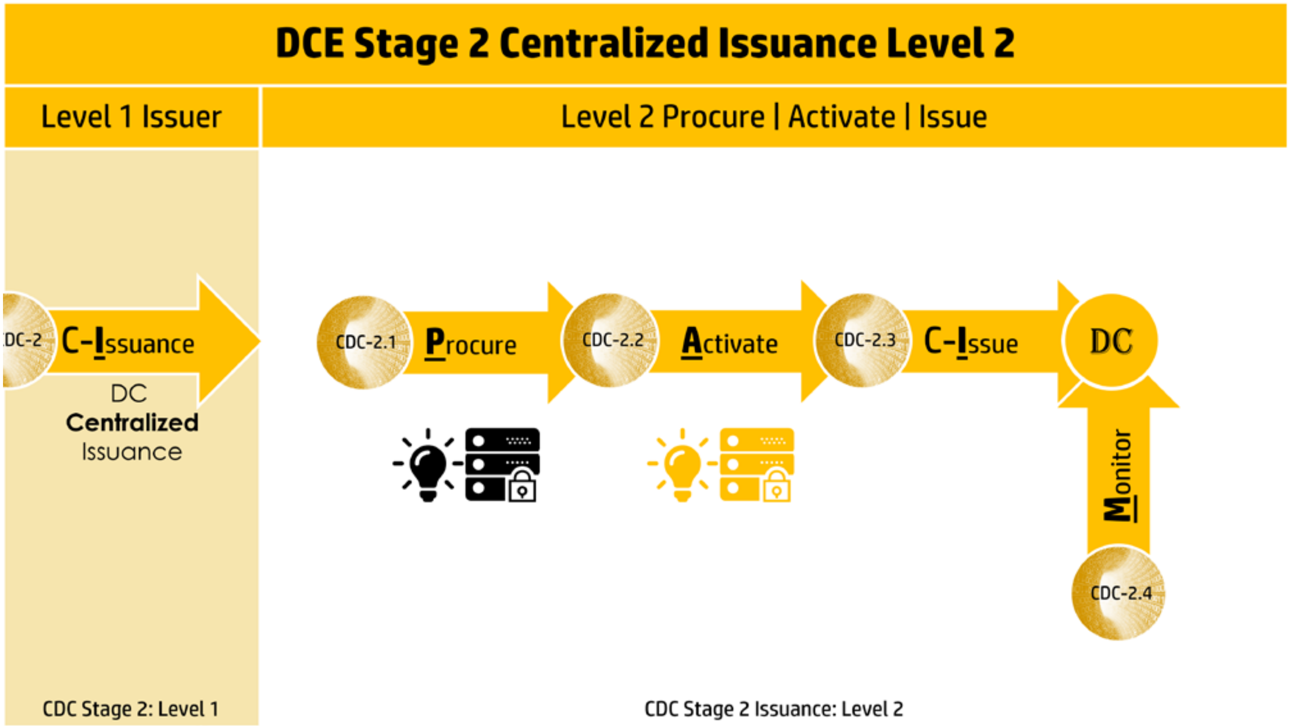


Figure 13: DCE Stage 2 Centralized Issuance Level 2 Decomposition

The following are the people, process and technology involved in centralized DC issuance: Involves the procurement, set-up and activation of all hardware, software, and processes involved in the issuance of DFC and monitoring its liquidity and transaction activity.

The CDC Stage 2 level 3 decomposition results in the following People, Process & Technology

- CDC People & Roles:
  - Procure: ensure the selection of certified DC Technology
  - Activate: trusted individuals involved in the DC issuance event
  - Issue: persons required to initiate and complete issuance
    - Trusted Issuance Participants
    - Ceremony Master (CM)
    - Internal Witness(s) (IW)
    - External Witness(s) (EW)
    - Security Officer (SO)
    - Operations Officer (System Admin)
- CDC Process: processes to acquire, activate and issue DC.
  - Procure: processes involved in the selection and evaluation of DC Technology
  - Activate: processes involved in the DC issuance event
  - Issue: process of issuance

- The assembly of Hardware & Applications.
- Root Key Generation Process
- Secure Storage Process
- Root Key Ceremony Process

- CDC Technology: technology both hardware and software are used to issue a unit of DC.
    - Procure & Activate:
        - Trusted DFC Hardware
            - Root Key Hardware Security Module (HSM)
            - Secure Laptop (Operations Officer)
        - Trusted DFC Software | Services | Applications
            - Credential Management Services
            - Trusted Time Services
        - Trusted DFC Interfaces

4.2.2 DCE Stage 2: Decentralized Issuance

The Stage 2 decomposition of Issuance following a decentralized Issuance Authority modifies the DCE model into a Decentralized Digital Currency (DDC) model, as illustrated in Figure 14. The level 2 decentralized issuance involves multiple nodes where each node has the same capability to issue DC, where a Distributed Ledger Technology validates and tracks all DC issuances.

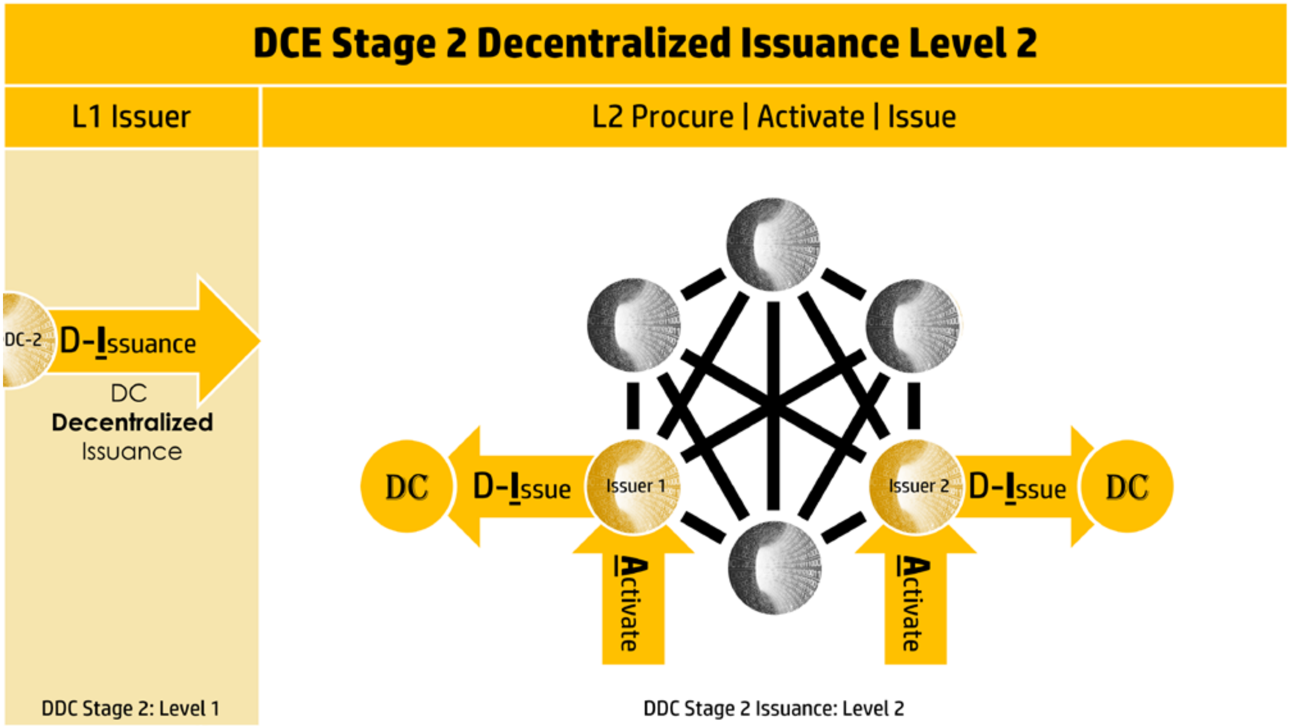


Figure 14: DDC Stage 2 Decentralized Issuance Level 2 Decomposition

On the basis that each node has identical issuance capabilities, one capability is comprised of the following components representing a level 3 decomposition.

