VORLAGE ZU ABSCHNITT 2.3 DES BANDES 5A

Der Weg der Karte

Jede Tür, durch die Kartennummern ins Haus kommen, auf einem Blatt, und was an ihre Stelle tritt.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 2.3 (Leitfrage, Tabellen 1, 2, 4 und 5); Norm: Maßnahmen A 5.10, 5.14, 5.31, 8.10, 8.12 und 8.24 sowie Klausel 7.2 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes; der Sicherheitsstandard der Kartenindustrie ist kein Gesetz, er gilt über den Vertrag mit der Acquiring-Bank. Rechtsstand des Bandes: 27. September 2026.

Haus		**Acquiring-Bank**	
Verantwortliche für den ganzen Weg (benannt)		**Fragebogen der Kartenindustrie: zuletzt am · für welche Wege**	

So nutzen Sie diese Vorlage

1. Durchsuchen Sie die Postfächer von Reservierung, Verkauf und Veranstaltung nach dem Wort «Prüfnummer» und sehen Sie in die Schubladen am Reservierungsplatz nach einem Formular mit handschriftlicher Kartennummer (Teil 1). Jeder Treffer ist eine Kartennummer, die Ihr Haus hält, ohne sie zu brauchen.
2. Füllen Sie Teil 2 gemeinsam aus: Finanzleitung, Reservierung und Verkauf vor einem Blatt. Die Terminals sind die am besten geschützte Tür; die anderen kamen aus Bequemlichkeit hinzu, und niemand hat je ein Bild von allen zusammen gezeichnet.
3. Der billigste und wirksamste Weg, Kartennummern zu schützen, ist, sie nicht zu haben: Teil 3 hält fest, was das Haus nie halten sollte und was es stattdessen hält. Teil 4 stellt die Fragen, die Verantwortung, Fragebogen und Meldung betreffen.

Spalte «Im Buch»: verlangt = von der Norm oder aus dem Vertrag mit der Acquiring-Bank verlangt, wie der Band es nennt (Maßnahme oder Quelle in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Suchen

Treffer «Prüfnummer», Postfach Reservierung		**Treffer «Prüfnummer», Postfach Verkauf**	
Treffer «Prüfnummer», Postfach Veranstaltung		**Formulare mit handschriftlicher Kartennummer am Reservierungsplatz**	
Älteste aufbewahrte Formulare (Jahre)		**Formulare mit Kartendaten im Postfach (Anzahl)**	

Methode dieses Bandes: die Suche und die Zählung. Auf Sylt lagen rund zweitausend Autorisierungsformulare aus vier Jahren im Postfach der Verkaufskoordinatorin, mit vollständiger Nummer, Ablaufdatum, Prüfnummer, Unterschrift und oft einer Kopie des Ausweises. **verlangt:** Löschung, wenn Information nicht mehr gebraucht wird (A 8.10).

2 Die Türen, durch die Kartennummern ins Haus kommen

Tür	Beispiel Sylt: geschützt? · wo die Nummer blieb	Hat unser Haus diese Tür?	Geschützt? (ja · teilweise · nein)	Wo bleibt die Nummer?	Ersetzt durch · geschlossen am
Terminals an Empfang und Restaurants	ja, Verschlüsselung beim Lesen · nirgends im Haus	☐ ja ☐ nein			
Eigene Buchungsmaschine, Buchungsportale	teilweise · im Verwaltungssystem, nicht durchgehend als Token	☐ ja ☐ nein			
Telefon	nein · Garantieblätter im Ordner, mit Prüfnummer	☐ ja ☐ nein			
Fax	nein · Papierfach in der Reservierung	☐ ja ☐ nein			
Autorisierungsformular per E-Mail	nein · Postfach des Verkaufs	☐ ja ☐ nein			
Anzahlungen per E-Mail oder Telefon	nein · Postfächer, Notizzettel	☐ ja ☐ nein			
Gast liest Ziffern am Empfang vor	nein · im Ohr der Umstehenden	☐ ja ☐ nein			
weitere Tür: _____		☐ ja ☐ nein			
weitere Tür: _____		☐ ja ☐ nein			

