

## **BAB II**

### **KAJIAN PUSTAKA, KERANGKA PEMIKIRAN DAN HIPOTESIS PENELITIAN**

#### **2.1 Kajian Pustaka**

##### **2.1.1 Landasan Teori**

Dalam penelitian ini, teori yang digunakan sebagai landasan konseptual adalah *Protection Motivation Theory* (PMT) yang dikembangkan oleh (Rogers, 1975). Teori ini menjelaskan bagaimana individu merespons ancaman melalui proses evaluasi kognitif yang terdiri dari dua komponen utama, yaitu *threat appraisal* dan *coping appraisal*.

*Threat appraisal* berkaitan dengan penilaian individu terhadap tingkat ancaman, yang meliputi persepsi terhadap tingkat keparahan dampak (*perceived severity*) dan kemungkinan terjadinya ancaman (*perceived vulnerability*). Sementara itu, *coping appraisal* berkaitan dengan evaluasi individu terhadap kemampuannya dalam menghadapi ancaman, yang mencakup keyakinan terhadap efektivitas respons (*response efficacy*), keyakinan terhadap kemampuan diri (*self-efficacy*), serta pertimbangan terhadap hambatan tindakan (*response cost*).

Pada penggunaan QRIS oleh UKM *food and beverage*, risiko penipuan digital dipandang sebagai bentuk ancaman yang memerlukan respons protektif. Literasi digital dan perilaku keamanan berperan dalam meningkatkan kapasitas pelaku usaha untuk mengevaluasi dan merespons risiko tersebut, sedangkan *user awareness* mencerminkan proses kognitif dalam mengenali potensi ancaman.

Proses ini pada akhirnya memengaruhi kemampuan mitigasi risiko sebagai *outcome* perlindungan.

## **2.1.2 Literasi Digital**

### **2.1.2.1 Pengertian Literasi digital**

Gilster, (1997) mendefinisikan literasi digital sebagai *“the ability to understand and use information in multiple formats from a wide range of sources when it is presented via a computer,”* yang dapat diartikan sebagai kemampuan untuk memahami dan menggunakan informasi dalam berbagai format dari beragam sumber yang disajikan melalui komputer. Definisi ini menekankan bahwa literasi digital tidak hanya berkaitan dengan kemampuan teknis menggunakan perangkat, tetapi juga kemampuan memahami, menilai, dan memanfaatkan informasi digital secara efektif.

Literasi digital merupakan kompetensi yang semakin penting dalam era transformasi digital, terutama seiring meningkatnya pemanfaatan teknologi dalam berbagai aktivitas ekonomi dan sosial. Konsep literasi digital berkembang sejalan dengan integrasi teknologi digital dalam kehidupan sehari-hari, termasuk dalam layanan keuangan berbasis elektronik. Menurut (Bawden, 2008), literasi digital didefinisikan sebagai:

*“Digital literacy is the knowledge, skills and understanding that individuals require in order to use digital tools and resources effectively.”*

Definisi tersebut menegaskan bahwa literasi digital mencakup pengetahuan, keterampilan, dan pemahaman yang diperlukan individu untuk menggunakan teknologi digital secara efektif. Literasi digital tidak hanya terbatas pada

kemampuan teknis dalam mengoperasikan perangkat, tetapi juga meliputi kemampuan memahami, mengevaluasi, serta memanfaatkan sumber daya digital secara optimal.

UNESCO, (2021) memperluas pemahaman tersebut dengan menyatakan bahwa literasi digital mencakup kemampuan mengakses, mengelola, mengevaluasi, serta menciptakan informasi secara aman dan bertanggung jawab melalui teknologi digital. Dengan demikian, literasi digital tidak hanya mencakup kemampuan teknis, tetapi juga melibatkan aspek keamanan serta etika dalam penggunaan teknologi.

Dalam penelitian usaha mikro, kecil, dan menengah (UMKM), literasi digital berkaitan dengan kemampuan pelaku usaha dalam memahami serta memanfaatkan teknologi digital untuk mendukung aktivitas bisnis, seperti penggunaan platform digital, pemasaran daring, serta pengelolaan informasi usaha secara elektronik. Literasi digital juga berperan penting dalam meningkatkan kinerja UMKM melalui pemanfaatan teknologi digital dalam kegiatan usaha (Novela et al., 2024).

Pada sistem pembayaran digital, literasi digital mencakup pemahaman mengenai cara kerja QRIS, kemampuan mengenali berbagai ancaman keamanan seperti *quishing*, serta pemahaman terhadap praktik keamanan yang diperlukan. (van Deursen & van Dijk, 2019) menekankan pentingnya literasi digital dalam layanan keuangan digital:

*"Digital literacy for financial services requires not only the ability to use payment tools but also the understanding of security risks and the capacity to protect oneself from financial fraud"*

Berdasarkan berbagai pendapat tersebut, literasi digital dalam penelitian ini diartikan sebagai kemampuan pelaku UKM *food and beverage* yang mencakup pengetahuan, keterampilan teknis, serta kemampuan dalam memahami dan mengevaluasi informasi digital untuk menggunakan sistem pembayaran QRIS secara efektif dan aman.

Dalam perspektif *Protection Motivation Theory* (PMT), literasi digital membantu individu dalam melakukan *cognitive appraisal* terhadap ancaman digital, khususnya dalam memahami tingkat keparahan dan kemungkinan terjadinya ancaman pada penggunaan QRIS. Semakin tinggi literasi digital pengguna, semakin baik kemampuan pengguna dalam mengenali risiko keamanan digital dan membentuk *protection motivation* untuk melakukan tindakan protektif.

#### **2.1.2.2 Faktor-faktor yang Mempengaruhi Literasi Digital**

Literasi digital tidak terbentuk secara instan, melainkan berkembang melalui berbagai kondisi yang mendukung kemampuan individu dalam memanfaatkan teknologi. Kemampuan ini dipengaruhi oleh interaksi antara pengalaman penggunaan teknologi, ketersediaan akses, serta tingkat keterlibatan individu dalam aktivitas digital (Helsper & Eynon, 2010; van Deursen & van Dijk, 2019).