The DDC Stage 2 level 3 decomposition results in the following People, Process & Technology

- DDC People & Roles:
    - Procure: ensure the selection of certified DC Technology
    - Activate: trusted individuals involved in the DC issuance event
    - Issue: persons required to initiate and complete issuance
- DDC Process: processes to acquire, activate and issue decentralized DC?
    - Procure: processes involved in the selection and evaluation of DC Technology
    - Activate: processes involved in the DC issuance event
    - Issue: process of issuance
- DDC **Technology**: technology both hardware and software are used to issue a unit of DC?
    - Procure
    - Activate
    - Issue

4.3 DCE Stage 3: Liquidity Level 2 Decomposition

In the previous stage, DC issuance was either a CDC or DDC model. These two DCs types are issued into a network of nodes, each representing a function and value in the ecosystem. It is assumed the Liquidity stage in where the DC is distribution must remain segmented into the centralized and decentralized models. Consequently, the following will outline a semi-centralized and decentralized distribution model where the DC circulates in a semi-pure peer-to-peer network or a pure Peer to Peer network, respectively.

4.3.1 DCE Stage 3: Centralized Digital Currency Liquidity

Figure 15 illustrates a centralized post-issuance distribution model based on a semi-full peer-to-peer network where participants differ significantly in degree-of-centralization and role. In this case, some participants play a centralized distribution function (C), distributing DC to other participants.

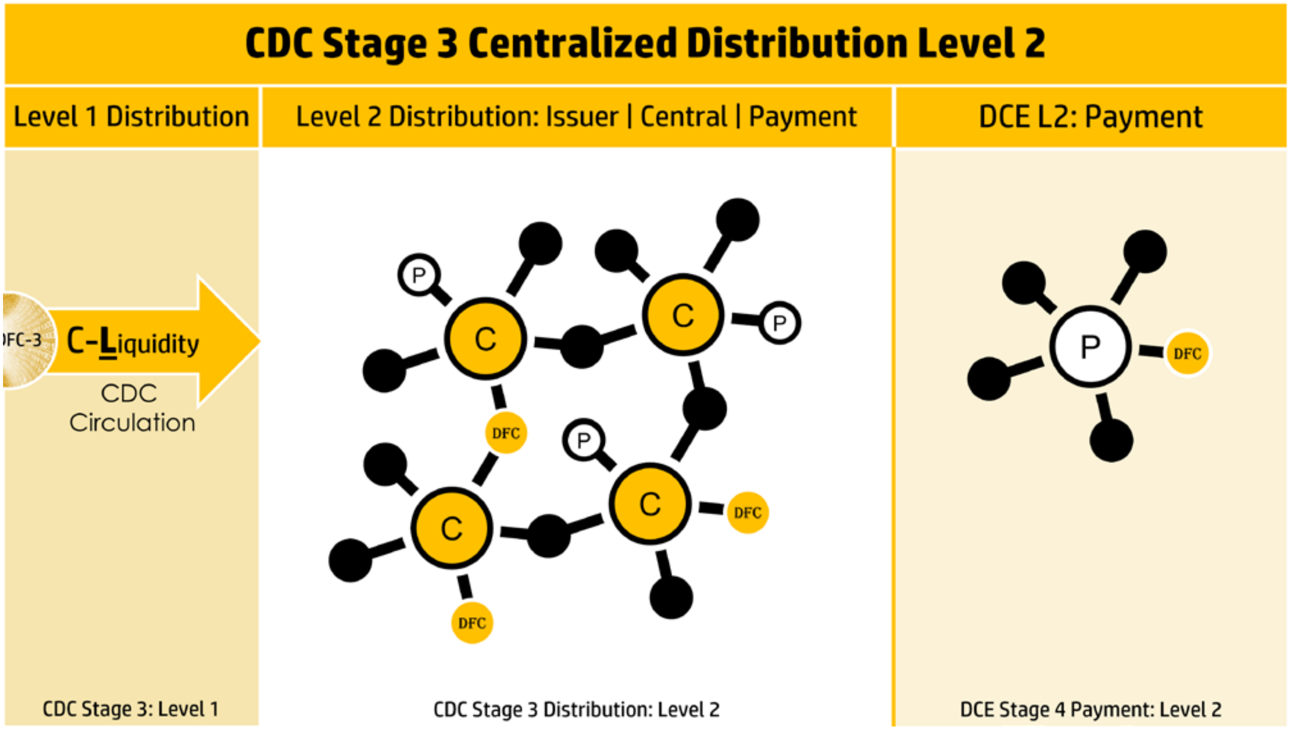

CDC Stage 3 Centralized Distribution Level 2
Level 1 Distribution
Level 2 Distribution: Issuer | Central | Payment
DCE L2: Payment
FC-3
C-Liquidity
CDC
Circulation
P
C
DFC
CDC Stage 3: Level 1
CDC Stage 3 Distribution: Level 2
DCE Stage 4 Payment: Level 2

Figure 15: CDC Stage 3 Centralized Distribution Level 2

The CDC Stage 3 level 3 decomposition results in the following People, Process & Technology

- People:
- Process: software applets and applications involved in the execution of centralized distribution
- Technology:

4.3.2 DCE Stage 3: Decentralized Digital Currency Liquidity

Figure 16 illustrates a decentralized post-issuance distribution model based on a full peer-to-peer network where participants do not differ in capability but may differ in roles. In this case, all participants execute common functions in a distributed manner.

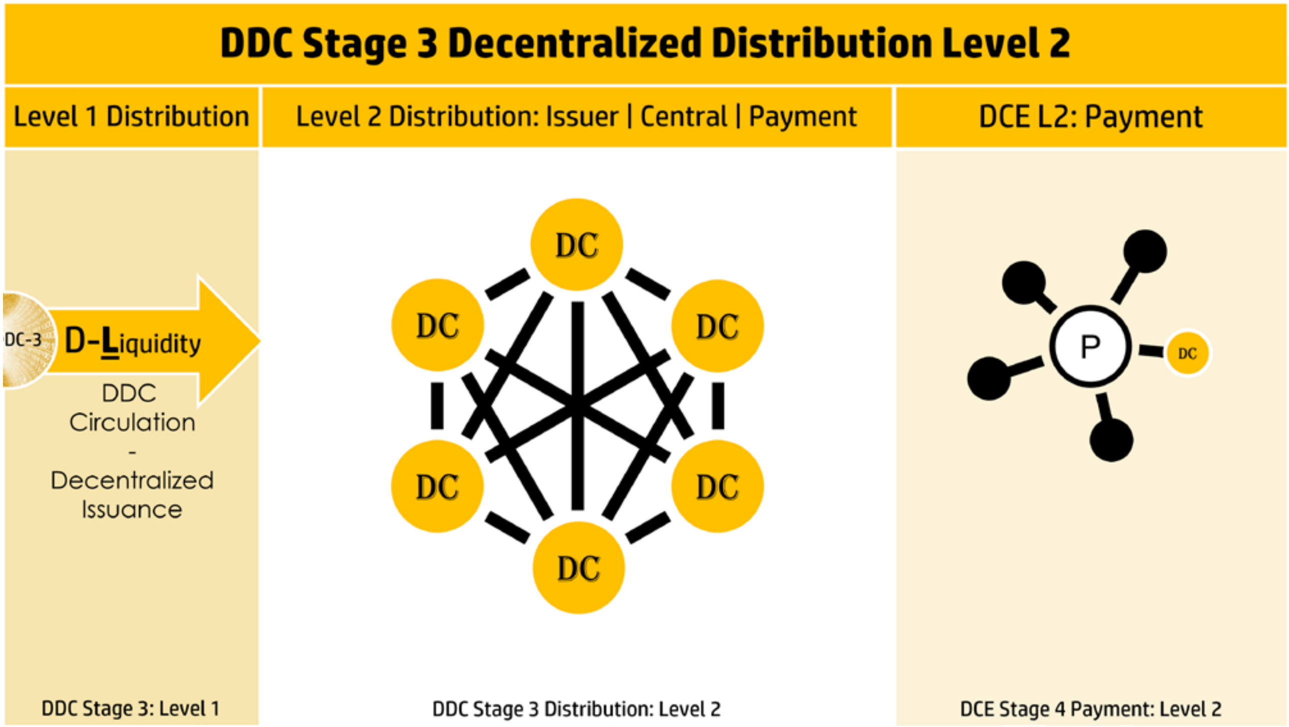

DDC Stage 3 Decentralized Distribution Level 2
Level 1 Distribution
Level 2 Distribution: Issuer | Central | Payment
DCE L2: Payment
DC-3
D-Liquidity
DDC Circulation - Decentralized Issuance
DC
DC
DC
DC
DC
DC
P
DC
DDC Stage 3: Level 1
DDC Stage 3 Distribution: Level 2
DCE Stage 4 Payment: Level 2

Figure 16: DDC Stage 3 Decentralized Distribution Level 2

The DDC Stage 3 level 3 decomposition results in the following People, Process & Technology

- People:
- Process: software applets and applications involved in the execution of distribution functions
- Technology:

4.4 DCE Stage 4: Payment Level 2 Decomposition

Figure 17 represents payment gateway providers (P) that execute transactions between Owners involved in value exchanges involving DC. This stage does not differ whether CDC and DDC is used in the value transfer.

