smart payment association

Business Continuity Management in the Payment Card Industry

December 2011

Abstract

This paper provides the conclusions of a detailed study by the Smart Payment Association (SPA) into the critical business continuity and disaster recovery aspects of the payment card issuance sector. The goals of the study, and the aims of this paper, are to bring clarity to the issues, offer a greater understanding of the value proposition associated with business continuity management, and to establish a set of guiding principles and best practices for developing and managing business continuity programmes.

- Consolidating the findings of the wide ranging SPA study, the paper provides readers with a background to the SPA project: 'Business Continuity Management in the Payment Card Industry'
- The necessary process steps card issuers should follow to deliver effective business continuity management across their operations
- A proposed business model that can be adapted by card issuers to determine the costs and benefits of the various implementation options
- 'Real world' scenarios to further articulate how business continuity management can be delivered to enhance differing strategic objectives
- The results of the study, and the conclusions within this paper, have been independently verified by key experts from the card issuance community across the globe

For more information or to contact SPA, please go to www.smartpaymentassociation.com

Table of Contents

1. Introduction

1.1. Background

Effective business continuity (BC) in the payment card industry is becoming ever more important as commercial transactions become increasingly reliant on various forms of electronic payment. For proof, simply look at the number of smart payment cards shipped in 2010; a massive 798 million. This almost doubles the figure from 2007.

Similarly, general purpose and private label credit, debit and prepaid payment cards are becoming ubiquitous, generating over $17 trillion worldwide in purchases of goods, cash advances and withdrawals in 2010 - up 16.4% ' compared to 2009*.

The adoption of electronic payment creates opportunity and challenge in equal measure; requiring the industry to adopt appropriate levels of management and monitoring to reduce both issuance-related and operational risks.

Of course, card issuers are not unaware of the need to mitigate the sort of risks that could threaten their payment infrastructures and are working to build comprehensive prevention mechanisms and fast, effective procedures to restore business operations should a disruption occur.

Such action is not limited to the smart payments industry. Managing risk is a priority across the business landscape – from building protection against fraud, through technical and operational issues, to assuring compliance in an increasingly complex regulatory world. Analysing the probability and the potential impact of risk is a crucial element in this process.

In the end though, it's next to impossible to forecast when and where incidents will strike. It would seem therefore that the best course of action is to follow the advice of Greek statesman, Pericles, some 2500 years ago: 'The key is not to predict the future, but to be prepared for it.'

1.2. The role of business continuity

Today most businesses are following this advice; developing business continuity strategies to effectively plan for incidents and business disruptions; and to put themselves in a position to respond effectively to continue business operations at an acceptable, predefined level.

Explicit principles have been derived in establishing business continuity management (BCM) as the comprehensive business process that identifies potential threats to an organisation and assesses the impacts to business operations that those threats might cause. BCM provides a frame of reference for building organisational safeguarding capabilities for an effective response that protects the interests of key stakeholders, reputation, brand and value-creating activities.

Companies are well advised to document - in a business continuity management plan (BCMP) - their agreed-upon set of procedures to enable their organisations to continue to deliver critical products and services at a predefined and acceptable level in the event of an incident.

**Smart Payment Association Press release, May 5, 2011*

The Nilson Report, Issue 980, September 2011

1.3. Smart Payment Association project on business continuity management (BCM)

Business continuity within the payment industry is critical and the Smart Payment Association (SPA) and its members have received a wide variety of requests from their card issuing customers to offer BC services in one form or the other. These requests differ with regard to the depth and breadth of the BC services under consideration. Yet despite a common understanding of the underlying roots of the risks, a cross-industry understanding and/or framework on how these risks are assessed and managed does not exist. More fundamentally, there appears to be a certain level of confusion regarding the complexity, regulatory frameworks and the business value of BCM and the necessary effort to ensure business continuity in a timely fashion.

Issuers' key questions include:

- What are the potential BC risks and threats a card issuer has to plan for and respond to?
- What are acceptable levels of service across the product portfolio following an incident?
- How can issuers prepare themselves to ensure that these predefined levels of service can be offered after a reasonable period of activation delay?
  - What are the options for issuers to organise BCM in partnership with their supplier network?
  - How could an efficient split of responsibilities be established between in-house stakeholders and third party technology and systems suppliers?

In response, the SPA commissioned a project with the following objectives:

- To provide an understanding of the underlying risk for an institution issuing payment cards which ultimately leads to a 'value proposition' for the appropriate set of business continuity management efforts.
- To define a set of industrial 'best practice scenarios' for BCM in the context of the issuance of payment cards or other form factors such as token and mobile phones used for payment.

Working together, experts from the SPA member companies have created a set of BC principles and best practices for the card payments industry.

2. Creating a BCM Plan

Creating a BCM plan follows well established management principles as shown in Diagram 1:

- During a thorough analysis phase the structure of the card issuance organisation and its operational status quo during normal operations are investigated and documented. This includes the scope of the business (e.g. size of the product portfolio and individual programme characteristics), the sourcing choices for all stages of the card issuance value chain during normal operations (e.g. single- or multi-suppliers, in-house or outsourced personalisation), the potential legal restrictions (e.g. international data transfer) imposed by governments, regulators and applicable standards, and the assessment of the potential risks the organisation might face. On the basis of this information, the analysis phase concludes with an assessment of the impact of all identified risks.
- The next phase establishes the overarching BCM strategy. The strategy will have to determine the balance between minimum service objectives and cost targets - always reflecting the regulatory framework the issuer operates under. The BCM strategy provides the foundation for deciding on the actual implementation.
- In a third step the strategic targets have to be turned into executable decisions regarding all implementation aspects. These decisions will cover how each product in the portfolio will be treated in case of an incident, how backup is organised for each element of the value chain, and whether these backup decisions are going to be implemented in-house or with the support of third party suppliers. The latter includes rules for testing and maintenance of the agreed upon implementations.
- Finally, the strategy and the implementation decisions need to be turned into reality by enacting them as corporate processes; identifying the process owner and resourcing the BCM efforts appropriately. Contracts and services level agreements need to be signed with internal and external suppliers. Tests are also essential to verify the actual implementation.

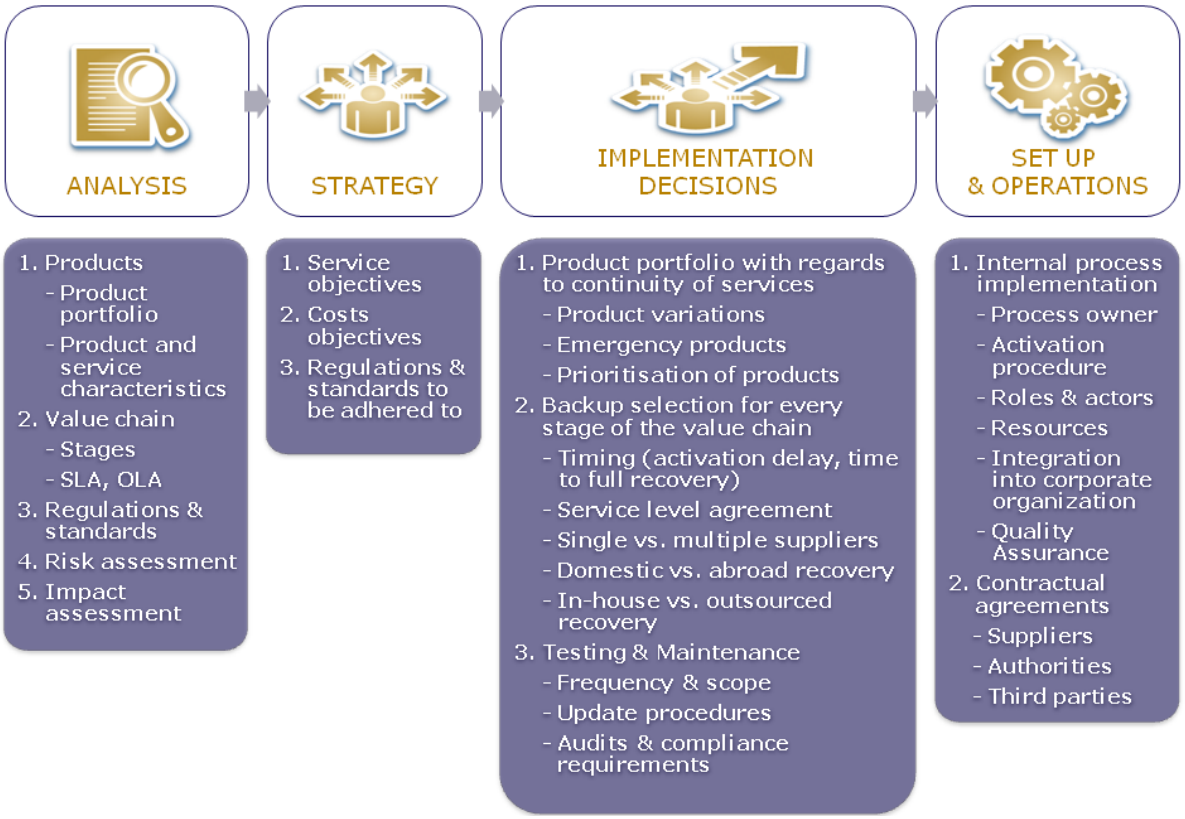

Diagram 1: Management process for BCMP creation

2.1. Analysis

2.1.1. Products

A thorough inventory of all elements and sub elements of an issuer's product portfolio is crucial before starting to prepare a BCM plan. In their push for differentiation, issuers tend to use more and more marketing promotion and innovation to deliver the most personalised services to their cardholders. This superiority of service requires substantial efforts during normal operations, but will require extended endeavours when it comes to supporting them as part of a BCM plan.