Berdasarkan kajian tersebut, beberapa faktor yang mempengaruhi literasi digital antara lain sebagai berikut:

### **1. Pengalaman Penggunaan Teknologi Digital**

Pengalaman menggunakan perangkat digital seperti komputer, *smartphone*, maupun aplikasi berbasis internet dapat meningkatkan kemampuan individu dalam memahami serta mengoperasikan teknologi digital. Semakin sering individu berinteraksi dengan teknologi digital, semakin berkembang pula keterampilan dalam menggunakan berbagai layanan digital.

### **2. Akses terhadap Teknologi dan Internet**

Ketersediaan perangkat digital serta konektivitas internet menjadi faktor penting dalam perkembangan literasi digital. Individu yang memiliki akses yang memadai terhadap teknologi digital memiliki kesempatan yang lebih besar untuk mempelajari serta memanfaatkan teknologi tersebut dalam berbagai aktivitas.

### **3. Intensitas Penggunaan Teknologi Digital**

Tingkat keterlibatan individu dalam aktivitas digital juga mempengaruhi kemampuan digital yang dimiliki. Individu yang secara aktif menggunakan teknologi digital dalam kehidupan sehari-hari cenderung memiliki kemampuan yang lebih baik dalam memahami serta memanfaatkan teknologi digital secara efektif.

### **4. Pelatihan dan Edukasi Digital**

Partisipasi dalam pelatihan atau program edukasi digital dapat meningkatkan kemampuan individu dalam memahami serta memanfaatkan teknologi digital. Program pelatihan digital memberikan pengetahuan dan keterampilan praktis yang membantu pengguna memahami penggunaan

teknologi secara lebih efektif, termasuk dalam memanfaatkan sistem pembayaran digital dalam kegiatan usaha.

Pada pelaku UKM *food and beverage*, faktor-faktor tersebut berperan dalam meningkatkan kemampuan pelaku usaha dalam memahami penggunaan teknologi digital serta memanfaatkan sistem pembayaran seperti QRIS secara lebih efektif dan aman dalam aktivitas bisnis.

### **2.1.2.3 Manfaat Literasi Digital**

Literasi digital memberikan dampak langsung yang dirasakan pelaku usaha dalam aktivitas sehari-hari, khususnya dalam penggunaan sistem pembayaran digital. (Bawden, 2008) menjelaskan bahwa literasi digital membantu individu memahami, mengevaluasi, serta memanfaatkan informasi digital secara lebih kritis dan bertanggung jawab. Beberapa manfaat yang dapat diperoleh pelaku UKM *food and beverage* antara lain sebagai berikut:

#### **1. Meningkatkan kemampuan menggunakan teknologi digital**

Literasi digital membantu individu memahami cara menggunakan perangkat digital seperti komputer, smartphone, serta berbagai aplikasi berbasis teknologi secara lebih efektif. Kemampuan ini memungkinkan pengguna memanfaatkan teknologi digital untuk berbagai kebutuhan, seperti komunikasi, pencarian informasi, maupun penggunaan layanan digital dalam kegiatan usaha (Gilster, 1997).

## **2. Membantu memahami dan mengevaluasi informasi digital**

Literasi digital memungkinkan individu untuk mengakses, memahami, serta mengevaluasi informasi yang diperoleh melalui media digital secara kritis. Kemampuan tersebut membantu individu membedakan informasi yang akurat dan dapat dipercaya dari informasi yang tidak valid, sehingga informasi digital dapat dimanfaatkan secara tepat dalam berbagai aktivitas (Bawden, 2008).

## **3. Mendukung pemanfaatan teknologi digital dalam kegiatan usaha**

Literasi digital membantu individu memanfaatkan berbagai layanan digital untuk mendukung aktivitas ekonomi dan bisnis. Kemampuan ini memungkinkan pelaku usaha menggunakan teknologi digital dalam pengelolaan transaksi, pemasaran, maupun komunikasi dengan konsumen secara lebih efektif sehingga dapat meningkatkan efisiensi dalam kegiatan usaha (van Deursen & van Dijk, 2019).

## **4. Meningkatkan kesadaran terhadap keamanan digital**

Literasi digital membantu individu memahami potensi risiko yang dapat muncul dalam penggunaan teknologi digital, seperti penipuan digital, penyalahgunaan data, maupun ancaman keamanan lainnya. Dengan pemahaman tersebut, pengguna dapat lebih berhati-hati dalam menggunakan teknologi digital serta menerapkan praktik penggunaan teknologi yang lebih aman (Ng, 2012).

#### **2.1.2.4 Tujuan Literasi Digital**

Berbeda dari manfaat yang bersifat langsung dan operasional, tujuan literasi digital merujuk pada arah pengembangan kemampuan individu secara lebih luas dalam menghadapi transformasi digital. Literasi digital bertujuan membentuk individu yang mampu berpikir kritis, menghindari informasi yang menyesatkan, serta memahami aspek keamanan dalam penggunaan teknologi digital (Naufal, 2021). Tujuan-tujuan tersebut relevan bagi pelaku UKM *food and beverage* sebagai landasan dalam membangun kapasitas digital yang berkelanjutan, sebagai berikut:

##### **1. Mendorong pemanfaatan teknologi digital secara optimal**

Literasi digital bertujuan membekali individu dengan kemampuan untuk mengintegrasikan teknologi digital dalam berbagai aspek kegiatan usaha secara efektif dan berkelanjutan.

##### **2. Mengembangkan kemampuan berpikir kritis**

Literasi digital mendorong individu untuk menilai kebenaran, relevansi, dan kredibilitas informasi yang diperoleh dari media digital sehingga tidak mudah terpengaruh oleh informasi yang menyesatkan.

##### **3. Membentuk pengelolaan informasi digital yang bertanggung jawab**

Literasi digital bertujuan membangun kemampuan individu dalam mengelola, menyaring, dan memanfaatkan informasi digital secara tepat dan bertanggung jawab dalam setiap aktivitas usaha.

##### **4. Mendorong partisipasi aktif dalam ekonomi digital**

Literasi digital membekali individu dengan kemampuan untuk terlibat secara aktif dalam berbagai aktivitas digital, termasuk penggunaan layanan

keuangan dan sistem pembayaran berbasis teknologi (Sunuantari et al., 2021).

## **5. Mempersiapkan adaptasi terhadap transformasi digital**

Literasi digital membantu individu dan pelaku usaha beradaptasi dengan perkembangan teknologi serta perubahan model aktivitas ekonomi di era digital (Saragih et al., 2024).