Die sieben Türen sind Tabelle 1 des Bandes (**Beispiel aus Abschnitt 2.3**, Sylt: Nur die erste Zeile war im Fragebogen des Hauses beschrieben). **verlangt:** die gesetzlichen, regulatorischen und vertraglichen Anforderungen ermitteln, dokumentieren und aktuell halten, bei den meisten Hotels auch den Kartenstandard aus dem Bankvertrag (A 5.31); Regeln für die Übermittlung über alle Wege, E-Mail eingeschlossen (A 5.14). **Methode:** das Bild aller Türen auf einem Blatt.

3 Was ein Hotel nie halten sollte, und was es stattdessen hält

Angabe	Regel	Stattdessen	Bei uns noch vorhanden?	Abgeschafft · gelöscht am	Im Buch
Prüfnummer der Karte	nach der Autorisierung nie aufbewahren, in keiner Form	nichts; der Zahlungsdienstleister prüft sie	☐ ja ☐ nein		**verlangt:** Regeln der Kartenindustrie über den Bankvertrag (A 5.31).
Vollständige Kartennummer im Klartext	nicht in Postfächern, auf Papier oder in Notizen	Token im Verwaltungssystem	☐ ja ☐ nein		**Methode** dieses Bandes; A 8.10, 8.12.
Autorisierungsformular mit Kartendaten	nicht per E-Mail anfordern oder annehmen	Zahlungslink an das Unternehmen	☐ ja ☐ nein		**Methode** dieses Bandes; Regeln für E-Mail (A 5.14).
Ausweiskopie des Karteninhabers	nicht zur Zahlung anfordern	starke Authentifizierung über den Link	☐ ja ☐ nein		**Methode** dieses Bandes.
Garantieblatt	abschaffen	unmittelbare Eingabe in ein Feld, das als Token speichert, oder Link	☐ ja ☐ nein		**Methode** dieses Bandes.

Der Verzicht auf die Speicherung kann den Prüfumfang des Kartenstandards verringern; Systeme nimmt er nicht automatisch aus dem Anwendungsbereich: Verarbeitung, Übertragung, Verbindungen und sicherheitsrelevante Einflüsse bleiben zu prüfen. Auch ausgelagerte Zahlungen entbinden das Haus nicht von allen Pflichten; das Ausmaß stimmt es mit der Acquiring-Bank oder der Stelle ab, die die Validierung annimmt.

