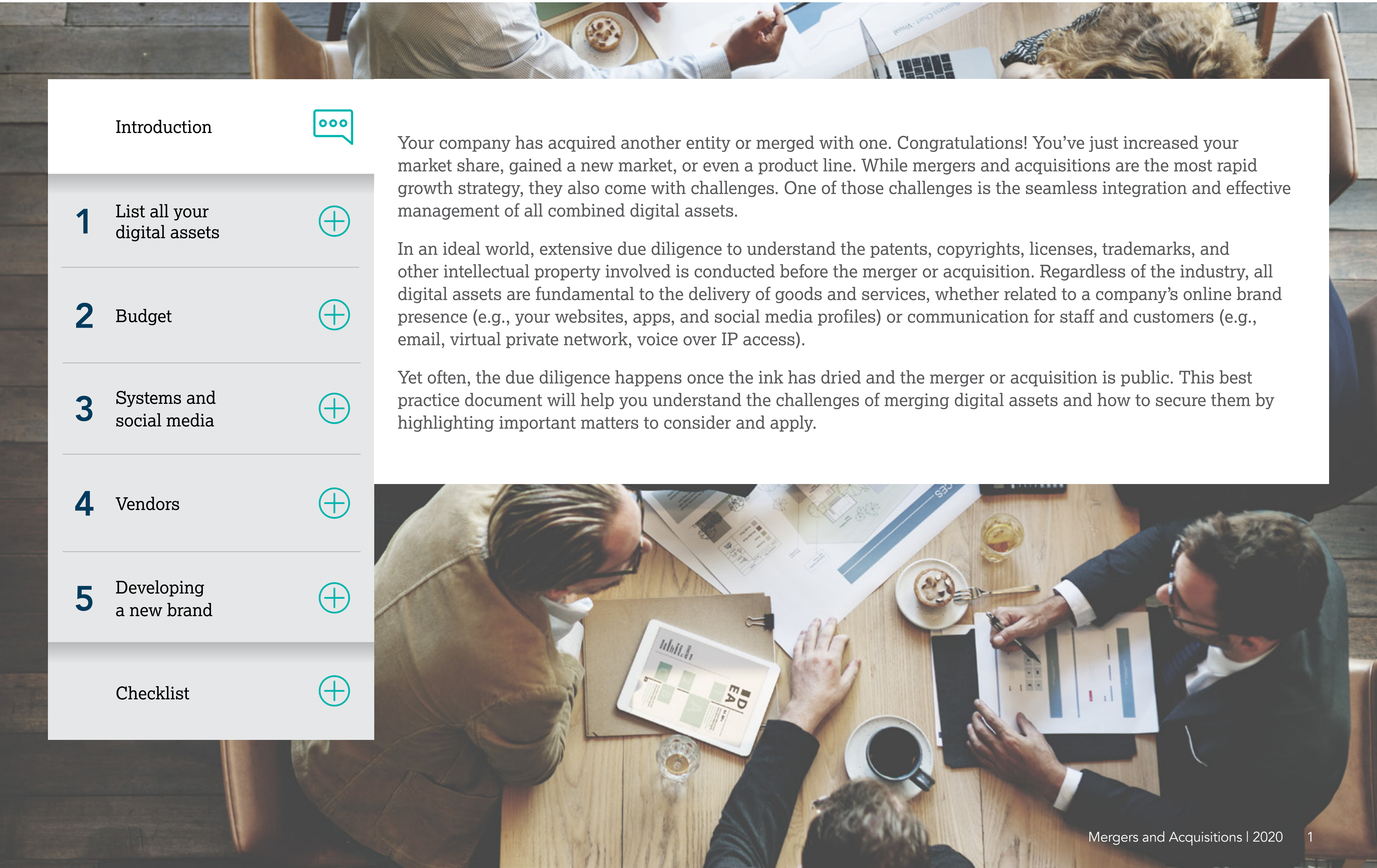
CSC

CSC Best Practice Guide

Mergers *and* Acquisitions

Taking care of digital brands during entity consolidation

Mergers *and* Acquisitions



Your company has acquired another entity or merged with one. Congratulations! You've just increased your market share, gained a new market, or even a product line. While mergers and acquisitions are the most rapid growth strategy, they also come with challenges. One of those challenges is the seamless integration and effective management of all combined digital assets.

In an ideal world, extensive due diligence to understand the patents, copyrights, licenses, trademarks, and other intellectual property involved is conducted before the merger or acquisition. Regardless of the industry, all digital assets are fundamental to the delivery of goods and services, whether related to a company's online brand presence (e.g., your websites, apps, and social media profiles) or communication for staff and customers (e.g., email, virtual private network, voice over IP access).

Yet often, the due diligence happens once the ink has dried and the merger or acquisition is public. This best practice document will help you understand the challenges of merging digital assets and how to secure them by highlighting important matters to consider and apply.

1. List all your domain names, digital certificates, and other digital assets

Creating a full account of your digital assets, how they are being managed, and what security measures are in place enables you to determine what to keep and what to divest. You'll also know which assets put your brand reputation or security at risk.