Dalam konteks penelitian ini, tujuan literasi digital tersebut relevan bagi pelaku UKM *food and beverage* dalam mendukung penggunaan QRIS secara efektif, aman, dan adaptif terhadap perkembangan transaksi digital.

### **2.1.2.5 Indikator Literasi Digital**

Menurut Gilster (1997), literasi digital terdiri dari empat indikator utama, yaitu *internet searching*, *hypertextual navigation*, *content evaluation*, dan *knowledge assembly*. Keempat indikator tersebut menggambarkan kemampuan dalam mencari informasi, menelusuri sumber digital, mengevaluasi kualitas informasi, serta mengolah informasi menjadi pengetahuan yang utuh. Indikator ini juga telah digunakan dalam penelitian untuk mengukur tingkat literasi digital pada pelaku UMKM (Farhan et al., 2022). Dalam penelitian ini, indikator tersebut digunakan untuk menjelaskan literasi digital pada pelaku UKM *food and beverage* dengan penjelasan sebagai berikut:

#### **1. Kemampuan mencari informasi di internet (*internet searching*)**

Kemampuan ini merujuk pada kemampuan pelaku UKM *food and beverage* dalam mencari informasi melalui internet, seperti informasi keamanan QRIS, tren usaha, harga bahan baku, strategi pemasaran, dan peluang usaha.

## **2. Kemampuan menggunakan platform digital (*hypertextual navigation*)**

Kemampuan ini menunjukkan kemampuan pelaku UKM *food and beverage* dalam menggunakan berbagai media digital, seperti website, marketplace, media sosial, dan aplikasi pembayaran digital untuk mendukung kegiatan usaha.

## **3. Kemampuan menilai informasi digital (*content evaluation*)**

Kemampuan ini menunjukkan kemampuan pelaku UKM *food and beverage* dalam menilai kebenaran dan kepercayaan informasi yang diperoleh dari internet agar tidak mudah terpengaruh oleh informasi palsu, penipuan digital, atau promosi yang menyesatkan.

## **4. Kemampuan mengolah informasi digital (*knowledge assembly*)**

Kemampuan ini merujuk pada kemampuan pelaku UKM *food and beverage* dalam menggabungkan informasi dari berbagai sumber untuk membentuk pemahaman yang lebih baik dalam mengelola usaha dan memahami risiko penggunaan QRIS.

### **2.1.3 Perilaku Keamanan**

#### **2.1.3.1 Pengertian Perilaku Keamanan**

Perilaku keamanan (*security hygiene practices*), yang juga dikenal sebagai *cyber hygiene* merupakan konsep dalam keamanan siber yang berkaitan dengan tindakan individu maupun organisasi dalam menjaga keamanan sistem informasi. Konsep ini mencakup berbagai kebiasaan yang dilakukan secara rutin untuk melindungi perangkat, jaringan, dan data dari ancaman siber. Dalam literatur, *cyber*

*hygiene* dipahami sebagai praktik rutin yang dilakukan untuk menjaga keamanan aset digital. Sebagaimana dinyatakan bahwa “*cyber hygiene refers to routine practices that ensure the safety and security of digital assets*” (Sharma, 2023).

Selain itu, *cyber hygiene* juga dipahami sebagai kombinasi perilaku yang bertujuan untuk meningkatkan keamanan data dan melindungi dari berbagai ancaman siber. Hasan et al, 2023 menegaskan bahwa “*cyber hygiene is a combination of behaviors to enhance data privacy, prevent data loss, and protect from various cyber threats*”. Definisi ini menekankan bahwa perilaku keamanan tidak hanya berkaitan dengan tindakan teknis, tetapi juga kebiasaan pengguna dalam menjaga keamanan secara berkelanjutan.

Vishwanath et al., (2020) menjelaskan bahwa *cyber hygiene* merupakan praktik keamanan yang dilakukan secara rutin oleh pengguna untuk melindungi perangkat dan informasi dari ancaman digital. Konsep ini bersifat multidimensi karena mencakup berbagai aspek perilaku dalam penggunaan teknologi, seperti keamanan perangkat, pengelolaan kredensial, serta kewaspadaan dalam aktivitas *online*. Hal ini menunjukkan bahwa perilaku keamanan tidak berdiri sendiri, tetapi terdiri dari berbagai tindakan yang saling berkaitan.

Dalam praktiknya, perilaku keamanan dapat dilihat dari berbagai tindakan seperti penggunaan kata sandi yang kuat, pembaruan sistem secara berkala, serta kehati-hatian dalam mengakses email dan internet. Tindakan-tindakan tersebut berperan penting dalam mengurangi risiko serangan siber, karena banyak insiden keamanan terjadi akibat kesalahan atau kelalaian pengguna (Sharma, 2023; Vishwanath et al., 2020). Hal ini juga sejalan dengan penelitian (Parsons et al.,

2017) yang menyatakan bahwa faktor manusia merupakan salah satu penyebab utama terjadinya pelanggaran keamanan sistem informasi.

Berdasarkan berbagai pendapat tersebut, perilaku keamanan dapat dipahami sebagai kebiasaan dan tindakan pengguna dalam menjaga keamanan perangkat, data, akun, serta aktivitas digital dari berbagai ancaman siber. Perilaku ini tidak hanya mencakup aspek teknis, tetapi juga mencerminkan kebiasaan pengguna dalam menerapkan praktik keamanan secara konsisten.

Pada Usaha Kecil dan Menengah (UKM), perilaku keamanan menjadi penting seiring meningkatnya penggunaan teknologi digital dalam aktivitas bisnis. ENISA (2021) menjelaskan bahwa UKM rentan terhadap ancaman siber karena keterbatasan kontrol keamanan dan belum optimalnya penerapan praktik keamanan dasar. Oleh karena itu, pelaku UKM *food and beverage* pengguna QRIS memerlukan perilaku keamanan yang memadai untuk menjaga keamanan transaksi digital dan meminimalkan risiko penipuan.

Dalam *Protection Motivation Theory (PMT)*, perilaku keamanan berkaitan dengan *coping appraisal*, yaitu penilaian individu terhadap efektivitas tindakan perlindungan dalam menghadapi ancaman. Dengan demikian, penerapan *security hygiene practices* pada penggunaan QRIS mencerminkan respons protektif pengguna terhadap risiko keamanan transaksi digital.