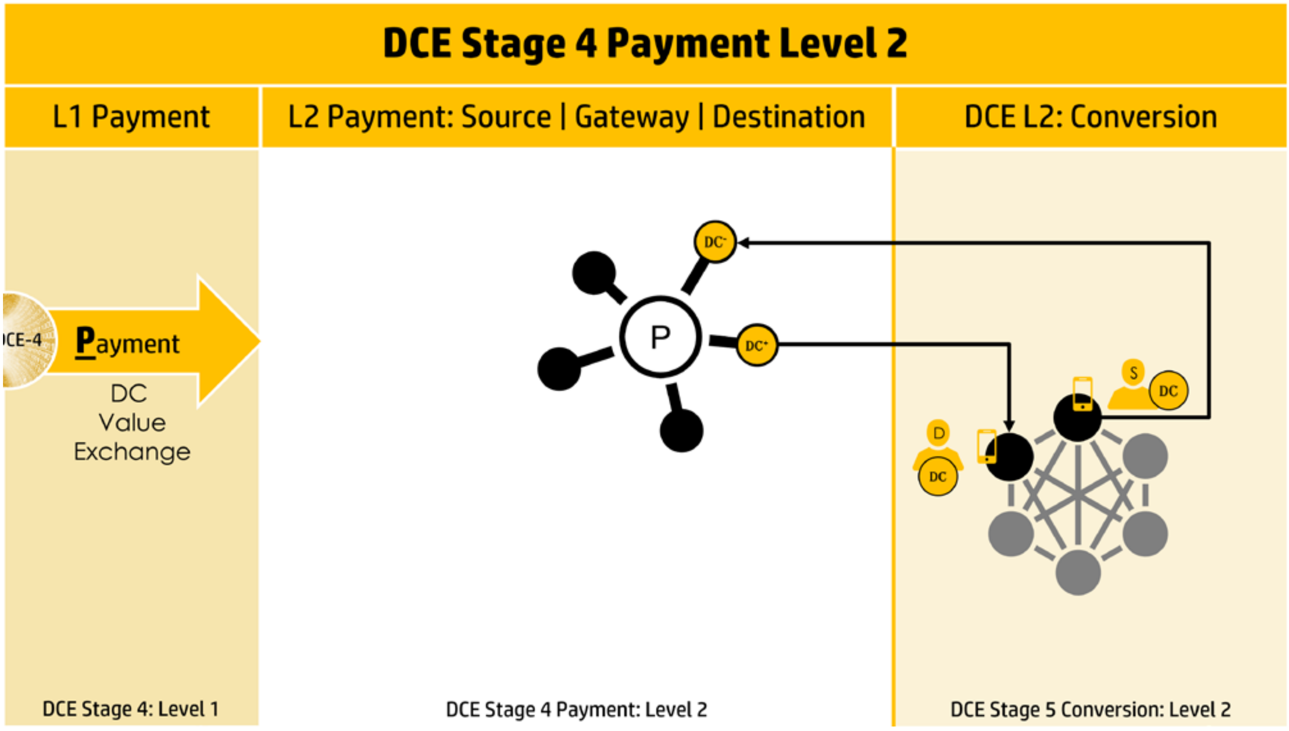

DCE Stage 4 Payment Level 2
L1 Payment
L2 Payment: Source | Gateway | Destination
DCE L2: Conversion
CE-4
Payment
DC
Value
Exchange
P
DC-
DC+
D
DC
$
DC
DCE Stage 4: Level 1
DCE Stage 4 Payment: Level 2
DCE Stage 5 Conversion: Level 2

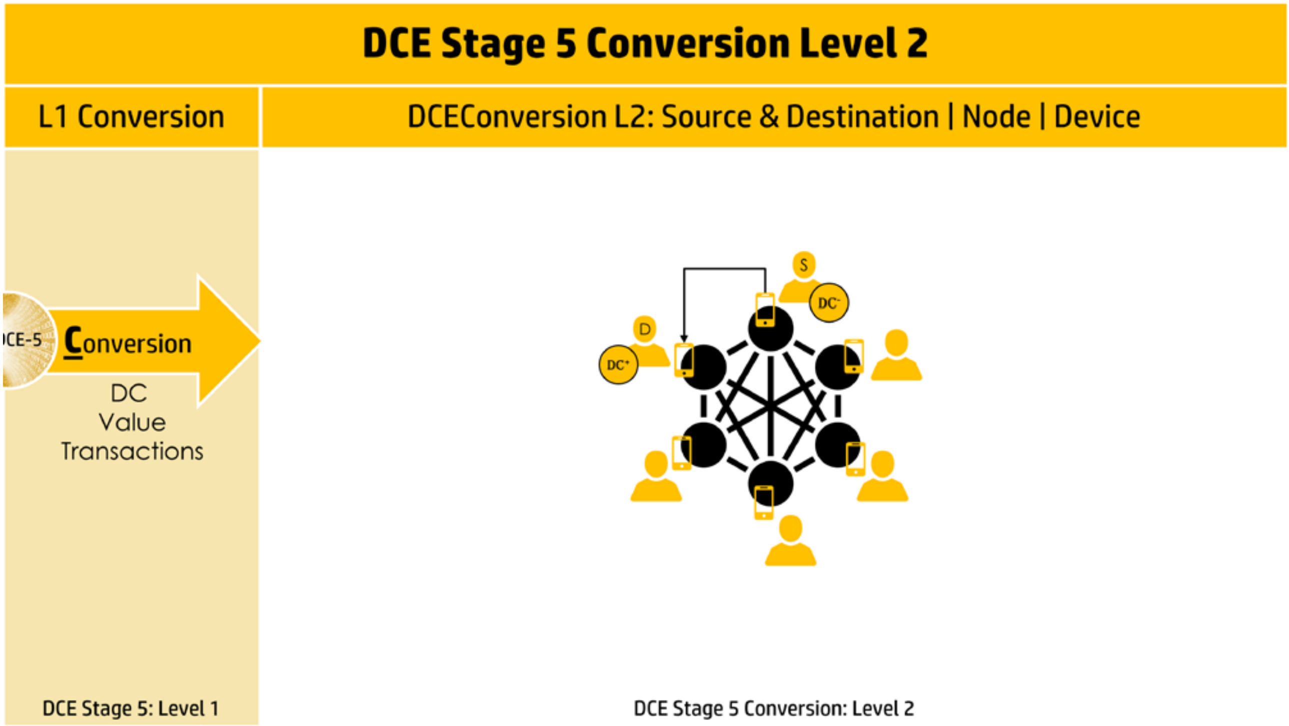
Figure 17: DCE Stage 4 Payment Level 2

The DCE Stage 4 level 3 decomposition results in the following People, Process & Technology

- People: Payment Gateway Provider
- Process: software applets and applications involved in the execution transactions
- Technology:

4.5 DCE Stage 5: Conversion Level 2 Decomposition

Figure 18 illustrates a pure peer-to-peer network of Owners exchanging value using DC. This model assumes no distinction in conversion whether the DC is CDC or DDC.



DCE Stage 5 Conversion Level 2

L1 Conversion

DCEConversion L2: Source & Destination | Node | Device

Figure 18: DCE Stage 5 Conversion Level 2

The DCE Stage 5 level 3 decomposition results in the following People, Process & Technology

- People: Owner. An Owner can be a source of DC or a receiver of DC, as illustrated in Figure 10.
- Process: software applets and applications involved in the coordination of nodes, execution of transactions, exchanges,
  - Consensus Algorithms such as Proof of Work and Proof of Stake.
- Technology:
  - A Device under the sole control of the Owner.
  - A Wallet application managing the DCs under control of the Owner and the execution of transactions initiated by Owner.

4.6 Centralized and Decentralize Digital Currency Models

Figure 19 illustrates the DCE model in its two fundamental forms – CDC and DDC. This DCE model assumes that only DCE Stage 2 and 3 change due to the different in issuance – centralized and decentralized.