4 Die Fragen, die der Weg stellt

Nr.	Frage	Grund (aus dem Band)	Im Buch	Eintrag
1	Wer verantwortet den ganzen Weg der Kartendaten, von den Terminals über Telefon und Formulare bis zu den Postfächern?	Jeder führte seinen Teil gut, und die Lücken zwischen ihnen waren die Orte, an denen die Kartennummern offen lagen.	**verlangt:** vertragliche Anforderungen ermittelt, dokumentiert, aktuell (A 5.31). **Methode:** eine Verantwortliche für den ganzen Weg.	
2	Beruht der jährliche Fragebogen auf dem vollständigen Bild der Kartenwege oder nur auf den Terminals?	Ein Fragebogen ist nur so richtig wie das Bild der Kartenwege, auf dem er beruht.	**verlangt:** Nachweis der Einhaltung nach dem Kartenstandard über den Bankvertrag. **Methode:** das vollständige Bild.	
3	Sind Token im Verwaltungssystem und der sichere Zahlungslink für Reservierung und Verkauf eingeschaltet, soweit der Vertrag sie enthält?	Beides war in den Verträgen des Hauses enthalten; keines war eingeschaltet, weil niemand darum gebeten hatte.	**Methode** dieses Bandes; Kryptografie nach Regeln (A 8.24): Token verringern das Vorkommen von Kartennummern, Verschlüsselung und Schlüsselverwaltung sind getrennt nachzuweisen.	
4	Werden Kartendaten per E-Mail nie angenommen, und gibt es eine Vorlage für die Antwort, die dem Absender den sicheren Weg nennt?	Kartendaten, die trotzdem per E-Mail kommen, werden sofort gelöscht, und der Absender erfährt, wie er sicher zahlen kann.	**verlangt:** Regeln für die Übermittlung (A 5.14). Die Vorlage: möglicher Nachweis.	
5	Sind die Postfächer durchsucht und bereinigt, sind alte Formulare und E-Mails gelöscht, mit Nachweis?	Ein Postfach, das Kartennummern hält, ist in der Sache eine ungeschützte Kartendatenbank, von überall mit einem Passwort erreichbar.	**verlangt:** Löschung (A 8.10), Schutz gegen Datenabfluss (A 8.12).	
6	Sind Reservierung und Verkauf in Token und Zahlungslinks geschult?	Die sichereren Werkzeuge waren vorhanden und ungenutzt, und das Personal war nicht darin geschult.	**verlangt:** Befähigung (7.2), Regeln für die Nutzung von Information (A 5.10).	
7	Wer meldet bei einem Abfluss, wem, und ab wann läuft die Frist?	Die Frist beginnt nicht mit dem Bericht des Ermittlers, sondern mit dem Brief der Bank, sobald das Haus Grund hat anzunehmen, dass seine Daten betroffen sind.	**verlangt:** Recht, siehe Teil 5. Wer meldet: Methode.	

5 Was das Recht zur Karte sagt

Ebene	Deutschland	Österreich	Schweiz
Meldung eines Abflusses	Aufsichtsbehörde unverzüglich und möglichst binnen 72 Stunden ab Kenntnis, außer bei voraussichtlich unwahrscheinlichem Risiko (Art. 33 DSGVO); Betroffene unverzüglich bei voraussichtlich hohem Risiko, vorbehaltlich gesetzlicher Ausnahmen (Art. 34)	ebenso, Datenschutzbehörde	EDÖB bei voraussichtlich hohem Risiko (revDSG Art. 24); Betroffene, wenn zu ihrem Schutz nötig
Telefonische und schriftliche Kartenangaben	bei echten Post- oder Telefonaufträgen nach der Auslegung der Europäischen Bankenaufsicht nicht von der starken Authentifizierung erfasst; nicht jede schriftliche oder elektronische Anweisung ist einem solchen Auftrag gleichzusetzen; Risiko der Rückbuchung vertraglich meist beim Händler	ebenso	vertraglich geregelt
Vom Hotel ausgelöste Belastungen (No-Show, Nebenkosten)	starke Authentifizierung bei Erteilung des Mandats über einen Fernkanal; spätere Belastungen darauf gestützt	ebenso	vertraglich geregelt

Informationen dürfen schrittweise geliefert werden: Das Haus auf Sylt meldete am dritten Tag nach dem Brief der Bank, mit dem Hinweis, die Untersuchung laufe und Angaben würden nachgereicht. Ein Zahlungslink mit starker Kundenauthentifizierung verschiebt in der Regel das Risiko einer späteren Rückbuchung vom Hotel zur ausgebenden Bank; die Garantie, die am Telefon diktiert wurde, trägt es meist beim Hotel.

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch den Kartenstandard noch eine Rechtsberatung und ist kein Nachweis: Ein ausgefülltes Blatt belegt weder, dass eine Tür geschlossen ist, noch, dass der Fragebogen der Kartenindustrie richtig ausgefüllt wurde, noch die Einhaltung des Standards; dafür gelten der Vertrag mit der Acquiring-Bank und die Stelle, die die Validierung annimmt. Suche, Bild der Türen und Fragen in dieser Form sind Methode dieses Bandes, keine Anforderung. Die Angaben zum Recht geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026).