#### **2.1.3.2 Faktor-faktor yang Mempengaruhi Perilaku Keamanan**

Perilaku keamanan (*security hygiene practices*) dipengaruhi oleh berbagai faktor yang berkaitan dengan karakteristik individu dalam menggunakan teknologi

digital. Dalam literatur keamanan informasi, perilaku pengguna tidak hanya ditentukan oleh aspek teknis, tetapi juga oleh faktor kognitif, pengalaman, serta persepsi individu terhadap risiko keamanan (Bulgurcu et al., 2010; Parsons et al., 2017; Vishwanath et al., 2020) . Adapun beberapa faktor yang dapat mempengaruhi perilaku keamanan antara lain sebagai berikut:

### **1. Pengetahuan (*Knowledge*)**

Pengetahuan berkaitan dengan tingkat pemahaman individu terhadap teknologi dan ancaman siber. Individu yang memiliki pengetahuan yang baik cenderung lebih mampu mengenali risiko serta menerapkan langkah-langkah keamanan yang tepat. Penelitian menunjukkan bahwa pengetahuan keamanan informasi berpengaruh terhadap kepatuhan dan perilaku keamanan pengguna (Parsons et al., 2017).

### **2. Pengalaman terhadap Ancaman Siber**

Pengalaman sebelumnya, seperti pernah mengalami serangan siber atau penipuan digital, dapat meningkatkan kewaspadaan individu sehingga lebih berhati-hati dalam menggunakan teknologi. Vishwanath et al., (2020) menjelaskan bahwa pengalaman dan paparan terhadap risiko digital dapat membentuk kebiasaan *cyber hygiene* yang lebih baik.

### **3. Persepsi Risiko (*Risk Perception*)**

Persepsi risiko mencerminkan bagaimana individu menilai tingkat bahaya dari ancaman siber. Semakin tinggi persepsi risiko, maka semakin besar kecenderungan individu untuk menerapkan perilaku keamanan. Hal ini sejalan dengan pendekatan *Protection Motivation Theory* yang menyatakan

bahwa persepsi risiko mempengaruhi perilaku protektif individu (Bulgurcu et al., 2010).

#### **4. Penggunaan Teknologi**

Intensitas penggunaan teknologi digital dapat meningkatkan paparan individu terhadap berbagai risiko keamanan siber. Semakin sering individu berinteraksi dengan teknologi, semakin besar kemungkinan terpapar terhadap potensi ancaman digital. Hal ini mendorong pentingnya penerapan praktik keamanan dalam aktivitas digital (Vishwanath et al., 2020).

##### **2.1.3.3 Manfaat Perilaku Keamanan**

Perilaku keamanan (*security hygiene practices*) memiliki peran penting dalam menjaga keamanan sistem informasi, baik pada tingkat individu maupun organisasi. Dalam literatur keamanan informasi, perilaku pengguna menjadi salah satu faktor yang berkaitan dengan keberhasilan perlindungan sistem dari berbagai ancaman siber. Adapun beberapa peran perilaku keamanan antara lain sebagai berikut:

##### **1. Mendukung perlindungan sistem dan informasi**

Perilaku keamanan memberikan perlindungan langsung terhadap aktivitas transaksi digital, khususnya dalam mencegah akses tidak sah terhadap akun dan data pembayaran yang digunakan dalam penggunaan QRIS sehari-hari (Hasan et al., 2023).

## **2. Mengurangi potensi terjadinya pelanggaran keamanan**

Penerapan perilaku keamanan secara konsisten memberikan manfaat langsung berupa berkurangnya paparan risiko penipuan digital dalam aktivitas transaksi, karena pelaku usaha yang memiliki kebiasaan keamanan yang baik cenderung lebih cepat mendeteksi indikasi ancaman (Vishwanath et al., 2020).

## **3. Mendukung efektivitas kebijakan keamanan organisasi**

Dalam lingkungan organisasi, perilaku pengguna berperan dalam mendukung keberhasilan implementasi kebijakan keamanan. Pengguna yang memiliki perilaku keamanan yang baik cenderung lebih patuh terhadap aturan yang ditetapkan, sehingga kebijakan keamanan dapat berjalan lebih efektif (Sharma, 2023).

## **4. Membentuk kebiasaan keamanan dalam penggunaan teknologi**

Penerapan *cyber hygiene* secara konsisten berkaitan dengan pembentukan kebiasaan pengguna dalam menjaga keamanan digital. Kebiasaan ini mencerminkan praktik keamanan yang dilakukan secara berulang dalam aktivitas sehari-hari, sehingga mendukung terciptanya perilaku yang lebih aman dalam penggunaan teknologi (Vishwanath et al., 2020).

## **5. Meningkatkan kewaspadaan terhadap risiko keamanan**

Perilaku keamanan juga berkaitan dengan tingkat kesadaran individu terhadap ancaman siber. Individu yang memiliki kesadaran keamanan yang lebih baik cenderung menunjukkan sikap yang lebih berhati-hati dalam menggunakan teknologi digital (Bada & Nurse, 2019).

#### 2.1.3.4 Tujuan Perilaku Keamanan

Perilaku keamanan (*security hygiene practices*) bertujuan untuk menjaga keamanan sistem informasi melalui penerapan praktik keamanan yang konsisten dan berkelanjutan. Dalam literatur keamanan siber, praktik *cyber hygiene* berkaitan dengan upaya menjaga keamanan sistem, melindungi data, serta mengurangi risiko ancaman digital melalui kebiasaan pengguna yang aman (ENISA, 2016; Vishwanath et al., 2020). Berdasarkan konsep tersebut, tujuan perilaku keamanan dapat diuraikan sebagai berikut:

##### 1. Melindungi sistem dan data dari ancaman siber

Perilaku keamanan berkaitan dengan upaya menjaga kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Prinsip ini merupakan dasar dalam keamanan informasi yang digunakan untuk melindungi sistem dan data dari berbagai ancaman (National Institute of Standards & Technology, 2020).

##### 2. Mengurangi kerentanan (*vulnerabilities*) dalam sistem informasi

Penerapan praktik keamanan seperti pembaruan sistem dan pengelolaan akses berkaitan dengan upaya mengurangi celah keamanan dalam sistem. Hal ini sejalan dengan praktik *cyber hygiene* yang menekankan tindakan preventif untuk menjaga keamanan sistem (ENISA, 2016).