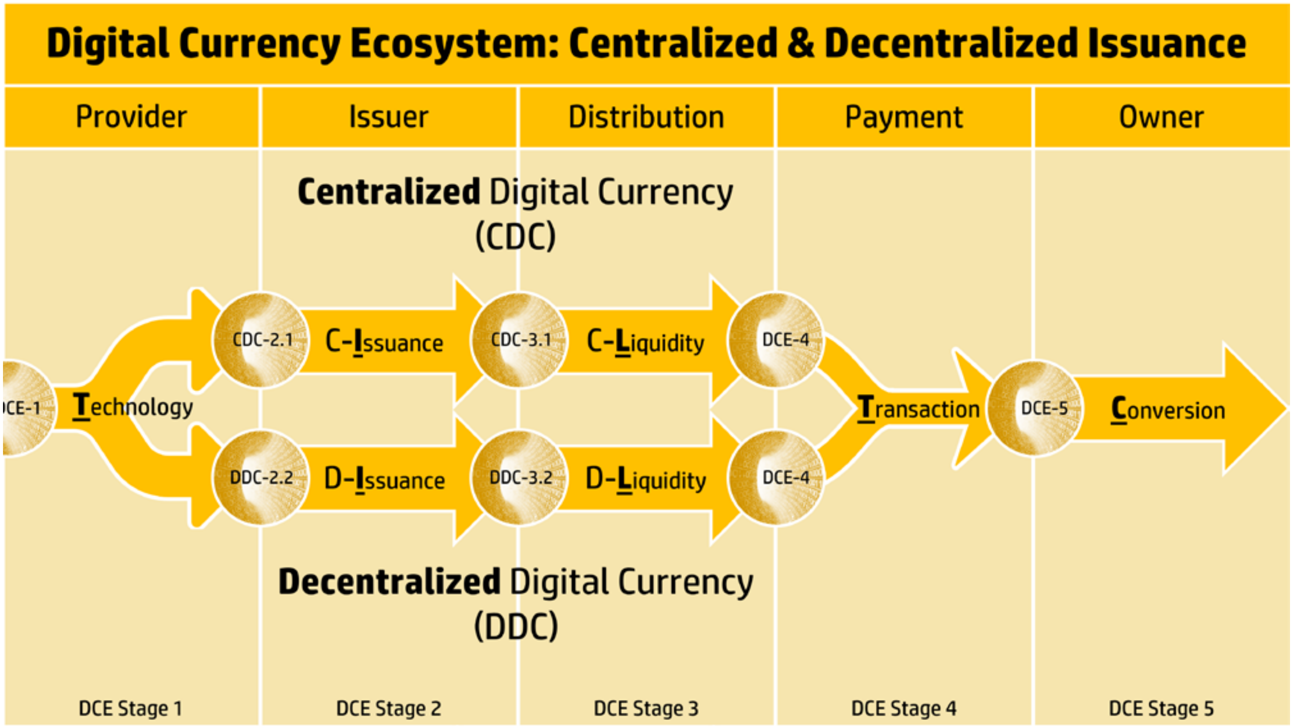
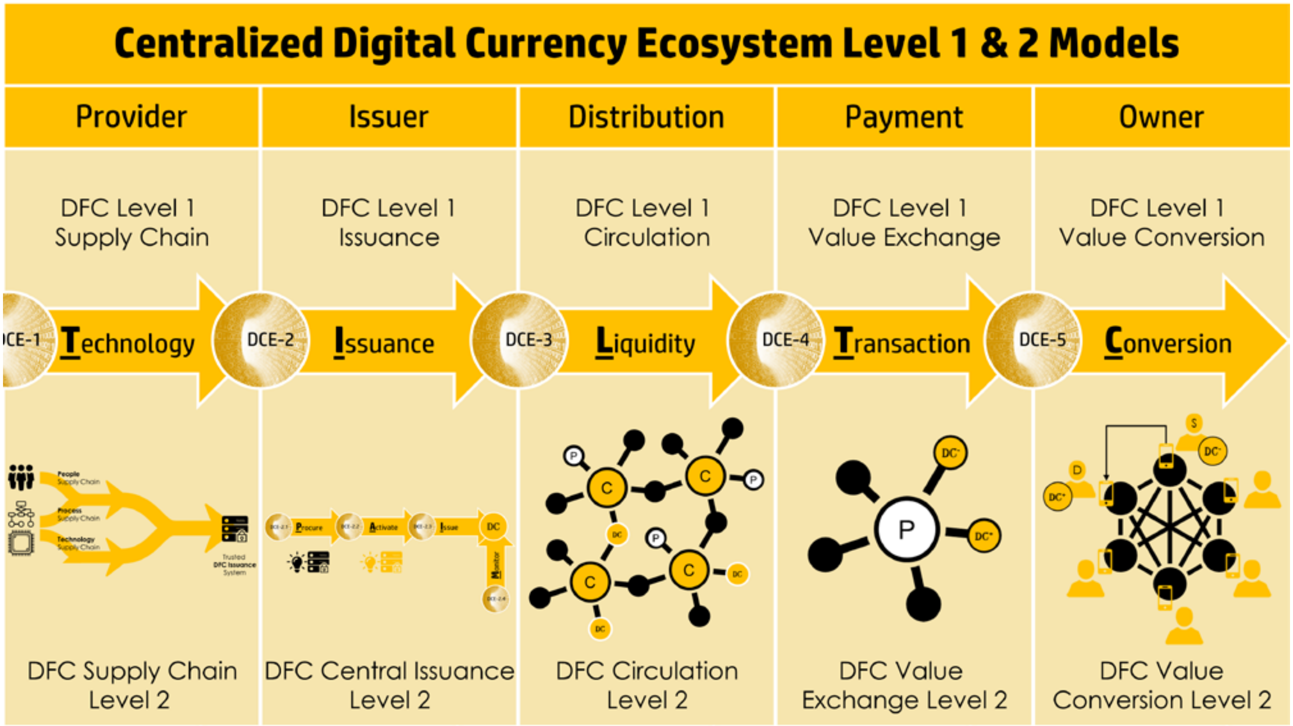


Figure 19: DCE Model as Centralized and Decentralized Digital Currency Models

4.6.1 Centralized Digital Currency Ecosystem

Figure 20 illustrates the level 1 and 2 of the centralized Digital Currency Ecosystem model referred to as Centralized Digital Currency (CDC).



Centralized Digital Currency Ecosystem Level 1 & 2 Models

Provider	Issuer	Distribution	Payment	Owner
DFC Level 1 Supply Chain	DFC Level 1 Issuance	DFC Level 1 Circulation	DFC Level 1 Value Exchange	DFC Level 1 Value Conversion
DCE-1 Technology	DCE-2 Issuance	DCE-3 Liquidity	DCE-4 Transaction	DCE-5 Conversion
DFC Supply Chain Level 2	DFC Central Issuance Level 2	DFC Circulation Level 2	DFC Value Exchange Level 2	DFC Value Conversion Level 2

Figure 20: Centralized Digital Currency Ecosystem Level 1 & 2 Model

4.6.2 Decentralized Digital Currency Ecosystem

Figure 21 illustrates the level 1 and 2 of the decentralized Digital Currency Ecosystem model referred to as Decentralized Digital Currency (DDC).