In order to understand and manage the complexity in an emergency situation, issuers need to document the characteristics for each of the programmes or artworks in the portfolio. An example is shown in Diagram 2.

Programme	Card program	Basic	Type	Credit
	Yearly volume	2 million cards	Monthly issuance peak	300,000 cards
	% of total cards	45%	% in cardholder value	28%
	Card usage	1st & 2nd card	Average time before use	5 days
Cryptography	RSA	Unique set of RSA keys per BIN => 4 sets of RSA keys		
	3DES	Generic set of 3DES keys		
Personalisation Features	Magnetic stripe	HiCo	Chip	Contact and contactless
	Additional applications	None		
	Optical personalisation	Laser engraving, embossing, indent printing		
	Carrier printing	Pre-printed black & white carriers with personalisation		
	Dispatching methods	ZIP code sorting; direct mailing for safe areas, else branch delivery		

Diagram 2: Issuer's portfolio inventory

A full set of documents for all parts of the portfolio will provide the necessary information to assess the complexity of supporting these programmes in the event a BCM plan needs to be invoked. This offers a first indication on how difficult and expensive full redundancy for all services within a BCM plan might be. Crucially, it also highlights where simplification could be possible without compromising the continued availability of basic card payment functionality to cardholders.

2.1.2. Value chain

An inventory of all players and their roles across the card issuance value chain (see Diagram 8 in Chapter 4 for details) must be established (e.g. single vs multiple suppliers, primary vs. secondary supplier, active vs passive backup), their relationships (e.g. can a secondary supplier by default personalise cards of the primary supplier and vice versa), and capabilities with regard to BCM (e.g. how difficult is it for a passive backup organisation to become an active supplier in case of emergency). And of course, it's vital to determine the business continuity policies of each of these players too.

The inventory could be organised as shown in the example in Diagram 3. The table clearly highlights current situation and potential BCM options.

Value Chain Service	Main Supplier	Redundant Service or BCP from Main Supplier	Active Backup from Alternate Supplier	Passive Alternate Supplier	Effort to make Passive Alternate Supplier Active
Card Body Management 	SPA Member A	Yes	N/A	No	++
Cardholder Data Distribution 	Internal IT Department	Yes	No	Alternate IT Supplier	+
Data Preparation 	Internal IT Department & SPA Member A	Yes	No	Alternate IT Supplier & SPA Member A, C	++
Personalisation 	SPA Member A	Yes	No	SPA Member A, C	++++
Fulfillment 	SPA Member A	Yes	No	SPA Member E, F	++
Shipment 	Postal Service Provider	Yes	No	Alternate Courrier	+

Diagram 3: Card issuance value chain player and roles

2.1.3. Regulations and standards

Government and/or standardisation organisations regularly issue new documents in which they describe, define, recommend and sometimes mandate rules or policies around BCM planning in the financial industry.

It is an indispensable part of the BCMP analysis phase to identify and understand these rules and recommendations as defined by the relevant regulatory and standard setting authorities – for example the national central banks or their international associations, or banking industry associations which may act as self-regulatory bodies or the global payment systems.

The analysis regarding BCMP should, at the very minimum, cover the following aspects:

- In case of a disaster, could regulations be bypassed by the way of a formal waiver? What would be the average lead time and process to obtain such a waiver?
- Has the central bank(s) or global payment system(s) setup a BCMP?
- Do the domestic regulations allow cardholder data management and/or physical card personalisation to be conducted abroad?

Naturally the constant evolution of the regulatory environment in which payment services operate demands organisation's keep abreast of all developments and make changes to their risk policies as a result.

2.1.4. Risk assessment

In the first instance the potential sources of risk BCM has to address in the payment card industry are as follows:

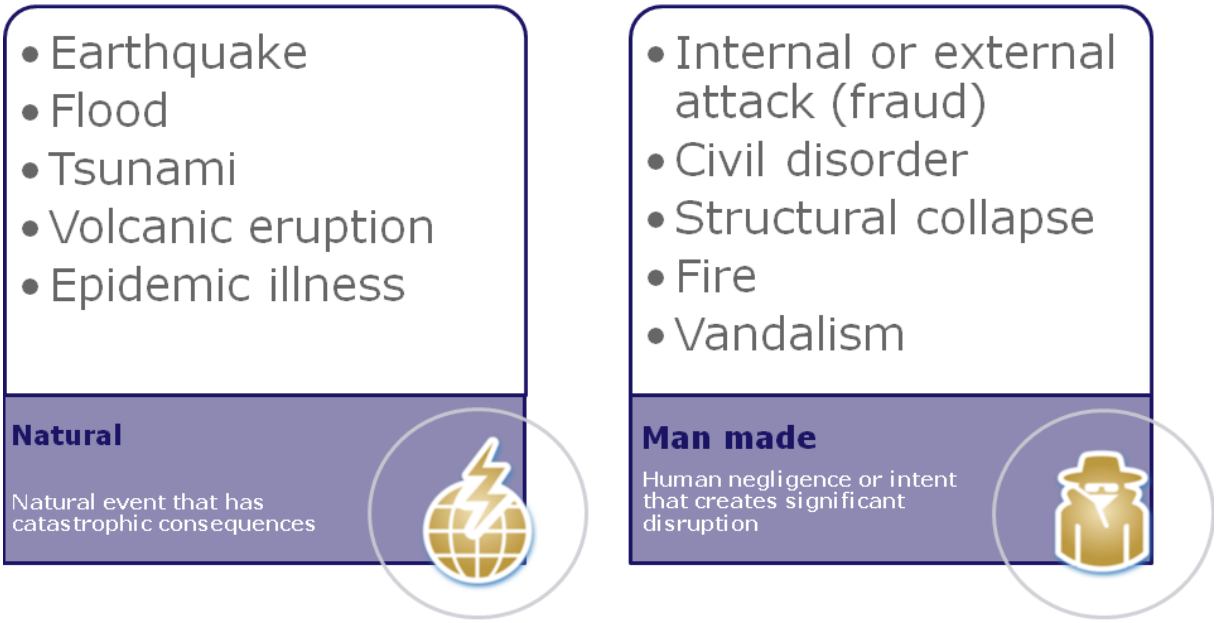

Diagram 4: Categories of risks

The above are, by definition, vague since the terms 'catastrophic' and 'significant' mean different things to different people, depending on various circumstances.

This study does not consider minor operational disruptions based on the temporary malfunctioning of hardware, software or communication lines - as all major suppliers are taking preventive and reactive measures to compensate for such disruptions; usually within hours and typically without any impact on normal output.

On the other hand, a company might declare a disaster and invoke their BCM plan in the face of a major threat even before an actual incident has occurred.

Therefore, the process of deciding whether a disaster has happened needs to be precisely defined in the BCM by the process owner. The authorities responsible for preparing and taking this decision must be clearly defined, and the course of action must be documented.

Within each of the aforementioned risk categories, the severity of the disruption, the impact on card issuance and the time it would take to recover depends on a set of parameters, for example:

- A natural incident may have global or at least significant regional repercussions.

- The impact of a structural collapse or a fire depends on how critical the damaged operations are for the entire card issuance process; their restoration depends on the effectiveness and availability of resources and the size of the actual damages.
- A multi-tier disaster that may strike in one or several phases of the card issuance value chain – with recovery time dependent on exactly where it struck and how severe it was.

2.1.5. Impact assessment

It is critical for issuers to identify all the potential impacts of their failure to deliver the personalised cards to customers as they expect them. As such, a key element of the analysis phase for an effective BCMP is to evaluate both the direct and indirect cost associated with an incident. Although the situation will be very different from issuer to issuer, the example below offers a guide to support issuers through this analysis.