##### 3. Menjaga kesehatan dan stabilitas sistem (*system health*)

Perilaku keamanan juga berkaitan dengan pemeliharaan sistem melalui praktik rutin seperti pembaruan perangkat lunak dan *monitoring* sistem. Hal

ini mencerminkan konsep *cyber hygiene* yang menekankan praktik berkelanjutan dalam menjaga kondisi sistem (Vishwanath et al., 2020).

#### 4. **Mencegah terjadinya pelanggaran keamanan (*security breach*)**

Perilaku keamanan bertujuan membangun sistem pencegahan yang terstruktur dan berkelanjutan terhadap berbagai bentuk pelanggaran keamanan, termasuk kebocoran data dan akses tidak sah dalam sistem pembayaran digital (ENISA, 2016).

#### 2.1.3.5 Indikator Perilaku Keamanan

Indikator perilaku keamanan dalam penelitian ini mengacu pada *Security Behavior Intentions Scale* (SeBIS) yang digunakan oleh (Baottong et al., 2025) dalam konteks sistem pembayaran digital berbasis *QR Code* di Indonesia, serta diperkuat dengan indikator dari (CISA, 2024) . Adapun indikator perilaku keamanan yang digunakan dalam penelitian ini adalah sebagai berikut:

1. **Pengelolaan Kata Sandi (*Password Management*)**, yaitu tindakan pengguna dalam melindungi akun digital melalui penggunaan kata sandi yang kuat dan unik serta penerapan kebijakan penggantian kata sandi secara berkala untuk mencegah akses tidak sah dalam transaksi.
2. **Pembaruan Perangkat Lunak (*Software Updates*)**, yaitu kebiasaan pengguna dalam melakukan pembaruan sistem operasi dan aplikasi secara rutin guna menutup celah keamanan yang dapat dieksploitasi dalam penggunaan sistem pembayaran digital.

3. **Perilaku Keamanan Perangkat (*Device Security Behavior*)**, yaitu tindakan aktif pengguna dalam mengamankan perangkat yang digunakan untuk bertransaksi, seperti penggunaan perangkat lunak antivirus, penguncian layar, serta penerapan autentikasi dua faktor sebagai lapisan perlindungan tambahan.
4. **Perlindungan Data dan Pengelolaan Akses**, yaitu kemampuan pengguna dalam menjaga kerahasiaan data pribadi serta mengatur hak akses informasi secara tepat sesuai prinsip keamanan informasi guna mencegah kebocoran data dalam aktivitas transaksi digital.

#### 2.1.4 *User Awareness*

##### 2.1.4.1 Pengertian *User Awareness*

Dalam penelitian ini, *user awareness* difokuskan pada aspek keamanan informasi yang berkaitan dengan *cybersecurity awareness* atau *information security awareness (ISA)*, yaitu pemahaman individu terhadap ancaman dan risiko keamanan dalam penggunaan teknologi digital.

*User awareness* atau kesadaran pengguna merupakan tingkat pemahaman individu terhadap ancaman keamanan informasi serta perannya dalam menjaga keamanan sistem (Hwang et al., 2021). Kesadaran ini mencakup kemampuan individu dalam mengenali potensi risiko, memahami kebijakan keamanan, serta menyadari pentingnya keamanan dalam penggunaan teknologi digital (Grobler et al., 2021). Dengan demikian, *user awareness* bersifat kognitif, yaitu berkaitan

dengan pengetahuan dan kesadaran individu, bukan sekadar tindakan atau perilaku yang ditampilkan dalam aktivitas digital sehari-hari (Khando et al., 2021).

Khando et al., (2021) menegaskan bahwa *information security awareness* (ISA) merupakan salah satu aspek kritis dalam melindungi aset sistem informasi organisasi dari eksploitasi faktor manusia yang secara langsung maupun tidak langsung menyebabkan sebagian besar insiden keamanan. Definisi ini menegaskan bahwa *user awareness* merupakan konstruk kognitif yang berfokus pada pemahaman dan pengetahuan individu terhadap isu keamanan informasi beserta konsekuensinya, yang membedakannya dari perilaku keamanan yang bersifat tindakan nyata.

Hwang et al., (2021) menjelaskan bahwa kesadaran keamanan merupakan "*the first step in information security compliance behavior*", yang menunjukkan bahwa sebelum individu dapat menerapkan perilaku keamanan, diperlukan terlebih dahulu pemahaman dan kesadaran terhadap kebijakan keamanan serta tanggung jawabnya. Pernyataan ini menunjukkan bahwa *user awareness* berperan sebagai dasar yang mendukung terbentuknya perilaku keamanan, di mana individu cenderung dapat menerapkan praktik keamanan secara lebih konsisten apabila memiliki pemahaman kognitif yang memadai.

Selain itu, Grobler et al., (2021) menjelaskan bahwa komponen pengguna dalam keamanan siber dipengaruhi oleh tingkat kesadaran keamanan, pengalaman, karakteristik individu, serta cara pengguna memandang risiko keamanan siber. Rendahnya *user awareness* dapat meningkatkan risiko pelanggaran keamanan akibat kelalaian pengguna, sedangkan pengguna dengan kesadaran yang baik

cenderung lebih peka terhadap ancaman siber seperti *phishing*, *malware*, maupun penipuan digital.

Kondisi tersebut juga relevan pada pelaku UKM *food and beverage* pengguna QRIS, karena *user awareness* yang baik dapat membantu pelaku usaha mengenali potensi risiko dan menjaga keamanan transaksi digital. Dari berbagai pendapat tersebut, *user awareness* dapat dipahami sebagai tingkat pemahaman dan kesadaran individu terhadap ancaman keamanan informasi, kebijakan keamanan, serta tanggung jawab pengguna dalam menjaga keamanan sistem dan merespons risiko secara tepat.

Dalam Protection Motivation Theory (PMT), *user awareness* berkaitan dengan *threat appraisal*, yaitu proses individu dalam menilai tingkat keparahan ancaman dan kemungkinan terpapar risiko. Pada penggunaan QRIS, kesadaran terhadap ancaman keamanan seperti *QR Code* palsu, manipulasi transaksi, atau penipuan digital dapat mendorong pengguna untuk lebih waspada dan melakukan tindakan perlindungan.