We recommend pulling together a team, including stakeholders from legal, IT, and marketing, to manage all digital assets and understand the following:

a. Domain names. Identify domain names owned by the business, and audit the domain portfolio for any risks or online threats. These range from ownership issues (if not using enterprise-class providers) to missing security controls built to thwart cyber attacks. Ask your registrar to assist with this. Some important questions to consider include:

- i. Which domains are critical to business?
- ii. Which have been registered for defensive reasons?
- iii. Which domains are neither of the above, but are important as they redirect to login or test pages?
- iv. What security measures are in place?

b. Security. Evaluate what additional security controls are in place to prevent domain hijacking, including whether you're protected against unauthorized changes and deletions.

- i. Has a registry lock been placed on all vital domain names?
- ii. Are you using two-factor authentication?

c. Digital certificates. Identify how secure socket layer (SSL/TLS) digital certificates are being managed and what types of digital certificate you are using.

- i. Are you using one or multiple providers? Consolidation may be needed.
- ii. Are they being reissued automatically by the vendor(s), or is renewal internal and manual?
- iii. Are you enforcing your digital certificate policy with certificate authority authorization (CAA) records?

d. Domain name system. Evaluate your DNS provider(s).

- i. What DNS provider(s) are you using?
- ii. Are domain name system security extensions (DNSSEC) in place?
- iii. Are you using a robust distributed denial of service (DDoS) solution?

The goal is to ensure no business-critical services are negatively impacted, and to decrease the possibility of a cyber attack. Ideally, all of these digital assets are centrally and securely managed by one enterprise-class provider to provide peace of mind during a merger or acquisition.