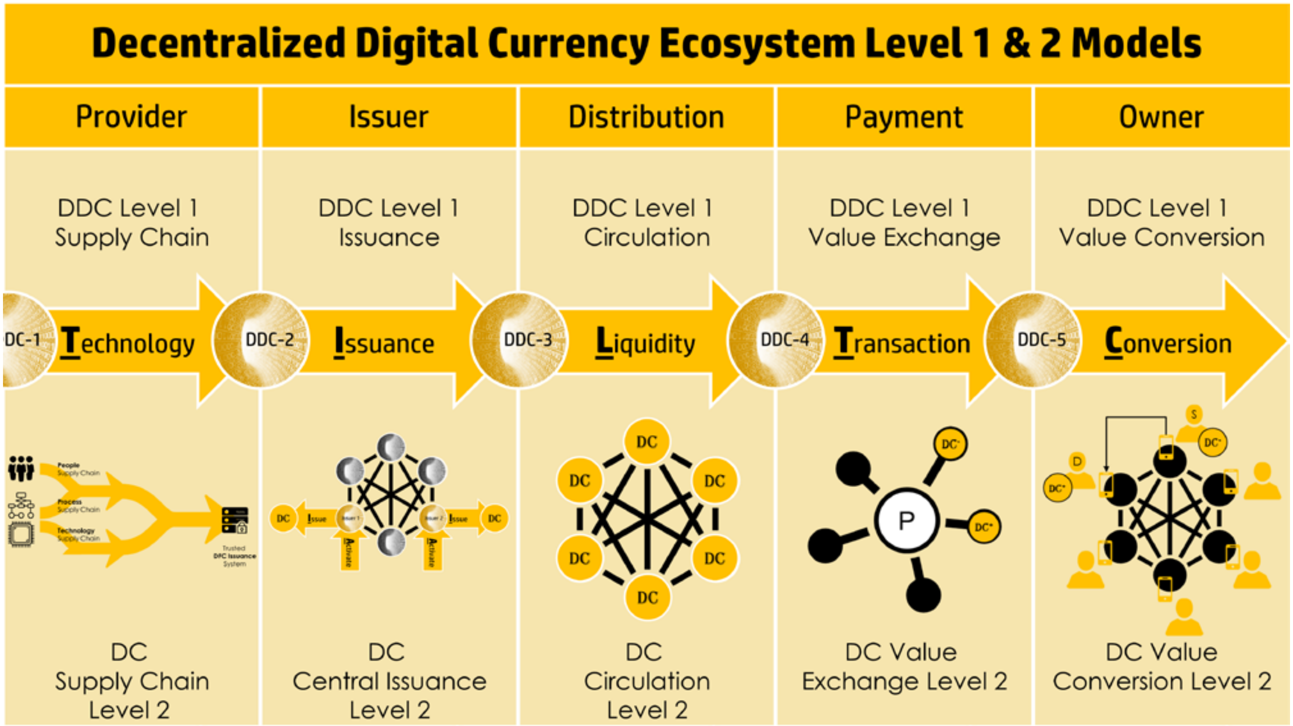


Figure 21: Decentralized Digital Currency Ecosystem Level 1 & 2 Model

5 Protection Assurance Model

The Protection Assurance Model (PSM) is constructed from a number of smaller constructs, as follows and illustrated in Figure 22:

- **Security Control Expression** (SCE) - a defined relationship between “security delivered” by Security Assets and “protection received” by Business Assets. Expressing any security control explicitly and unambiguously. Top of Figure 22
- **Threat Attack Expression** (TAE) - a relationship between a Threat Attack Vector and Business Assets. Expressing Protection of Target and Threat to Target, explicitly and unambiguously. 2nd from top of Figure 22
- **Threat Target Security Expression** (TTSE)– the integration of SCE and TAE with a common Target. Expressing Protection of Target, Threat to Target, explicitly and unambiguously as one construct. 3rd from top of Figure 22
- **Protection Assurance Expression** (PAE)– the integration TTSE with the addition of a Target Protection attack vector yielding a security assurance model delivering Protection with high confidence. Expressing Protection of Target, Threat to Target & Threat to Target Protection, explicitly and unambiguously as one construct.
  Bottom of Figure 22.

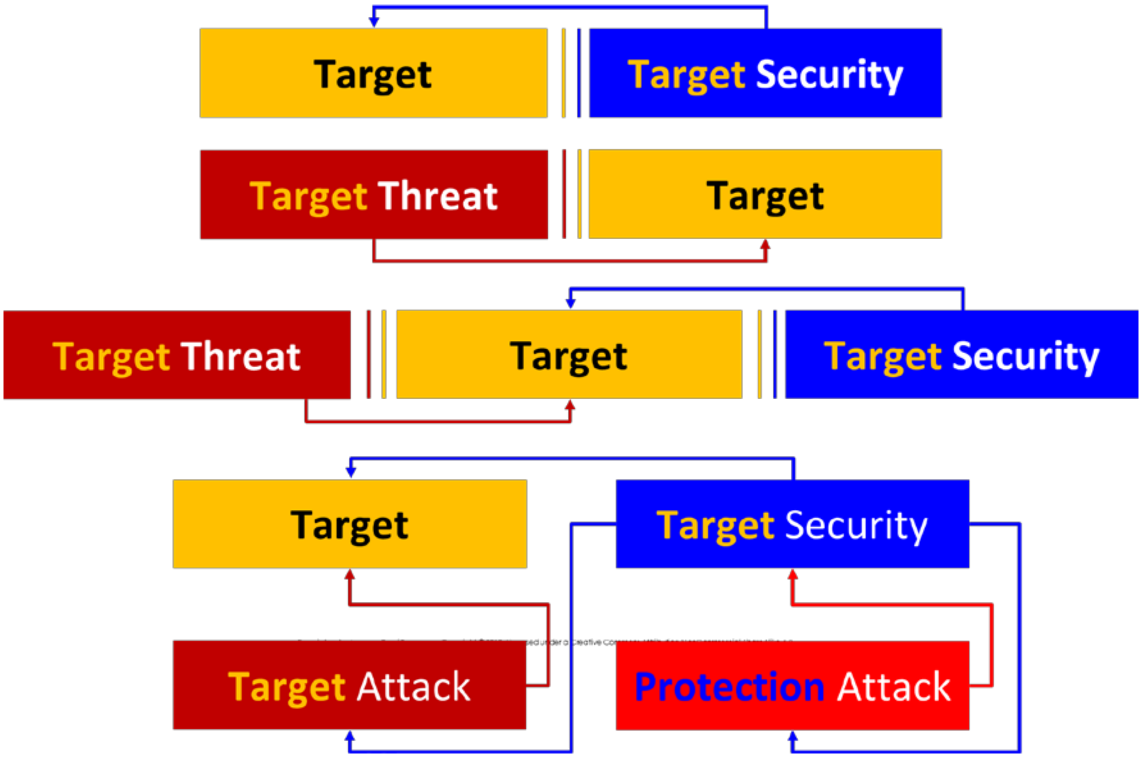
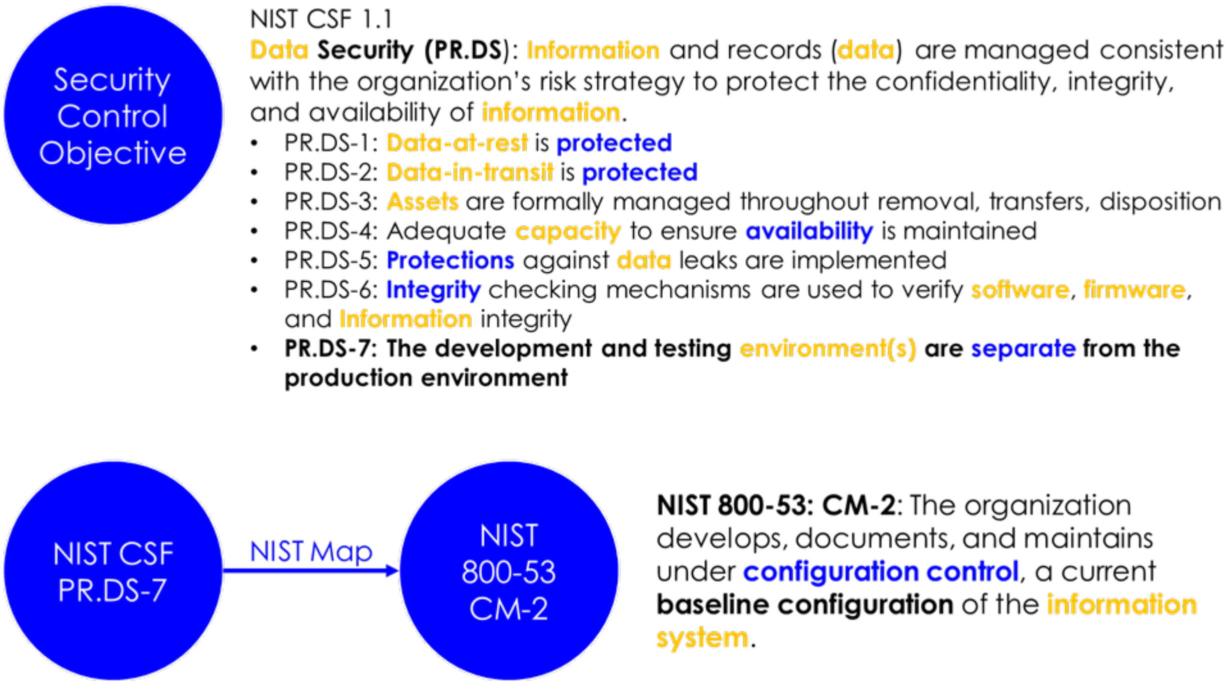


Figure 22: Four Expression Models: Top to bottom Security Control Expression, Threat Attack Expression, Threat Target Security Expression and Protection Assurance Expression.

5.1 Security Control Expressions

Security Standards and Regulations are de-compositional frameworks composed of statements of one or more security objectives. A typical security control is illustrated in Figure 23 where the cited target and protection requirements are highlighted.