#### **2.1.4.2 Faktor – Faktor Yang Mempengaruhi *User Awareness***

*User awareness* dipengaruhi oleh berbagai faktor yang berkaitan dengan paparan informasi serta lingkungan individu dalam memahami keamanan informasi (Chaudhary et al., 2023; Hwang et al., 2021). Relevansi faktor-faktor tersebut juga terlihat pada pelaku UKM *food and beverage* yang semakin memanfaatkan teknologi digital dalam aktivitas usaha, sehingga memerlukan tingkat kesadaran yang baik terhadap keamanan informasi. Faktor-faktor tersebut antara lain:

### **1. Edukasi dan Pelatihan Keamanan (*Security Education and Training*)**

Edukasi dan pelatihan keamanan membantu meningkatkan pemahaman individu terhadap ancaman serta kebijakan keamanan, sehingga membentuk kesadaran terhadap pentingnya menjaga keamanan informasi (Chaudhary et al., 2023; Hwang et al., 2021a).

### **2. Pengaruh Lingkungan Sosial (*Social Influence*)**

Lingkungan sosial seperti rekan kerja atau komunitas dapat mempengaruhi kesadaran individu melalui interaksi dan pertukaran informasi terkait keamanan (Yazdanmehr et al., 2020).

### **3. Paparan Informasi Keamanan (*Exposure to Security Information*)**

Paparan terhadap informasi keamanan seperti kampanye, komunikasi keamanan, atau peringatan sistem menjadi sumber penting dalam meningkatkan pemahaman dan kesadaran individu terhadap ancaman keamanan (Yazdanmehr et al., 2020).

### **4. Dukungan Organisasi atau Lingkungan Kerja (*Organizational Support*)**

Dukungan dari organisasi seperti kebijakan keamanan, aturan penggunaan sistem, serta partisipasi manajemen dapat meningkatkan kesadaran pengguna terhadap pentingnya menjaga keamanan informasi (Hwang et al., 2021a).

#### **2.1.4.3 Manfaat *User Awareness***

*User awareness* memberikan berbagai manfaat dalam meningkatkan keamanan informasi, seperti meningkatkan pemahaman terhadap ancaman,

meningkatkan persepsi risiko, membentuk sikap yang lebih peduli terhadap keamanan, serta meningkatkan kemampuan individu dalam mengenali dan merespons potensi ancaman siber (Chaudhary et al., 2022; Alsharida et al., 2023).

Manfaat tersebut menjadi penting bagi pelaku UKM *food and beverage* yang semakin bergantung pada teknologi digital dalam kegiatan usaha, karena penggunaan sistem digital juga diikuti oleh meningkatnya risiko ancaman siber yang dapat memengaruhi keberlangsungan usaha. Adapun rincian manfaat dari *user awareness* adalah sebagai berikut:

- 1. Meningkatkan Pemahaman terhadap Jenis dan Sumber Ancaman Siber**

*User awareness* memberikan manfaat langsung berupa kemampuan pelaku usaha dalam mengenali berbagai bentuk ancaman yang relevan dengan transaksi QRIS, seperti quishing, manipulasi bukti pembayaran, dan penggantian kode QR palsu, sehingga potensi kerugian dapat diantisipasi sejak dini (Chaudhary et al., 2022).

- 2. Meningkatkan Persepsi terhadap Risiko Keamanan**

*User awareness* berperan dalam meningkatkan persepsi individu terhadap risiko keamanan, sehingga individu lebih memahami kemungkinan terjadinya ancaman serta dampaknya. Peningkatan persepsi risiko ini mendorong individu untuk lebih berhati-hati dalam menggunakan teknologi dan tidak mengabaikan potensi bahaya yang ada (Bada & Nurse, 2019).

### **3. Membentuk Sikap yang Lebih Peduli terhadap Keamanan Informasi**

*User awareness* memberikan dampak langsung pada perubahan sikap pelaku usaha dalam aktivitas transaksi sehari-hari, di mana kesadaran yang lebih tinggi mendorong pelaku usaha untuk lebih teliti dalam memverifikasi transaksi dan tidak mengabaikan indikasi yang mencurigakan (Bada & Nurse, 2019).

### **4. Meningkatkan Sensitivitas dalam Mengenali Indikasi Ancaman**

*User awareness* meningkatkan kemampuan individu dalam mengenali tanda-tanda atau indikasi adanya ancaman, seperti aktivitas mencurigakan, pesan yang tidak dikenal, atau perilaku sistem yang tidak normal. Kemampuan ini membantu individu dalam mengidentifikasi potensi risiko sejak dini sebelum berkembang menjadi insiden keamanan yang lebih serius (Alsharida et al., 2023).

### **5. Mendorong Kesiapan Kognitif dalam Merespons Risiko**

*User awareness* membantu individu dalam merespons ancaman secara tepat berdasarkan pemahaman yang dimiliki. Individu yang memiliki kesadaran tinggi cenderung lebih siap dalam mengambil tindakan yang sesuai, seperti menghindari aktivitas berisiko, melaporkan insiden, atau menerapkan langkah pencegahan yang diperlukan (Chaudhary et al., 2022).

#### 2.1.4.4 Tujuan *User Awareness*

*User awareness* (kesadaran pengguna) memiliki tujuan untuk mengarahkan perhatian dan kesadaran individu terhadap pentingnya keamanan informasi dalam penggunaan teknologi digital. Tujuan ini berfokus pada pembentukan kesadaran kognitif serta pola pikir individu agar lebih memperhatikan aspek keamanan sebagai bagian dari aktivitas digital. Melalui peningkatan awareness, individu diharapkan mampu memahami perannya dalam menjaga keamanan sistem serta menyadari pentingnya kepatuhan terhadap kebijakan dan aturan keamanan yang berlaku (ENISA, 2019; NIST, 2017) . Adapun tujuan dari *user awareness* antara lain sebagai berikut:

1. **Mengarahkan perhatian terhadap isu keamanan informasi**

*User awareness* bertujuan membangun fondasi kognitif yang mendorong individu untuk secara konsisten memperhatikan aspek keamanan sebagai bagian yang tidak terpisahkan dari setiap aktivitas digital, bukan sekadar respons sesaat terhadap ancaman yang sudah terjadi.

2. **Menanamkan pemahaman mengenai tanggung jawab individu**

*User awareness* bertujuan menanamkan pemahaman bahwa keamanan sistem tidak hanya bergantung pada teknologi, tetapi juga pada kesadaran dan tanggung jawab setiap pengguna secara individual.