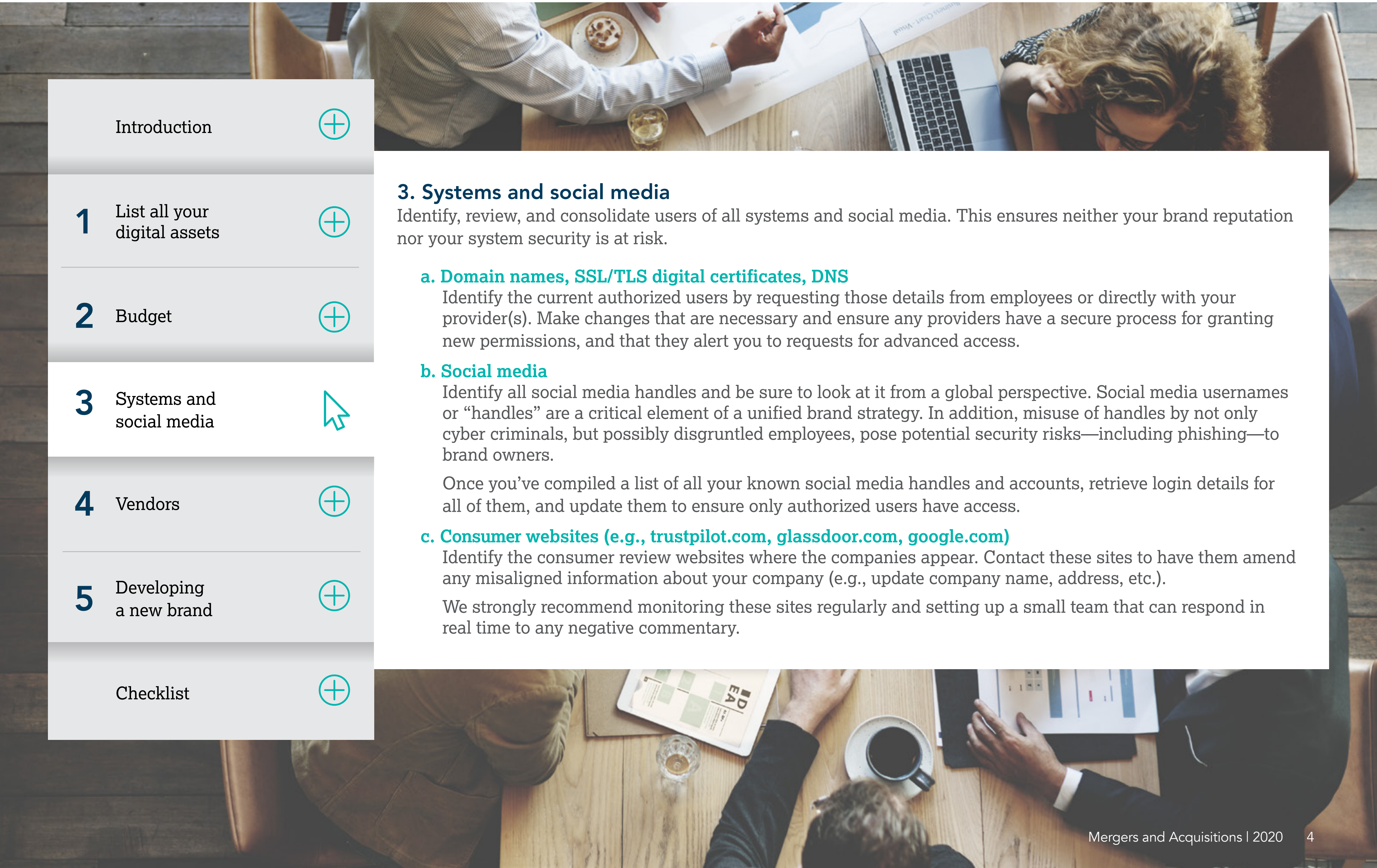
2. Budget

During a merger or acquisition, a company may go through various changes such as company name, registered address, contacts, and more.

According to domain name registration regulations, a registrant is obliged to report any changes to the contact details for both technical and administrative staff authorized to represent the organization. This includes changes to the full name, street name, house number, postal code, place of residence, email addresses, and telephone number.

Making these changes incurs costs; while these costs can be nominal per domain transaction, it can certainly add up if your company acquires a large portfolio. The additional portfolio may also be under a different domain name registrar. If so, consider the transfer-in costs if you decide to consolidate your domain names with one provider.

Furthermore, consider budget for the new brand you merged with or acquired, as this might involve registering additional domain names and monitoring those for brand abuse.



Introduction

1 List all your digital assets

2 Budget

3 Systems and social media

4 Vendors

5 Developing a new brand

Checklist

3. Systems and social media

Identify, review, and consolidate users of all systems and social media. This ensures neither your brand reputation nor your system security is at risk.

a. Domain names, SSL/TLS digital certificates, DNS

Identify the current authorized users by requesting those details from employees or directly with your provider(s). Make changes that are necessary and ensure any providers have a secure process for granting new permissions, and that they alert you to requests for advanced access.

b. Social media

Identify all social media handles and be sure to look at it from a global perspective. Social media usernames or "handles" are a critical element of a unified brand strategy. In addition, misuse of handles by not only cyber criminals, but possibly disgruntled employees, pose potential security risks—including phishing—to brand owners.

Once you've compiled a list of all your known social media handles and accounts, retrieve login details for all of them, and update them to ensure only authorized users have access.

c. Consumer websites (e.g., trustpilot.com, glassdoor.com, google.com)

Identify the consumer review websites where the companies appear. Contact these sites to have them amend any misaligned information about your company (e.g., update company name, address, etc.).

We strongly recommend monitoring these sites regularly and setting up a small team that can respond in real time to any negative commentary.

4. Vendors

Evaluate your vendors carefully. Your enterprise-level provider can help you develop or update your digital asset strategy upon a merger or new acquisition. Remember that your company's online presence is only as good as the infrastructure behind it. A good enterprise-level provider should:

a. Offer digital asset strategic advice

b. Have excellent customer service that includes 24/7 support

c. Have global reach and expertise

d. Possess technical know-how

e. Use industry-leading technology

f. Focus on security, and security education of it's employees, at all times

5. Developing a new brand

Sometimes mergers and acquisitions create an entirely new brand. To guide you through how to develop and launch a new brand, read our Developing and Launching a New Brand: Best Practices Guide.

Checklist

Audit

- ☒ Domain audit
- ☒ SSL/TLS digital certificate audit
- ☒ DNS audit

Security

- ☒ Registry locks
- ☒ Two-factor authentication
- ☒ SSL/TLS digital certificates
- ☒ DDoS mitigation
- ☒ DNSSEC
- ☒ CAA records

Budget

- ☒ Modification costs
- ☒ Transfer-in costs

Systems and social media

- ☒ Authorized users for domain portfolio, SSL/TLS digital certificates, and DNS
- ☒ Authorized users for social media handle credentials (e.g., LinkedIn®, Twitter®, Facebook®, Instagram®, etc.)
- ☒ Key consumer review websites
- ☒ Continuous monitoring of digital assets for security blind spots and brand dilution

Vendors

- ☒ Current and new vendor evaluation

CSC is the trusted provider of choice for the Forbes Global 2000 and the 100 Best Global Brands® in enterprise domain names, domain name systems (DNS), digital certificate management, as well as digital brand and fraud protection. As global companies make significant investments in their security posture, CSC can help them understand known security blind spots and help them secure their digital assets. By leveraging CSC's proprietary solutions, companies can be secure against cyber threats to their online assets, helping them avoid devastating revenue loss, brand reputation damage, or significant financial penalties because of policies like the General Data Protection Regulation. CSC also provides online brand protection—online brand monitoring plus enforcement activities—taking a holistic approach to digital asset protection, along with fraud protection services to combat phishing. Headquartered in Wilmington, Delaware, USA, since 1899, CSC has offices throughout the United States, Canada, Europe, and the Asia-Pacific region. CSC is a global company capable of doing business wherever our clients are, and we accomplish that by employing experts in every business we serve. Visit cscdbs.com.

cscdbs.com