2.1.5.1. Direct costs

In this example we assume 1 million cards are shipped per year, which results in an average of 4,000 new users per day failing to receive their payment cards. The consequences are that financial services are no longer available (purchasing with cards at physical or internet retailers and cash withdrawal from ATMs) and results in no revenues being generated from these transactions.

Customers will call to complain to customer service, and there's a significant chance they could move to a competing bank should the issue not be resolved rapidly.

The assumptions for this scenario are:

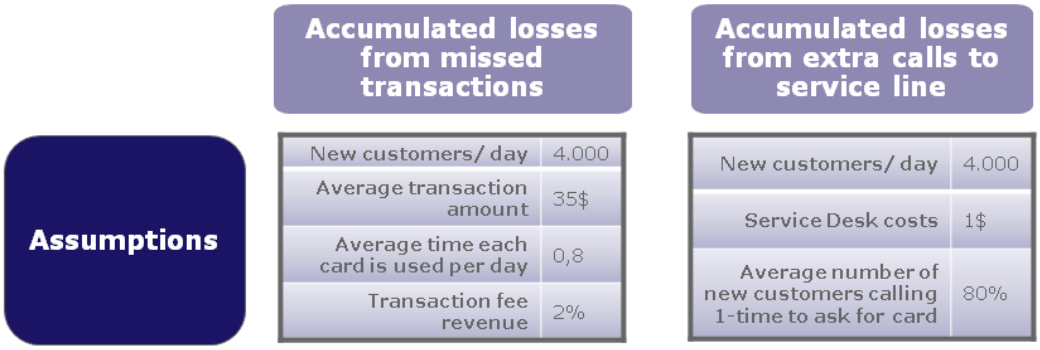

Diagram 5: Direct cost assumptions

The direct costs can be calculated as follows:

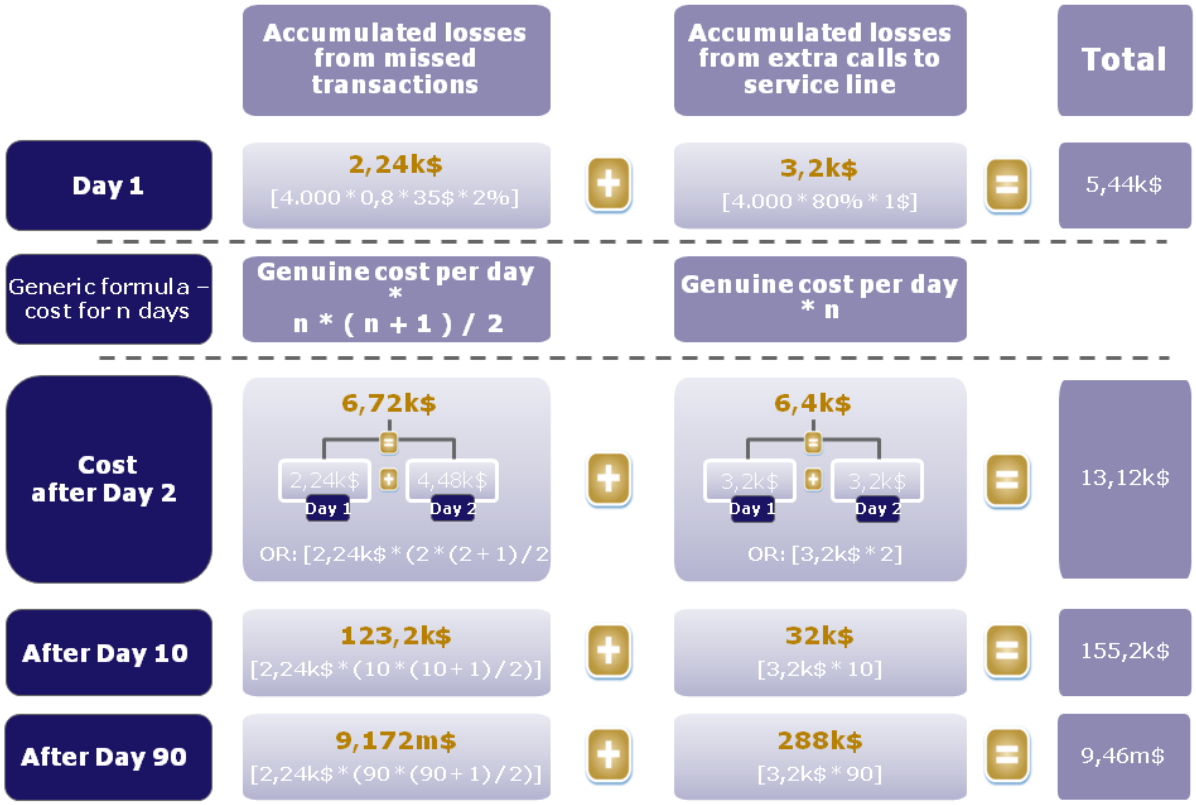

Diagram 6: Direct costs

In this example, the total costs after 10 days are 155,2k$ and grow to 9.46M$ after 90 days.

2.1.5.2. Indirect costs

In the event of an incident the issuer may have to go through the additional complexities of dedicated crisis management; particularly when dealing with the media and regulators. Also, cardholders will address their concerns to customer service even if their cards are not affected by the current disaster. And of course, in the wake of the incident the issuer will have to re-establish trust and rebuild its reputation.

Below are some guidelines for estimating the size and impact of more indirect factors. This is, of course, a more complex and wide-ranging activity than calculating the direct losses. The variance on the quoted average numbers is therefore very high and depends significantly on the nature and magnitude of the incident.

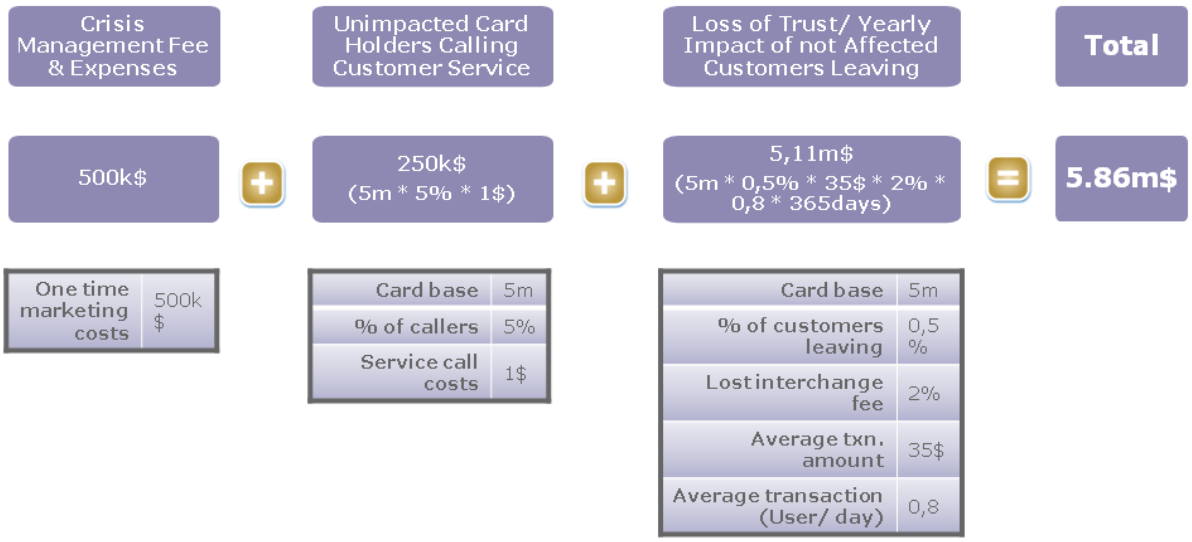

Diagram 7: Indirect costs

In this example, the total costs are 5.86 M$.

The purpose of this analysis is to enable the issuer to define an acceptable BCM coverage and activation delay based on the total costs that may occur from an incident.

2.2. Strategy

Following the analysis phase, the issuer has to create a BCM strategy which defines the overall objectives to be achieved through business continuity management planning.

The major questions an issuer must address in this phase are:

- What is a reasonable and/or maximum period of delay before recovery measures need to be activated in order to avoid prohibitive or even irreversible damages?
- What is the scope of the initial recovery offerings? Should BCM cover the whole product portfolio or only part of it?
- What is a realistic/desirable timescale before the normal level of service has to be restored?
- What is an acceptable level of expenditure (investment and resources) to be spent for BCM within the issuer's organisation and with 3rd party suppliers?

The answers to these questions depend on some basic considerations:

- How do we meet customer expectations regarding continuity of service?