3. **Mendorong kesadaran terhadap pentingnya kebijakan keamanan**

*User awareness* bertujuan untuk membuat individu menyadari bahwa kebijakan dan aturan keamanan merupakan bagian penting dalam menjaga

keamanan informasi, sehingga perlu diperhatikan dalam penggunaan sistem digital.

#### **4. Membentuk pola pikir yang berorientasi pada keamanan digital**

Kesadaran pengguna diarahkan untuk membangun pola pikir yang menjadikan keamanan sebagai pertimbangan dalam aktivitas digital, sehingga individu lebih peka terhadap aspek keamanan dalam berbagai situasi.

##### **2.1.4.5 Indikator *User Awareness***

Indikator *user awareness* dalam penelitian ini dikembangkan berdasarkan integrasi beberapa sumber dalam literatur keamanan informasi yang relevan dengan konteks penggunaan sistem pembayaran digital. Pengukuran *user awareness* tidak memiliki indikator baku tunggal, sehingga indikator dalam penelitian ini disusun dengan mengacu pada aspek kognitif yang mencerminkan pemahaman dan kesadaran individu terhadap ancaman keamanan dalam bertransaksi menggunakan QRIS. Adapun indikator *user awareness* yang digunakan dalam penelitian ini adalah sebagai berikut:

##### **1. Kesadaran terhadap Ancaman (*Threat Awareness*)**

Indikator ini mencerminkan tingkat kesadaran pengguna dalam mengenali dan memahami potensi ancaman siber yang dapat terjadi dalam penggunaan sistem pembayaran berbasis *QR Code*, seperti serangan *quishing* yang memanfaatkan kode QR palsu untuk mengarahkan pengguna ke situs berbahaya. Pengguna dengan *threat awareness* yang tinggi terbukti lebih

mampu mengidentifikasi tanda-tanda serangan dan mengambil tindakan pencegahan secara tepat (Baottong et al., 2025).

## **2. Kesadaran terhadap Kerentanan (*Perceived Vulnerability*)**

(Hameed & Arachchilage, 2019) Indikator ini mencerminkan kemampuan individu dalam menyadari bahwa aktivitas digital memiliki potensi risiko keamanan yang dapat terjadi. Kesadaran terhadap kerentanan membantu individu memahami kemungkinan terjadinya ancaman (Hameed & Arachchilage, 2019).

## **3. Kesadaran terhadap Konsekuensi (*Consequence Awareness*)**

(Nikolova & Jecheva, 2021) Indikator ini menunjukkan sejauh mana individu memahami dampak atau kerugian yang dapat timbul akibat pelanggaran keamanan informasi. Pemahaman terhadap konsekuensi berperan dalam meningkatkan kesadaran terhadap pentingnya keamanan (Nikolova & Jecheva, 2021).

## **4. Perhatian terhadap Keamanan Informasi (*Security Attention*)**

Indikator ini menggambarkan tingkat perhatian individu terhadap aspek keamanan dalam penggunaan teknologi digital, termasuk kepekaan terhadap ancaman dan potensi risiko yang ada (Chaudhary et al., 2023).

### **2.1.5 Kemampuan Mitigasi Risiko QRIS**

#### **2.1.5.1 Pengertian Kemampuan Mitigasi Risiko QRIS**

Mitigasi risiko merupakan upaya yang dilakukan untuk mengurangi kemungkinan terjadinya risiko serta dampak yang ditimbulkan. Dalam literatur

manajemen risiko, Hopkin, (2018) menyatakan bahwa *“risk mitigation involves selecting and implementing measures to reduce the likelihood or impact of a risk,”* yang menunjukkan bahwa mitigasi risiko berfokus pada pengendalian risiko secara efektif. Sejalan dengan itu, (ISO 31000, 2018) menjelaskan bahwa mitigasi risiko merupakan bagian dari proses *risk treatment* yang bertujuan untuk memodifikasi risiko agar berada pada tingkat yang dapat diterima.

Selain itu, mitigasi risiko juga bersifat proaktif, sebagaimana dinyatakan bahwa *“risk mitigation refers to the proactive actions taken to prevent or reduce the impact of potential risk events”* (Franch et al., 2014) . Dalam konteks sistem digital, mitigasi risiko merupakan proses yang berkelanjutan yang mencakup identifikasi, evaluasi, serta pengendalian terhadap potensi kerentanan sistem. Hal ini sejalan dengan pernyataan bahwa *“cyber risk mitigation requires continuous identification, assessment and reduction of vulnerabilities in digital systems”* (Radanliev et al., 2020) .

Dalam sistem pembayaran digital, pengelolaan risiko menjadi aspek yang sangat penting untuk menjaga keamanan transaksi dan mencegah terjadinya kerugian. Hal ini didukung oleh pernyataan bahwa *“digital payment systems require effective risk management strategies to prevent fraud and ensure transaction security”* (Arner et al., 2016). Selain itu, efektivitas mitigasi risiko tidak hanya ditentukan oleh teknologi, tetapi juga oleh kemampuan pengguna dalam memahami serta mengantisipasi potensi risiko yang ada (ENISA, 2019).

Kondisi tersebut menjadi semakin penting pada penggunaan QRIS sebagai sistem pembayaran berbasis kode QR yang digunakan secara luas dalam aktivitas

transaksi, termasuk oleh UKM *food and beverage*. Penggunaan QRIS tanpa diimbangi kemampuan mitigasi risiko yang memadai dapat meningkatkan potensi kesalahan transaksi, penipuan, maupun gangguan keamanan data.

Dalam *Protection Motivation Theory (PMT)*, kemampuan mitigasi risiko QRIS merupakan bentuk *protective behavior* atau respons protektif individu dalam menghadapi ancaman keamanan digital. Kemampuan ini tercermin melalui tindakan pengguna dalam mengidentifikasi, mencegah, serta merespons risiko penipuan pada transaksi QRIS.

#### **2.1.5.2 Faktor – Faktor Yang Memengaruhi Mitigasi Risiko**

Kemampuan mitigasi risiko berkaitan dengan berbagai aspek yang melibatkan individu dan sistem dalam mengelola risiko. Dalam literatur manajemen risiko, mitigasi risiko menekankan pada kemampuan untuk mengidentifikasi, memahami, serta mengendalikan risiko yang muncul melalui penerapan langkah-langkah pengendalian yang tepat (Hopkin, 2018; ISO 31000, 2018). Secara umum, beberapa faktor yang dapat mendukung kemampuan mitigasi risiko antara lain:

##### **1. Pengalaman dalam Penggunaan Sistem Digital**

Pengalaman penggunaan sistem digital mempengaruhi kemampuan individu dalam mengenali pola risiko serta memahami potensi ancaman yang dapat terjadi. Individu yang memiliki pengalaman lebih tinggi cenderung lebih mampu mengidentifikasi dan mengantisipasi risiko secara lebih efektif.