NIST CSF 1.1
Data **Security (PR.DS)**: Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

- PR.DS-1: Data-at-rest is **protected**
- PR.DS-2: Data-in-transit is **protected**
- PR.DS-3: Assets are formally managed throughout removal, transfers, disposition
- PR.DS-4: Adequate capacity to ensure **availability** is maintained
- PR.DS-5: **Protections** against data leaks are implemented
- PR.DS-6: **Integrity** checking mechanisms are used to verify software, firmware, and Information integrity
- **PR.DS-7: The development and testing environment(s) are separate from the production environment**

NIST 800-53: CM-2: The organization develops, documents, and maintains under **configuration control**, a current **baseline configuration** of the information system.

Figure 23: Current Security Control Objective and NIST CSF to NIST 800-53 Mapping

When an Objective is reviewed with the goal of fulfilling it, a natural decomposition process begins to occur: In Figure 23, PR.DS-1 and 2 simply states: Data at rest and in motion should be protected. The receiver of the security is Data. The device storing the data is either a database or repository. The most likely protection function to be applied to the Data in is encryption. Is PR.DS-5 not satisfied by 1 and 2?

We individually break down the Objective into what we think it requires, we then seek to have one's interpretation validated internally and verified by external auditors. This is a painful process.

A security control inter-framework mapping is a mapping between Objectives originating from different control frameworks. It is a commonality claim. It is a statement that there is some degree of "coverage" or overlap between the two mapped Objectives. This represents the current industry state of maturity of security control modeling.

The following proposes a security control model called "Security Control Expressions."
It greatly improves the clarity of articulating what security is being provided to what assets – uniquely and unambiguously.

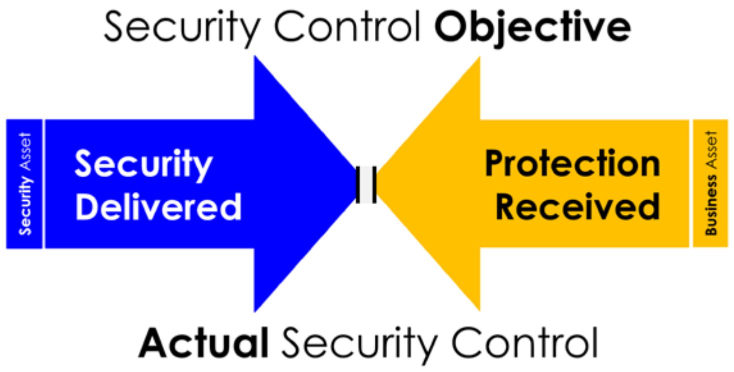


Figure 24: General Security Control Model

What is a Security Control Objective (“Objective”) versus an actual implemented control (“Control”)? An Objective is generally defined in technique or method neutral terms while an actual control is defined to environment specific protocol terms. An Objective is subject to interpretation as to how it can be fulfilled.

A General Security Control model is illustrated in Figure 24. It depicts any form of security value being “delivered” by a Security Asset to a Business Asset as protection received. Protection received is not necessarily the same as security delivered, as indicated by the double center lines in Figure 24.

The Control model in Figure 24 can be decomposed into a “mirror” model illustrated in Figure 25 as both sides of the relationship are identical at the underlying code | data | device level.

- Security Delivered is achieved by security software executing with security data from a secure source.
- Protection Received is delivered to business software operating business data executing on a host.

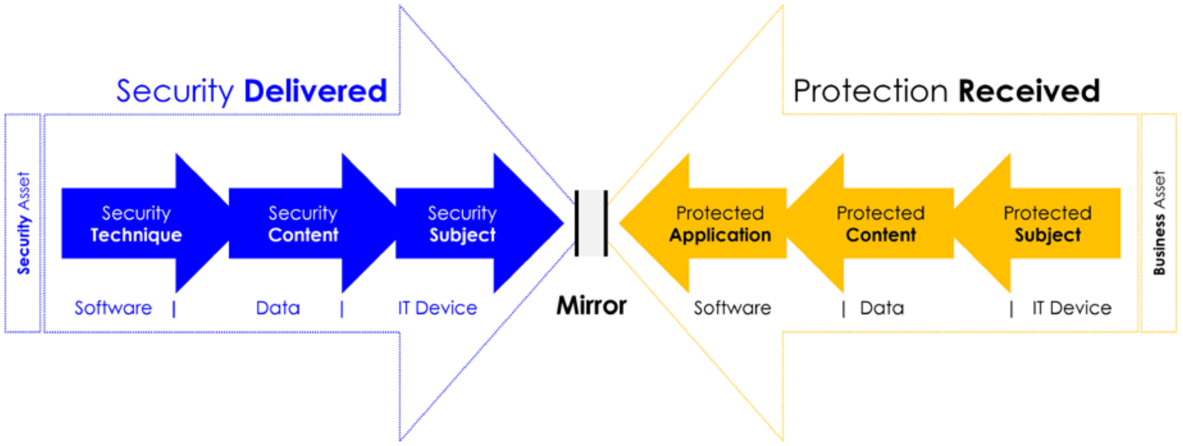


Figure 25: Decomposing Security Delivered & Protection Received

The model discussed in Figure 25 can be replaced by the block model of Figure 26.

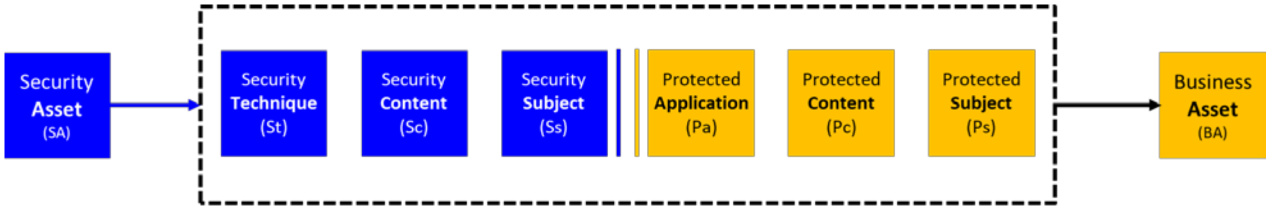


Figure 26: General Security Control Block Model

Figure 27 defines the Security Control Expression (“Expression”) model, the core subject of this paper. It outlines how to define what each security technique is delivering in the form of protection to individual business asset components.

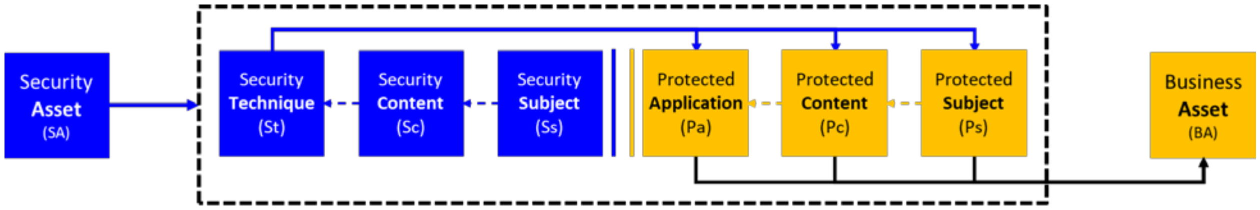


Figure 27 Security Asset delivers protection to Business Asset

An Expression illustrated in Figure 27 reads as follows:

*“**Security Delivered** is achieved by a **Security Asset** performing one or more **Security Techniques**, each technique requiring trusted **Security Content** from a trusted **Security Subject** or source”*

*“**Protection Received** by **a Business Asset** is more specifically articulated to protect either the **protected application**, the **protected content** being used by the application and/or the **protected device** the application is hosted on.”*