Every serious incident will have a service impact to the production and delivery time. Understanding customers' expectations helps keep costs and resources within reasonable limits. In case of very demanding customers, there may be no other choice than to set up a full backup procedure. If, however, the only customer expectation for a mass market product is to have a

working card delivered in the shortest period of time, then a generic card artwork might be used or a single product (e.g. a gold card) is delivered to all customers no matter what their contractual card level might be. Also, service levels in the fulfilment and shipment stages may be reduced (e.g. the customer may be asked to collect the card from a branch or a central location).
For a premium card, the situation might be different.

- How do we make sure legal and regulatory standards are adhered to?

Payment card data is very sensitive. Even in times of disruption, regulators (e.g. central banks) may require that cardholder data is not sent abroad. The global payment systems insist that backup facilities are certified according to their site data protection standards. Altogether, these rules may determine the location of a backup facility within the country of operation or abroad.

- How do we keep BCM efforts within a reasonable financial range?

Effective BCM planning requires a substantial investment of time and resources; and so becomes a balance of 'what level is desirable' against 'what is affordable'. This may result in a maximum expenditure level for BCM. While such a cap may result in service level degradation, and the potential of long term reputational damage, the cost-benefit analysis may make business sense. But this, of course, is exactly what strategy setting at this stage is all about.

2.3. Implementation decisions

Once the strategic objectives have been determined the issuer needs to focus on an efficient implementation that defines the scope for deliverables and SLAs in a business continuity situation. This step ensures that the strategic goals are reached at acceptable cost level, and with the minimum level of manageable complexity.

2.3.1. Product portfolio with regard to continuity of service

As a first step issuers should consider the huge level of differentiation within their product portfolio. During normal operation a large number of product variants are produced and delivered with numerous artworks and features paired with various carriers, marketing inserts and other collaterals.

Establishing comprehensive backup production and personalisation for all combinations is an expensive and complex business – particularly a BC case may very well be a worst case scenario. However, if the strategic goal is to ensure card delivery to all customers under all circumstances then this goal can be achieved by a different tactical approach detailed below:

- Support is only provided for a limited number of products – which are delivered to all consumers irrespective of their individual product.
- Consumers receive a special predefined 'emergency' product in the BC situation.
- Some products are prioritised over others.

The original diversity of products is, of course, delivered again after full recovery, but the above approaches help to reduce the complexity and costs for the initial BCP setup – both for stock management as well as for regular maintenance and testing.

Similar decisions can be made for delivery times and methods. For instance, a collective delivery to a distribution centre or a limitation to registered mail would only be acceptable for a period of days or weeks. Again, this would provide acceptable customer service while optimising costs.

Part of this stage should also focus on defining responsibilities that remain with the supplier and those that are taken over by the issuer. For example, an issuer could store some backup inserts, and deliver these to the supplier as soon as a BC incident occurs.

2.3.2. Backup selection for every stage of the value chain

Once the scope of BCM activities is defined, the operational aspects need to be clarified to a point where a comprehensive programme can be put in place and contractually agreed by all parties. From the analysis phase it is clear who provides the regular services for each stage of the value chain.

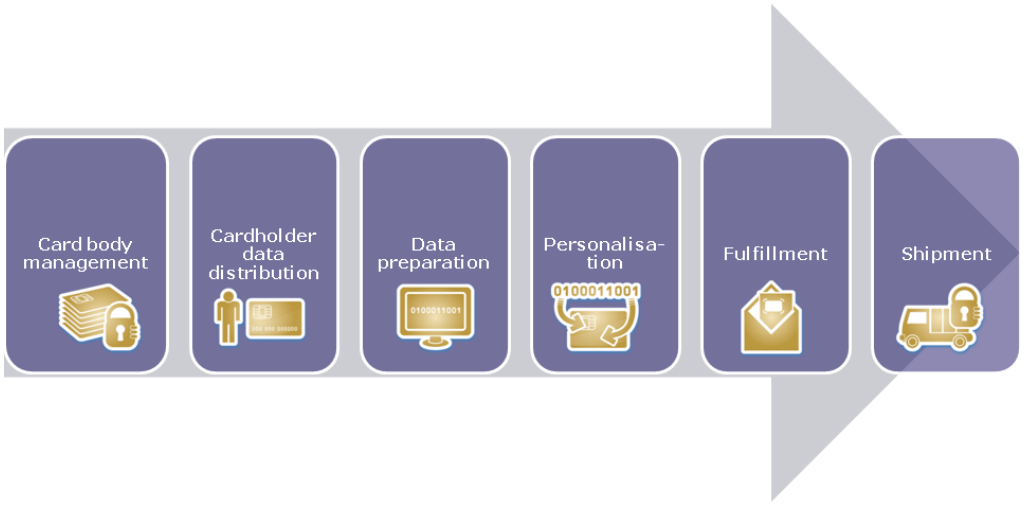

Diagram 8: Card issuance value chain

Based on the risk analysis and impact assessment described in chapter 2.1 an issuer has to decide whether disruptions of any stage of the value chain can be treated in an isolated way or whether they have to be treated as being interrelated. For instance, if the major portion of card stock is physically located at the personalisation site, both card body management and personalisation stages have to be addressed simultaneously.

Next, a decision has to be made how to complement the in-house vs. outsource situation for regular operations in a BC case. In other words, if the entire value chain is normally sourced in-house then a backup regime could be developed to replicate the entire infrastructure (at a potentially high investment cost) in-house or to use industry supplier capacities just for the BC case.

If parts of the normal operations are outsourced it might be the best option to rely on the supplier's BCM plans and the associated backup facilities. In some cases, multiple suppliers might

have to be contracted to ensure full coverage in case of an emergency. The potential limitations of shipping cardholder data abroad need to be reflected in this setup.

In any case, the aforementioned portfolio decisions and timings for backup activation delay and time to full recovery need to be reflected in clear service level agreements, whether the BC suppliers are in-house or outsourced.

2.3.3. Testing & maintenance

As discussed earlier in the paper, the BCMP has to be regularly tested and reviewed in order to keep it relevant and up-to-date. It is therefore vital to confirm the scope and frequency of all test efforts. This can be a complex undertaking as testing must be carried out across the entire value chain, by multiple parties. As such, effective coordination of all test efforts is a priority.

2.4. Set up and operations

The final phase concerns establishing and managing BCMP as a corporate business process. The issuer will have to identify and install a process owner, and provide them with the proper resources and budget to manage the entire process - from creation and implementation, all the way through day-to-day operation.

The process owner is responsible for:

- Defining the BCM procedures in line with the decisions made before and addressing the objectives of the BCM strategy.
- Creating and controlling the process documentation and obtaining approval from the proper levels of management - potentially including sign-off by corporate management and regulators.
- Identifying and signing up those members of the organisation who have to play a role in the process, and educating them about their obligations.
- Managing the invocation of the BCMP in coordination with other BCMP players.
- Establishing and maintaining all the necessary contracts and service level agreements with internal and external suppliers.
- Testing, updating, quality assurance and audit readiness across the lifecycle of the BCMP.

The BCMP has to be updated regularly reflecting new card products, carriers and collaterals. Backup stock must be periodically re-filled, updated or fully exchanged. Re-tests should be scheduled to verify the continuous readiness of the procedures and measures in place for business continuity. The frequency of the updates and re-tests influences the activation delay in case of an incident. Audits can be considered to ensure compliance to the requirements.

3. Business model

Many of the decisions that the issuer must make in developing the BCM plan are predicated on identifying and maintaining customer service levels during the incident. Based on the detailed study, a formal business model has been created that issuers can use as a basis to build a comprehensive picture of the financial implications of an incident. Diagram 9 provides a top line overview, while the associated spread sheet is available on request.

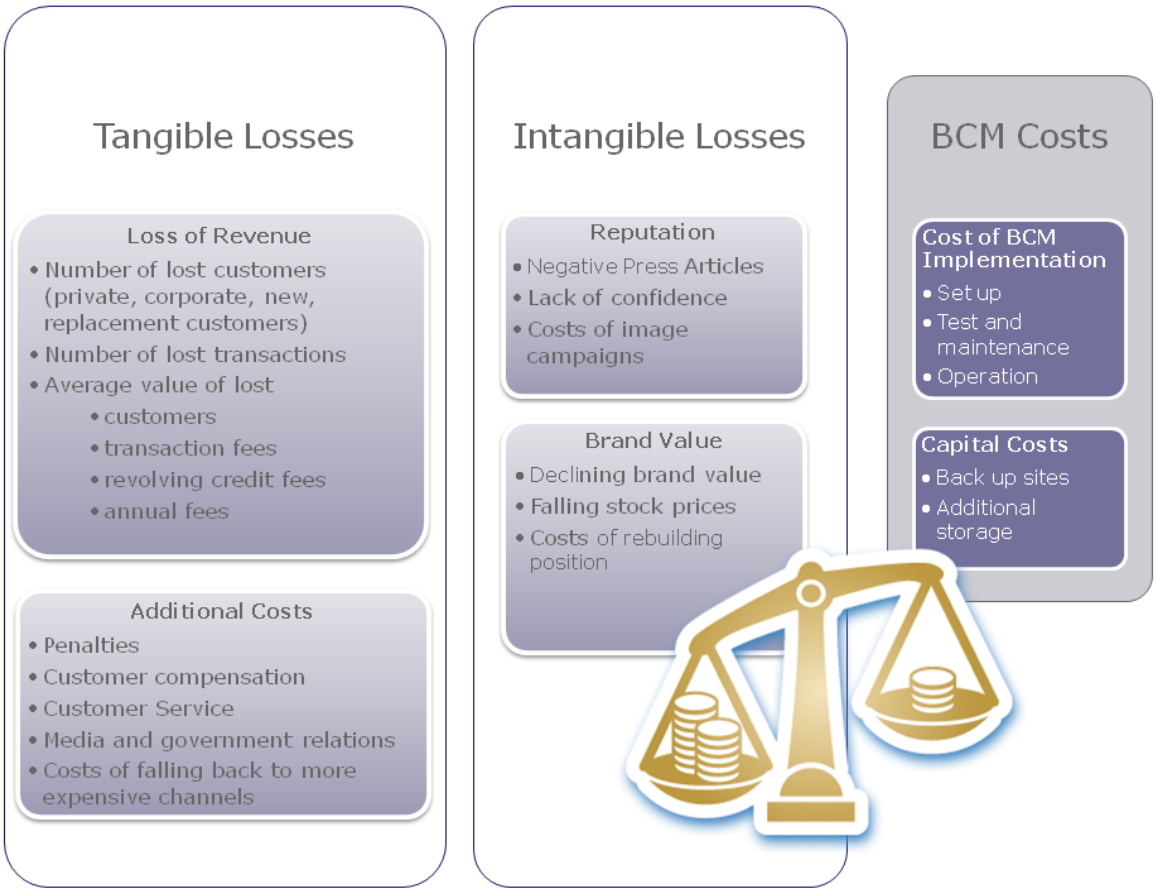

Diagram 9: BCM cost versus loss in case of disaster

3.1. Potential damage

3.1.1. Tangible losses

Each time the issuer loses the ability to issue, or more accurately, to ship cards, the number of payment transactions will fall, and, depending on the severity of the problem, may cause a breakdown in the customer relationship.

Similarly, the issuers' efforts to acquire new customers are jeopardised – again resulting in lost transactions. In the SPA business model the issuer will have to estimate the number of lost customers, and lost transactions, on a monthly basis. Issuers will also have to define the average value of a lost customer and transaction, plus any fixed fees associated with a subscription customer. The model will then calculate the resulting revenue losses.

On top of these revenue losses, issuers may encounter additional costs. They include contractual penalties and other forms of compensation for having violated service level agreements, the increased costs for customer service and the handling of media, government and regulators, as well as those costs borne by the customer in having to fall back to more expensive channels to conduct their businesses (e.g., branch, cheque or cash).

3.1.2. Intangible losses

Any major incident will impact brand, as a loss of service to end-users will be widely reported. The costs of rebuilding corporate reputation cannot be underestimated, and need to be assessed and entered into the model.

3.2. Costs of BCM implementation

A major element of the costs of BCM is incurred independently of an incident happening at all. The expenditure for initial set-up, scheduled maintenance, regular testing and continued operation of a BCMP will all have to be estimated based on the chosen service level strategy. If the issuer decides to build in-house backup facilities and to hold emergency stock for card bodies, the associated capital expenditure has to be reflected in the model.

4. The Value Chain for Payment Card Issuance

The next step evaluates the potential implications of BCM decisions throughout the value chain in more detail.

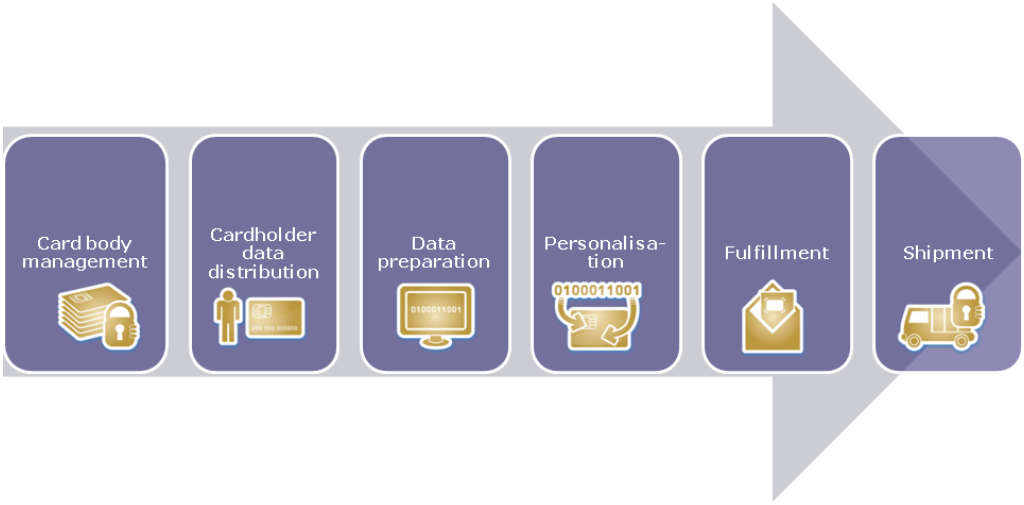

Diagram 8: Card issuance value chain

The different elements in the chain are subject to varying threats and vulnerabilities. Depending on the nature and severity of the incident, and the sensitivity the issuer attributes to the various stages, recovery approaches will differ. It is therefore vital to plan on a case-by-case basis – with a thorough analysis and understanding of individual need throughout the chain.

4.1. Card body management

At the beginning of the value chain, the plastic card body has to be produced. As a matter of standard practice of supply chain management a certain number of card bodies are stocked and waiting for further processing during personalisation. The combination of card production capabilities and card storage levels determines the vulnerability to any potential threats.

Should a card body production facility experience a disaster, card personalisation will rely on an existing card body stock and/or an operational backup production facility.

In many cases, card body production today is distributed across a number of manufacturing sites – all capable of backing themselves up. Also, card bodies can be relatively easily shipped across the globe. Card bodies are normally stocked close to the personalisation sites and are covered by the associated security and control regimes. Should an issuer decide to maintain an independent backup storage site for card bodies, this facility has to be compliant with the requirements of the global payment systems:

- Card bodies must be stored in a secure vault in the high security area with limited access conditions. The size of the vault affects the quantity of cards and therefore the time the personalisation plant can produce without receiving new card bodies from other sources.

- Dual Control. Card bodies can only be managed under control of two or more persons.
- Quantity Control. Documentation and counting equipment is required.
- Video Control. Enabling traceability and factory control.

Finally, issuers can make upfront choices on what level of flexibility they want in the case of card body stock and/or card body production being significantly disrupted. At one end of the spectrum issuers may want to have full backup access to card bodies for all of their card products (graphical layouts, magnetic stripe options, contact only, dual interface, etc.) in order to continue to personalise these cards for a predefined period of time.

At the other end, issuers may decide that in the case of a disaster they can sustain their business for a predetermined time period with few card body options available. Or, of course, issuers may opt for anywhere in between.

Diagram 10 below summarises the decisions and implications of those decisions for card body management.