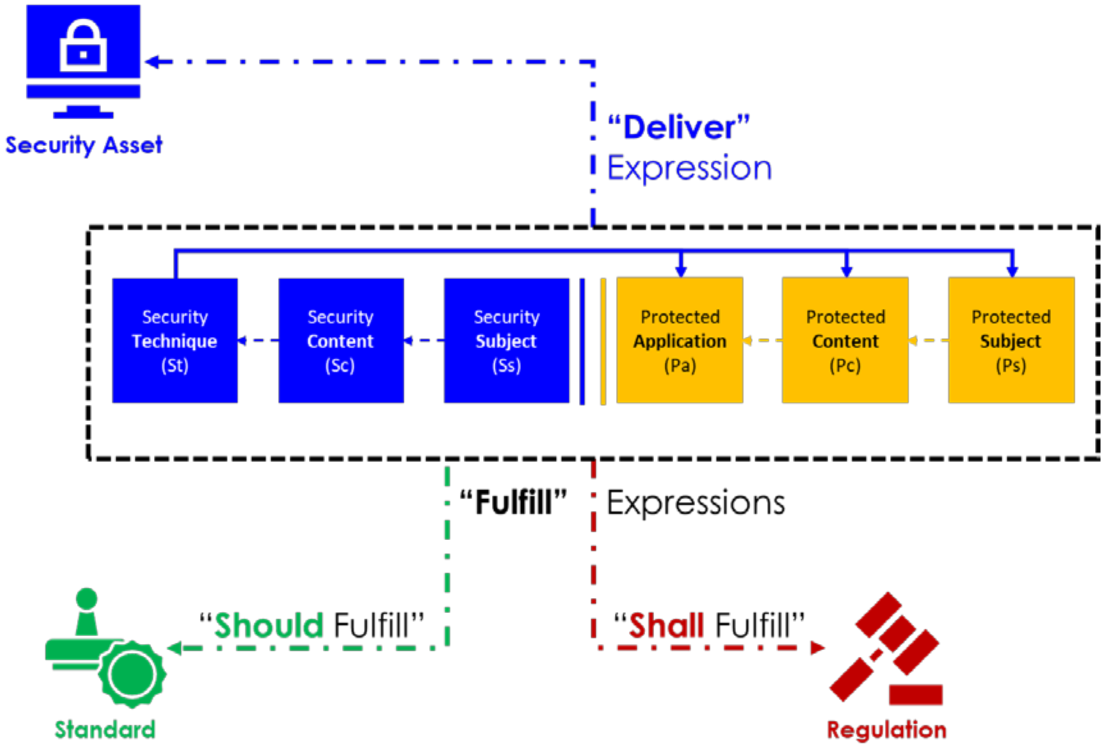


Figure 28 Expression Tense Derived by Association

A General Security Control Expression (“Expression”) is an explicit expression of what security is to be, is being, should be, or shall be delivered to what Business Asset. However, the purpose of the Expression is only realized by its association to either a regulatory or standard control objective or a security vendor product, as follows and illustrated in Figure 28.

- **Deliver** Expression: Expression is associated to a vendor security product which delivers the following one or more expressions.
- **Fulfill** Expression: Expression defines what should or shall be fulfilled
  - ***Shall*** Fulfill Expression: Expression associated to a **Standard** framework Objective.
  - ***Should*** Fulfill Expression: Expression associated to a **Regulatory** framework Objective.

A key outcome of Expressions and their associations to security products and regulatory Objectives is that:

Deliver Expressions *[available from Vendors]*
meet
Fulfill Expressions *[required by Regulators]*
- automatically

The Expression model represents a method to define to a higher level of precision the relationship between security & protection. The following Figure 29 illustrate how the Security Control Expression elements integrate into Security Asset and Business Asset inventories that deliver and preserve value.

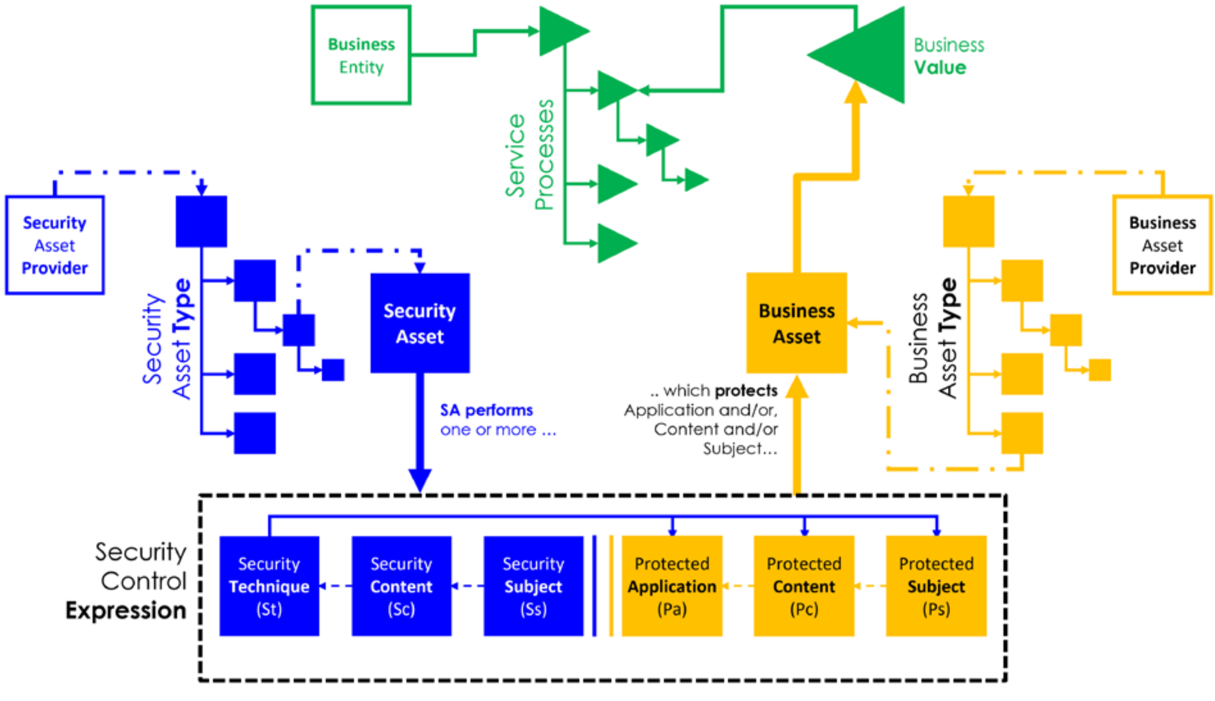


Figure 29 Security Control Expression Integrated with Security Asset & Business Asset Inventories

4.2. Threat Attack Expressions

Threat Attach Expression (TAE) builds on the construct of a Security Control Expression by taking the same Target construct and defining a threat attack vector expression that targets it. A TAE model is illustrated in Figure 30 below. TAE enables the addition of threats to the Security Control Model in Figure 2. A TAE models the following three attack stages:

- Attack **Deliver** (A_d): How the attack content is delivered to the point-of-exploitation. For example, email, USB, text link;
- Attack **Content** (A_c): this is the "content" data and/or code required to complete the exploit;
- Attack **Exploit** (A_e): this is the mechanism of exploiting a vulnerability in the Target to gain a foothold.

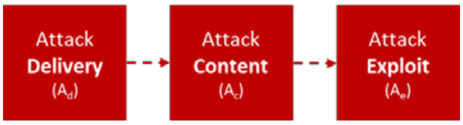


Figure 30: General Threat Attack Expression Model

An actual attack in the sense of achieving an intent, exfiltrate data for example may involve more than one Attack Exploit (A_e) each of which may involve different Attack Contents (A_c) (e.g. payloads). Attack Delivery (A_d) of the A_c may occur on the initial delivery or after external Command & Control communication is established.

The Security Control Expression model illustrated in Figure 27 is based on the distinction between security delivered and protection received. An attack can be on the target itself or on the protection being provided to the target. The Threat Attack Expression Model in Figure 30 can be nuanced into two fundamental intents, attack the target and/or attack the protection of the target, as illustrated in Figure 31. The pre-superscript indicates the target and the subscript indicates the attack stage.

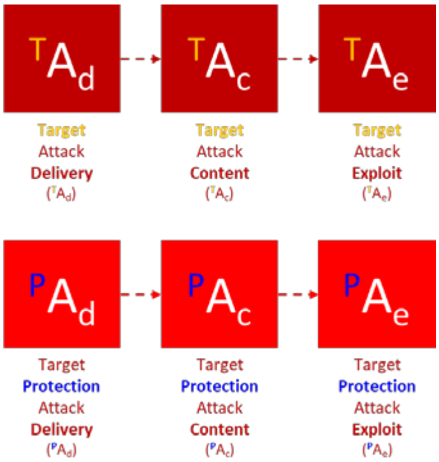


Figure 31: Target Attack Intent and Target Protection Attack Intent models

4.3. Threat | Target | Protection Assurance Expression Model

The two threat vector expression models illustrated in Figure 31 can be integrated with the Security Control and threat vectors Expression models to yield Protection Assurance Model illustrated in Figure 32.

The TTP Model has 4 zones.