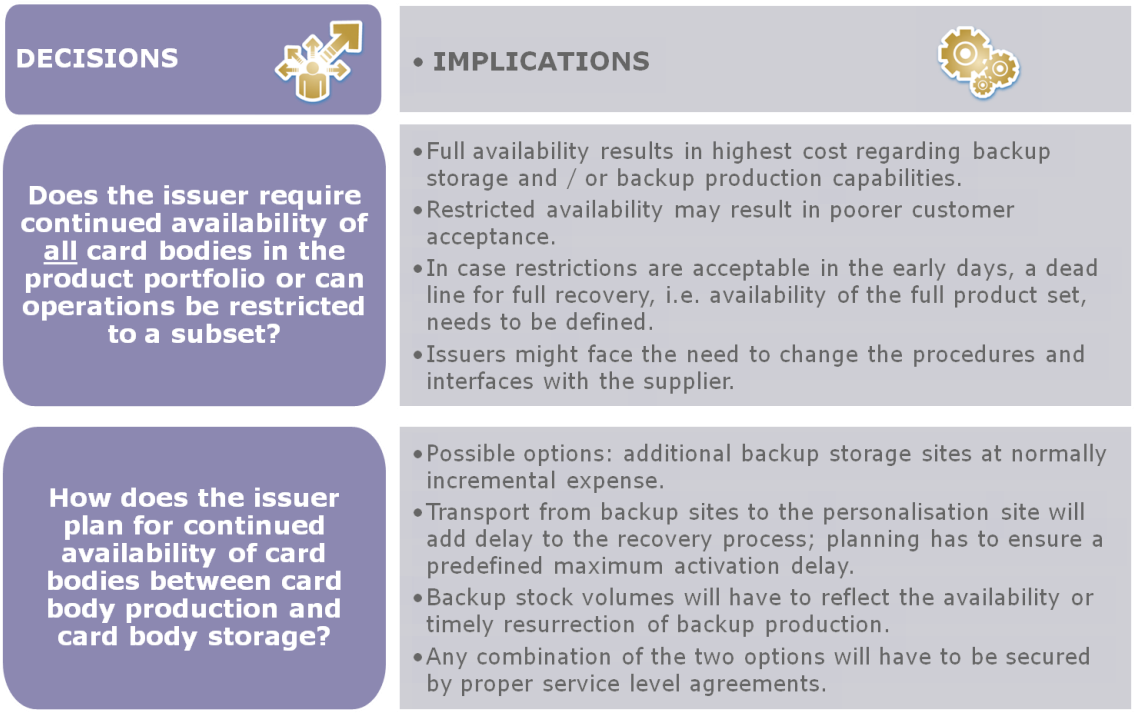

Diagram 10: Card body management decisions & implications

4.2. Cardholder data distribution

Cardholder data distribution, defined as the process transmitting the cardholder data from the issuer to the personalisation bureau, is an essential part of the card issuance value chain. There are different ways of how issuers can deliver cardholder data to a personalisation bureau, including:

- E-mail.
- Secure FTP or FTPS.
- Connect Direct.
- Web Services.

Cardholder data need to be transmitted in compliance with security requirements established by the global payment systems:

- Cardholder data must be encrypted.
- Procedures must be documented.
- Access control is enforced.
- Data authenticity and integrity checks are in place.

A potential disruption in the cardholder data distribution sub process is constituted by a failure of either the lines of transmission, or of the sending / receiving data server. In case of disaster, the recovery process must therefore provide different transmission protocols and/or different destinations.

Assuming that the standard transmission protocol is via Secure FTP or FTPS to a fixed server address, issuers have to make the following upfront choices in cooperation with their personalisation bureaus:

DECISIONS	• IMPLICATIONS
Is it sufficient to fall back to e-mail transmission for a limited period of time?	• Cardholder data has to be properly encrypted during transmission, the associated encryption keys have to be set up in advance. • Dedicated e-mail addresses have to be established in advance. • The personalisation bureau has to take care of the process of "loading" cardholder data into their production software.
Is it acceptable to the issuer to reroute the cardholder data via the normal transmission method to a different server with a different address?	• The issuer sends the cardholder data via the normal transmission method to a different server with a different address. • The backup personalisation bureau has to assure that access data to this backup server are properly prepared and keys, passwords etc. are established in advance.
Is it desirable for the issuer to send the cardholder data via the normal transmission method to a different server with the same address?	• There are no changes in the issuer's process. • The backup personalisation bureau has to assure that the issuer's input is routed from the standard address to the backup address, access data are properly prepared and keys, passwords etc. are established in advance.

Diagram 11: Cardholder data distribution decisions and implications

Of course, the burdens on the issuer and on the receiving personalisation bureau differ from one option to the other as described above; with the setup, management and availability of the proper keys being critical issues.

4.3. Data preparation

Data preparation is based on a combined hardware and software solution which can be executed either in house by the issuer or outsourced to a personalisation bureau. During data preparation all information necessary for linking a card to an individual cardholder is organised. This includes optical, magnetic stripe, chip and fulfilment data. In particular, the cryptographic and payment application data necessary for personalising the EMV chip is generated.

According to EMVCo, EMV chip data preparation is defined as 'the process that creates the data that is to be placed in an IC card application during card personalisation. Some of the data created may be the same across all cards in a batch; other data may vary by card. Other data, such as keys, may be secret and need to be encrypted at all times during the personalisation process. Data preparation may be a single process or it may require interaction between multiple systems'.

A potential incident would incapacitate the systems environment in which the data preparation normally occurs. This includes the data processing but also the secure storage of sensitive cryptographic keys. The only effective way issuers can prepare themselves for such a disaster is to establish and maintain a backup site.

Again, as a minimum, any backup site must comply with the global payment systems' requirements (see chapters 4.1 and 4.2). Above and beyond these minimum requirements issuers have a couple of choices which again tend to either limit their flexibility or increase their expenditure.

Diagram 12: Data preparation decisions & implementations

Again, the bigger the desired flexibility in case of a disruption is, the higher the associated upfront effort and cost. Issuers need to determine the proper balance on a case-by-case basis.

4.4. Personalisation

According to EMVCo, 'card personalisation means the use of data personalisation commands sent to a card that already contains the basic EMV application'. In case of a multi-application card, EMV payment applications and non-EMV applications may well use the same personalisation process. Non chip-related personalisation activities for the card (e.g. embossing, printing, magnetic stripe encoding), usually take place within one integrated personalisation process.

Similar to data preparation, a potential disaster here would incapacitate the systems environment in which the personalisation normally occurs. This includes the personalisation equipment and associated software setup as well as card bodies stocked close to the personalisation equipment. The only fundamental way issuers can prepare themselves is to establish and maintain a backup personalisation site which, as a minimum, must comply with the global payments system requirements (see chapters 4.1 and 4.2).

Above and beyond these minimum requirements issuers have a number of choices which either limit their flexibility or increase their expenditure.

DECISIONS	• IMPLICATIONS
Is the issuer legally allowed to temporarily transmit cardholder data abroad?	• If yes, then issuers have more flexibility to engage backup data centres outside of the country. • If not, flexibility may be limited to the point that – in case of a nationwide natural disaster – continuation of service becomes impossible.
Should a back up site be set up and maintained in advance or only when the disaster strikes?	• A backup site needs to be in compliance with global payment system requirements. Since certifying this compliance is a lengthy process, a basic contractual relationship with such a backup site must be in place anyway. • Data preparation requires the secure exchange and storage of application and payment system keys, certificates etc. The exchange has to follow certain 'ceremonies' and takes a certain amount of time to setup and execute. • If the backup site is managed as a 'cold' site these ceremonies will have to be performed after the disaster strikes. Also, potential updates applied to the main site will have to be replicated at the backup site before it can accept cardholder data. • If the backup site is managed as a 'hot' site all the necessary installations will have been completed ahead of time, updates are applied in timely intervals and regularly tested. Rerouting of data streams and processing can start without significant delay after the incident.

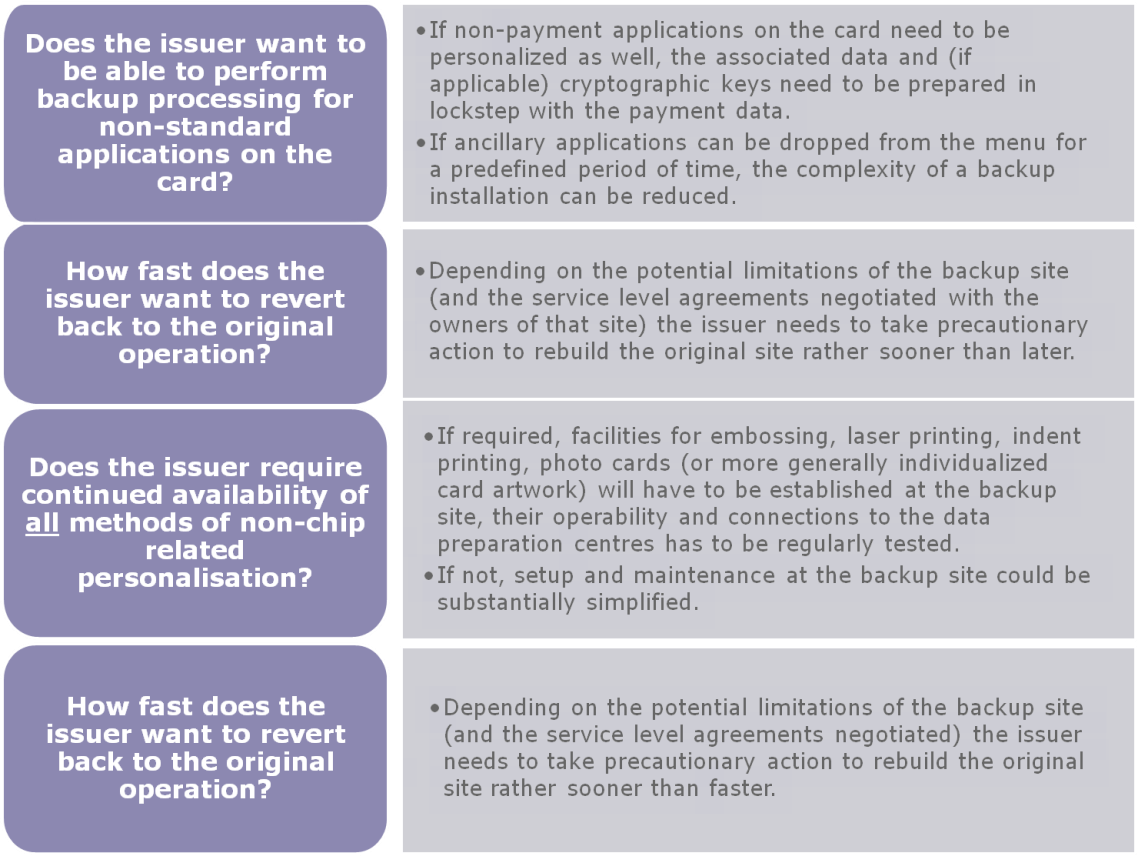

Diagram 13: Personalisation decisions & implications

4.5. Fulfilment

Often BCP discussions end with personalisation. However, fulfilment is a crucial part, too. It is the process by which a card is affixed to a card carrier and inserted into an envelope. The process may be complicated by adding more inserts (e.g. documents carrying legal or contractual information or marketing material).

Normally issuers stock multiple card carriers prepared with marketing pictures, the bank's logo, fixed text (e.g. describing the particular card programme) onto which variable text with cardholder data (e.g. name, address, etc.) is printed during the fulfilment process.

Disruption of service at the fulfilment stage means that one or more carrier/envelope supplier is not in a position to deliver - and there is no material stock at the regular fulfilment site. Similar to card body management the combination of production capabilities and storage levels determines the vulnerability of this part of the value chain, and issuer options include:

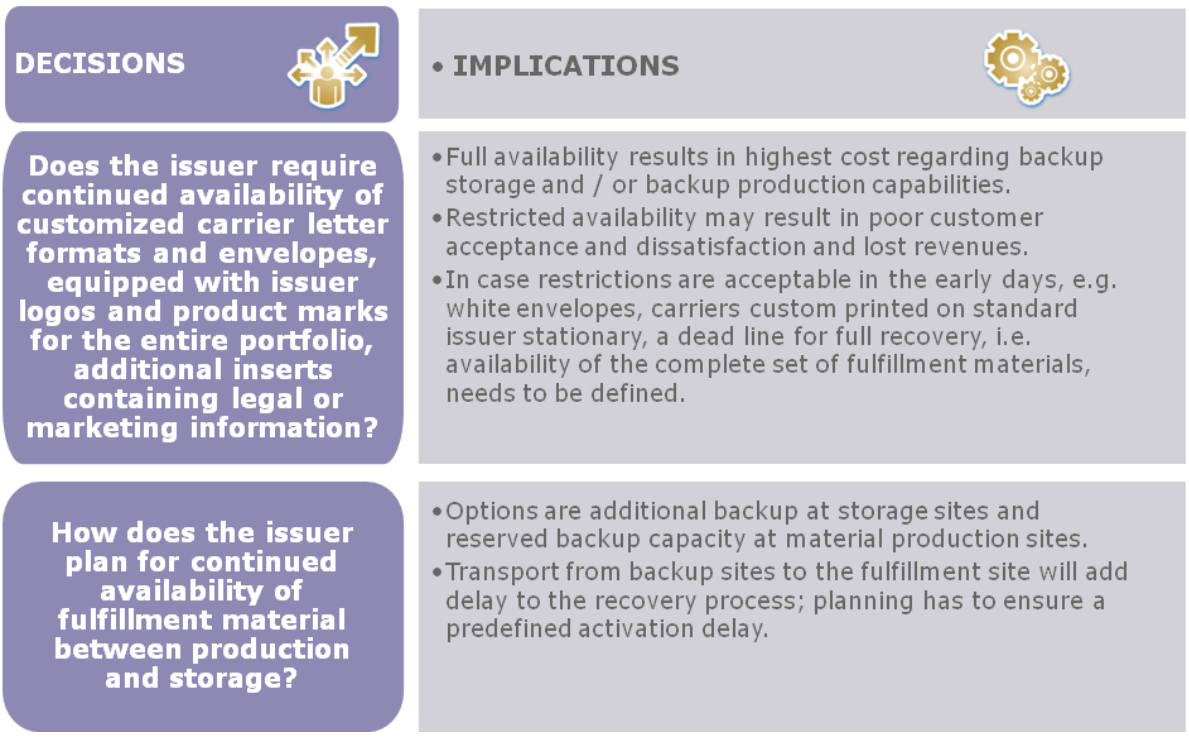

Diagram 14: Fulfilment decisions & implications

4.6. Shipment

Cards shipment is regulated by the security standards of the global payment systems. A potential disaster would disrupt the process of distributing regularly stuffed, personalised envelopes from the fulfilment site to the end customer, e.g. disrupted access to the fulfilment site or failure of the designated courier service to operate.

Regarding the former, there does not seem to be an obvious remedy other than to restart the production process. This would have to be decided by the BCM authorities based on the expected duration of the disruption.

Regarding the latter (e.g. bankruptcy of the main courier service or major labour disputes), the issuer needs to decide whether the probability of such an incident warrants a dual supplier policy. In this case a service level agreement with the suppliers would have to be set up regarding mutual stand-in.

Similar to other stages, it has to be evaluated what the backup site's capability is and if service limitations such as bulk shipments to distribution centres might be acceptable for a period of time to reduce the complexity and to maximise the throughput of the backup site.

5. Best practices

In this final section we describe two real life examples where issuers have made consistent decisions along the elements of the value chain. In both cases the underlying objective was to maintain basic payment card functionality and service.

The scenarios differ with regard to the visible impact for the cardholder resulting from the choices the issuer has made in order to accomplish the basic objective of continued payment service (e.g. by a limited choice of artwork). However, in both cases customers get their cards and can continue to pay electronically - albeit with a varying time delay and feature mix.

5.1. Scenario A: Minimal perceived impact for the cardholder

In this approach the issuer establishes a hot switching backup environment with ample stock of card bodies for the entire card portfolio.

The disaster case is defined as the personalisation centre along with the stock of non-personalised cards is no longer available to the issuer.

In this scenario, a properly certified site is maintained with regard to the cryptographic environment regardless of an incident occurring. Once the BCMP is activated, the already established and tested connections between the issuer's data centre, the data preparation centre and the backup personalisation centre will be switched on in a matter of hours.

With the backup stock moved to the backup personalisation centre, a fully redundant backup environment is able to support every card programme in the portfolio with service levels as expected by the issuer and the cardholders. The size of the card body stock is supposed to give the issuer enough time to establish a new card body production capability before the stock is depleted.