- Upper left block is the **Target** which generates value.
- Upper right block **Target Security** block is where protection is provided to the **Target**;
- Lower left block is a **Threat Block** attacking the **Target**; and
- Lower right block is a **Target Attack** on the protection to the target - **Target Security**

The arrows between the blocks indicate the essential relationships:

- **Target Attack** *directed* to **Target**
- **Protection Attack** *directed* to **Target Security**
- **Target Security** *is applied to:*
  - **Target** *in the form of preventive controls such as encryption of Data*
  - *Counter* **Target Attacks** on **Targets** in the form of detective controls;
  - Counter **Protection Attacks** *to* **Target Security** also in the form of detective controls

Note the following about the model:

- Threats consider relate to both the **Target** and to the **Target Security**, yielding a high assurance model which considers the strength of the security in maintaining its protection of the Target.
- Protection is achieved by Security being applied to protect the **Target** intrinsically like encrypt the data or **Target Security** applied to detect and prevent attacks on the Target and to its protection.

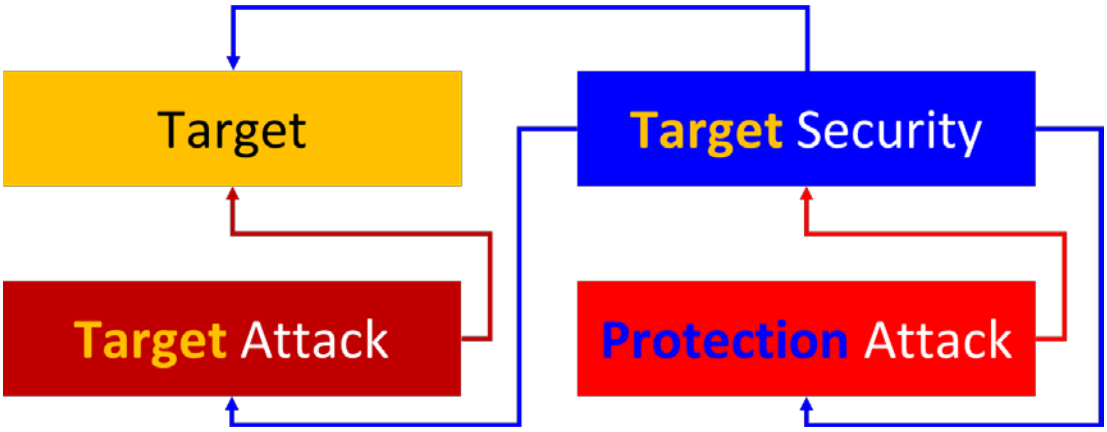


Figure 32: Threat | Target | Security Block Model

Each block in Figure 32 is decomposed into the logical constituents required to affect the purpose of each block - generate value, provide protection, execute an attack on target and/or its protection.

The Security Control Expression Model of Figure 27 is the top portion of the Protection Assurance Model of Figure 32 while the bottom portion is represented the two Threat Attack Expression models of Figure 31.

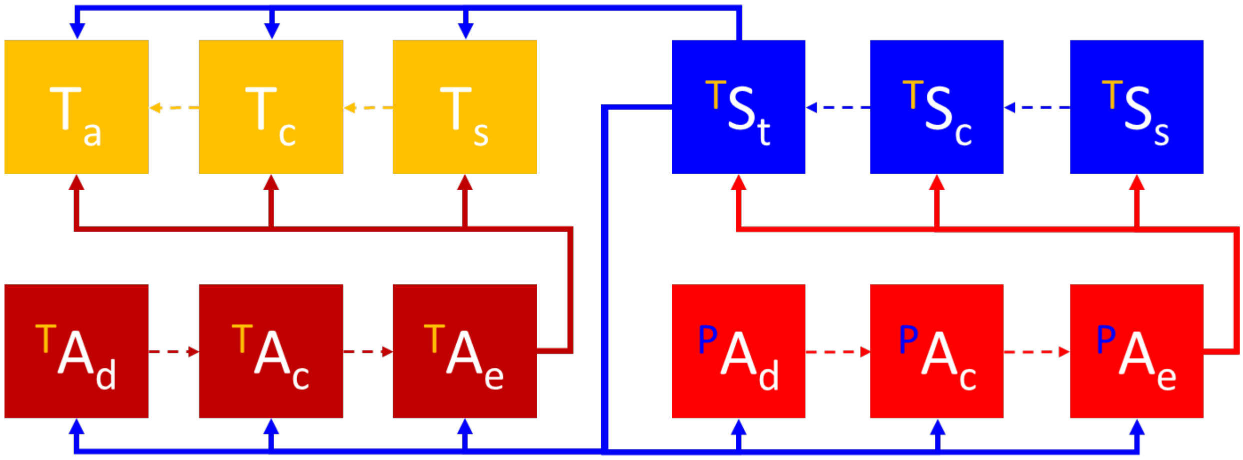


Figure 33: Threat | Target | Protection Assurance Model

The Protection Assurance Model in full text is illustrated in Figure 35 can be "read" within each of the four blocks following the dotted line and between each block following the solid lines, as follows:

- **Top Left Value Blocks**: A **business asset** is generating value by its software **Application** (**T_a**) executing as designed and intended with its business **Content** (**T_c**) and executing on an IT host **Subject** (**T_s**) each of which becomes a potential Target;
- Top Left **Value** Block protected by **Top Right Security Blocks**: Protection is delivered to a **Business Asset** by a **Security Asset** performing one or more **Security Techniques** (**$^{T}S_t$**), each technique requiring trusted **Security Content** (**$^{T}S_c$**) from a trusted **Security Source** (**$^{T}S_s$**);
- Top Left Value Blocks attacked by **Bottom Left Attack Blocks**: A **Target Attack** is executed by the **Attack Delivery** (**$^{T}A_d$**) of the **Attack Content** (**$^{T}A_c$**) to the **Attack** point of **Exploitation** (**$^{T}A_e$**);
- Top Right **Protection Blocks** attacked by **Bottom Right Attack Blocks**: A **Target Protection Attack** is executed by the **Attack Delivery** (**$^{P}A_d$**) of the **Attack Content** (**$^{P}A_c$**) to the **Attack** point of **Exploitation** (**$^{P}A_e$**).

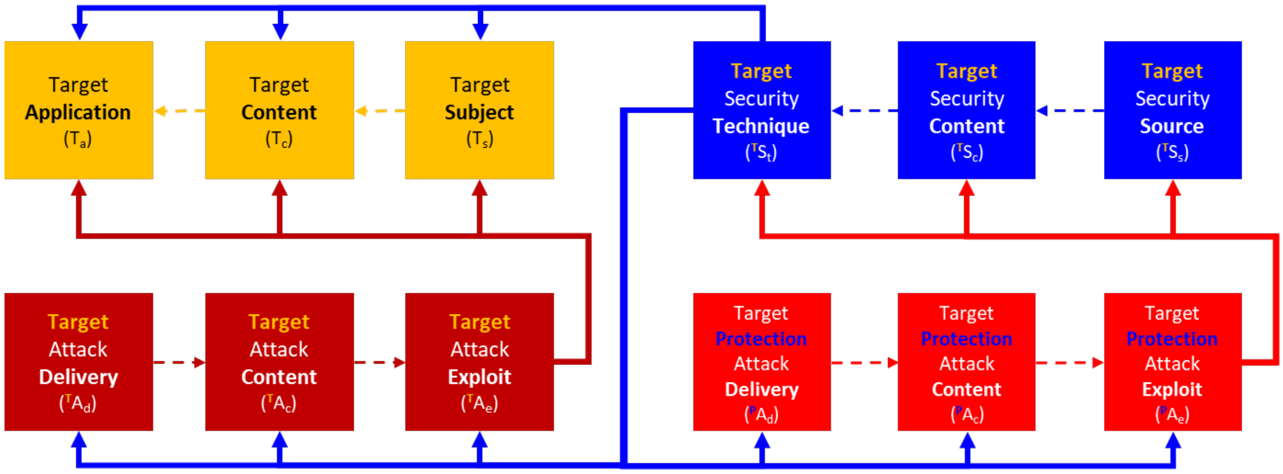

Target Application (T_a)
Target Content (T_c)
Target Subject (T_s)
Target Security Technique ($^{T}S_t$)
Target Security Content ($^{T}S_c$)
Target Security Source ($^{T}S_s$)
Target Attack Delivery ($^{T}A_d$)
Target Attack Content ($^{T}A_c$)
Target Attack Exploit ($^{T}A_e$)
Target Protection Attack Delivery ($^{P}A_d$)
Target Protection Attack Content ($^{P}A_c$)
Target Protection Attack Exploit ($^{P}A_e$)

Figure 34: Threat | Target | Protection Model in Full Text with Nomenclature

Integrating Attack Threat Expressions with Security Control Expressions into a Threat |Target | Protection Assurance model provides an ability to build fully integrated constructs of business Targets, how they can be attacked and how they should be Protected.