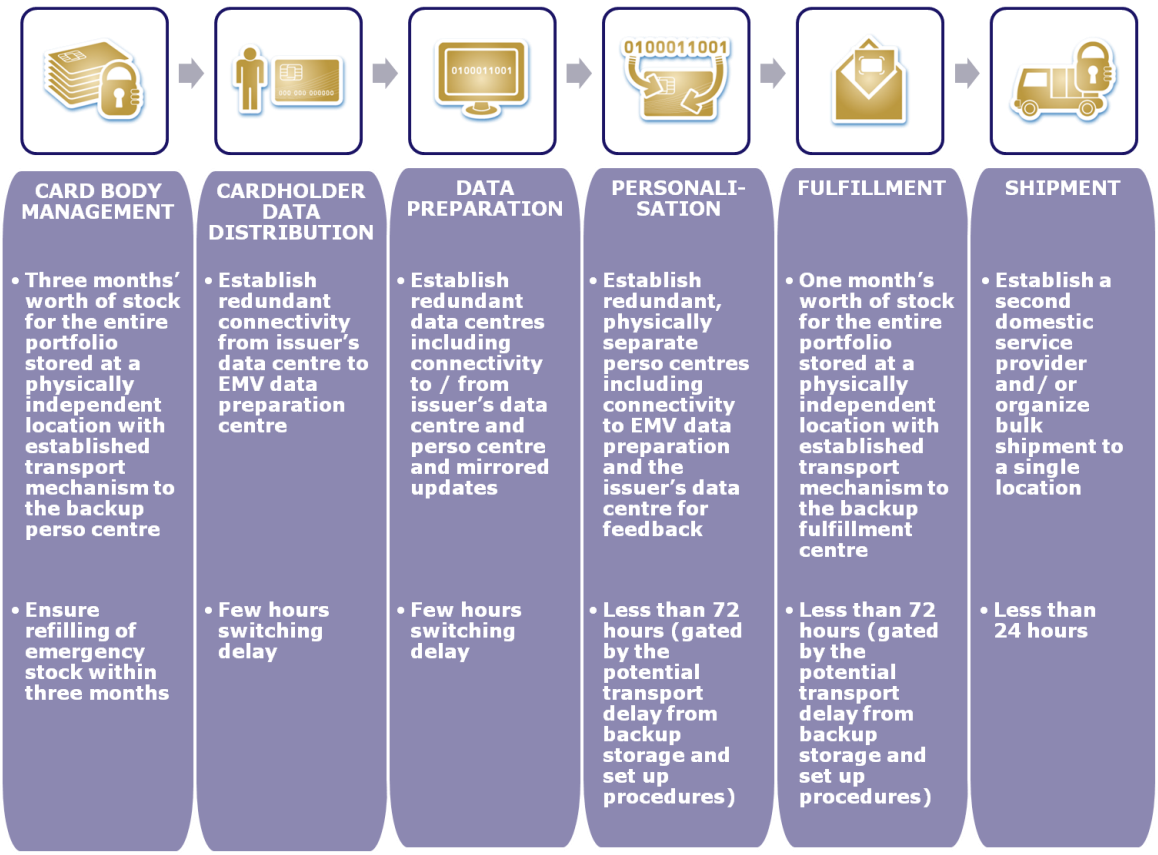

Diagram 15: BCM scenario with minimal perceived impact for the cardholder

This is obviously the most complex and expensive BCM plan providing the most superior level of service.

5.2. Scenario B: Reduced service level options

In this scenario, the service levels for all stages of the value chain have been reduced while still maintaining the basic objective of providing functioning payment cards to the consumer.

Instead of storing all card artwork variations, only the artwork for three card programmes are stored while the rest of the portfolio has been mapped to these three programmes ahead of time.

Data centre connectivity is not switched immediately but established after the incident happened.

The data preparation centre has been updated and tested as part of a planned annual test.

Fulfilment will be restricted to bulk shipment to the issuer or a distribution centre that will then have to organise shipment or other means of distribution.

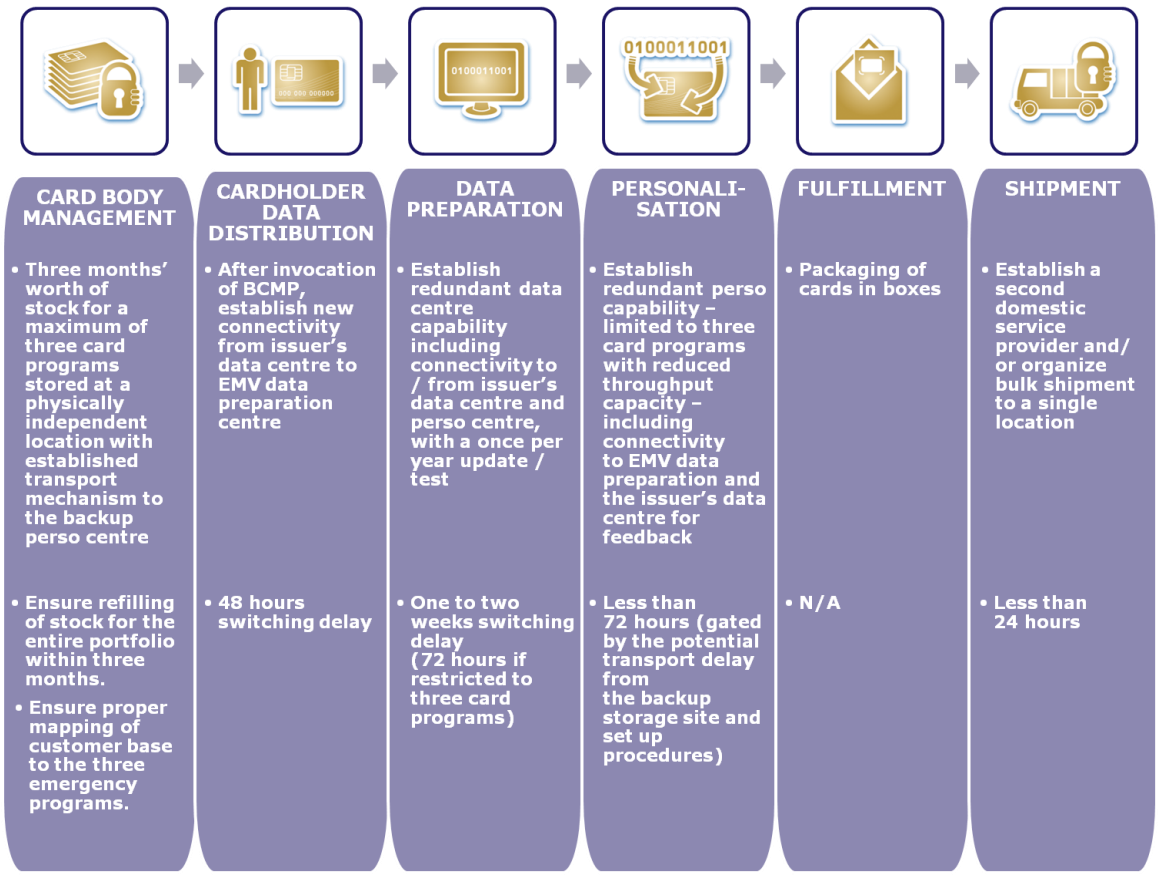

Diagram 16: BCM scenario with reduced service level options

5.3. Assessment and Conclusion

These scenarios have been fully validated as real-world examples by a panel of issuers around the world. Obviously, many variations exist in the marketplace and are operated by other issuers upon the completion of a thorough analysis of their specific situations. Crucially, the decisions on how to source normal operations, and on how fast backup operations have to be up and running, have a significant overall impact on the way business continuity is managed.

- Some issuers perform almost all stages of the value chain in-house. While their data centres normally have established backup sites based on standard regulations of the financial industry, backing up card body management and the actual personalisation centre requires thorough analysis before reaching a decision whether to build the respective backup sites in-house (at a remote location) or engage a third party.

- Many issuers outsource all parts of the card issuance value chain although in most cases they keep the cardholder data management and data preparation in-house. If they have multiple suppliers for card body management and personalisation, they must make decisions as to whether their BCM plans only cover the primary supplier or whether the distribution of the product portfolio requires that each supplier is part of the issuer's BCMP. Both choices have been implemented in the market. In some cases, issuers require that personalisation centres of one

supplier are capable of personalising the cards of other suppliers in order to achieve higher flexibility in case of an incident striking one of the suppliers.

- In case the entire value chain is fully outsourced to a single supplier BCM planning evidently relies exclusively on the BCM capabilities of that supplier. As with any single source decision, such a choice requires in-depth analysis, proper planning and the creation, maintenance and enforcement of proper service level agreements.

- Issuers which are part of international or even global banking groups should be able to naturally leverage the availability of multiple locations in different geographies for their BCM planning. In practice, efforts to do so seem to be in early stages.

- No matter which decision is taken regarding the sourcing of the potential backup sites, major consideration is usually given to the acceptable activation delay when switching to the backup scenario. Whether an issuer requires 'hot' or 'cold' switching (or anything in between) very substantially influences the complexity, investment and running expense associated with BCMP. Specifically, if an issuer requires hot-switching for the entire product portfolio sustaining all regular features all the way through fulfilment and shipment, he will have to face significant upfront and running efforts and must manage the resulting complexity.
- The fact that – fortunately – BCM plans are not invoked very often underlines the importance of incorporating regular reviews, audits, updates and tests of the business continuity procedures into any state-of-the-art BCMP.

There's little doubt that business continuity management must be front and centre for today's card issuers. As we have modelled above, the potential significance of both financial and reputation damage is such that failure to put effective policies in place is tantamount to corporate suicide.

However, there is no easy fix. To be truly effective, business continuity management must begin with a thorough situation and risk analysis, variables must be understood, service levels defined and programmes extended out from the issuer to encompass the entire supply chain.

Of course, as with any business process, a detailed cost-benefit analysis must be carried out to define the level of BCM appropriate to each individual organisation and their supply chains. Defining the level of 'acceptable' service delivery in the event of an incident is as important as understanding likely points of failure and the consequences of such, and will do much in helping the issuer to develop a sound business case for action.

So while variations abound in developing the most appropriate BCM plan, the best practices and models described in this paper will deliver the consistency of approach needed to assure effective business continuity management strategies going forward.