## **2. Pemahaman terhadap Risiko (*Risk Understanding*)**

Pemahaman terhadap jenis, sumber, dan dampak risiko membantu individu dalam menentukan strategi mitigasi yang tepat. Semakin tinggi pemahaman terhadap risiko, semakin baik kemampuan dalam mengendalikan risiko.

## **3. Ketersediaan dan Akses Informasi Risiko**

Informasi terkait ancaman dan keamanan memungkinkan individu untuk mengenali risiko lebih awal dan melakukan evaluasi secara tepat. Informasi yang memadai meningkatkan efektivitas proses mitigasi risiko.

## **4. Kualitas Sistem dan Teknologi**

Sistem yang memiliki fitur keamanan dan kontrol yang baik dapat membantu mengurangi potensi ancaman dan meningkatkan kemampuan mitigasi risiko.

### **2.1.5.3 Manfaat Mitigasi Risiko**

Penerapan mitigasi risiko memberikan berbagai manfaat dalam menjaga keamanan serta keberlangsungan sistem. Dalam literatur manajemen risiko, mitigasi risiko berperan dalam mengurangi tingkat risiko serta dampak yang ditimbulkan melalui penerapan pengendalian yang tepat (COSO, 2017; ISO 31000, 2018). Dalam konteks sistem digital, mitigasi risiko juga berkontribusi dalam meningkatkan ketahanan sistem serta mengurangi potensi kerugian yang dapat terjadi akibat gangguan atau risiko penggunaan teknologi. Secara umum, manfaat mitigasi risiko antara lain:

### **1. Mengurangi Tingkat Risiko ke Level yang Dapat Diterima**

Mitigasi risiko membantu menurunkan tingkat risiko hingga berada pada batas yang dapat diterima melalui penerapan kontrol dan pengendalian yang tepat. Manfaat ini dirasakan secara langsung oleh pengguna QRIS melalui berkurangnya insiden penipuan dan kegagalan transaksi.

### **2. Meminimalkan Kerugian Finansial akibat Ancaman Digital**

Penerapan mitigasi risiko memberikan manfaat langsung berupa berkurangnya insiden penipuan dalam transaksi QRIS sehari-hari, sehingga potensi kerugian finansial akibat penggantian kode QR palsu maupun manipulasi bukti pembayaran dapat diminimalkan secara signifikan.

### **3. Meningkatkan Ketahanan (*Resilience*) Sistem terhadap Ancaman**

Mitigasi risiko memperkuat ketahanan sistem pembayaran digital dalam menghadapi berbagai bentuk ancaman yang terus berkembang. Sistem yang tangguh mampu bertahan dan beradaptasi terhadap serangan siber maupun gangguan operasional tanpa menimbulkan dampak yang signifikan bagi pengguna.

### **4. Menjaga Keberlangsungan Operasional**

Dengan adanya mitigasi risiko, gangguan terhadap sistem pembayaran digital dapat diminimalkan sehingga aktivitas transaksi QRIS dapat berjalan secara lebih stabil dan berkelanjutan. Manfaat ini penting bagi pelaku UKM *food and beverage* yang bergantung pada transaksi digital dalam kegiatan usaha sehari-hari.

## **5. Meningkatkan Kredibilitas dan Reputasi Penyelenggara**

Penerapan mitigasi risiko yang baik dapat meningkatkan rasa aman pengguna dalam menggunakan QRIS, sehingga pelaku usaha lebih percaya diri dalam menjalankan transaksi digital. Kepercayaan tersebut menjadi penting dalam mendukung pemanfaatan QRIS secara berkelanjutan dalam aktivitas usaha.

### **2.1.5.4 Tujuan Mitigasi Risiko**

Mitigasi risiko merupakan bagian dari pengelolaan risiko yang bertujuan untuk mengidentifikasi, menganalisis, serta mengurangi potensi dampak risiko yang dapat memengaruhi suatu sistem. Dalam konteks sistem pembayaran digital, mitigasi risiko menjadi penting karena berkaitan dengan keamanan dan keandalan transaksi. Dalam literatur manajemen risiko, mitigasi risiko dilakukan melalui pendekatan yang sistematis guna membantu memahami berbagai faktor yang dapat memengaruhi pencapaian tujuan serta menentukan langkah pengelolaan risiko yang tepat (Aven, 2016; ISO 31000, 2018). Oleh karena itu, secara umum tujuan mitigasi risiko antara lain sebagai berikut:

#### **1. Melindungi Pengguna dari Kerugian Finansial dan Reputasi**

Mitigasi risiko bertujuan untuk menekan kemungkinan terjadinya kerugian finansial akibat penipuan, kesalahan transaksi, maupun penyalahgunaan data dalam penggunaan QRIS. Dengan adanya upaya mitigasi, pelaku usaha diharapkan mampu meminimalkan dampak ekonomi yang ditimbulkan oleh insiden keamanan.

## **2. Meningkatkan Kemampuan Mengidentifikasi Potensi Risiko**

Mitigasi risiko bertujuan meningkatkan kapasitas pelaku usaha dalam mengenali secara dini berbagai bentuk ancaman yang dapat terjadi dalam penggunaan QRIS, seperti indikasi penggantian kode QR, manipulasi bukti transaksi, maupun aktivitas mencurigakan lainnya. Kemampuan identifikasi yang baik memungkinkan pelaku usaha mengambil tindakan pencegahan sebelum risiko berkembang menjadi kerugian yang lebih besar.

## **3. Meningkatkan Kepercayaan Pengguna terhadap Sistem Pembayaran Digital**

Mitigasi risiko yang efektif bertujuan untuk membangun dan mempertahankan kepercayaan masyarakat terhadap sistem pembayaran QRIS. Dengan pengelolaan risiko yang baik, penyelenggara tidak hanya terlindungi dari ancaman, tetapi juga mampu mendorong adopsi QRIS secara lebih luas dan berkelanjutan.

## **4. Mendukung Kepatuhan terhadap Regulasi Sistem Pembayaran**

Penerapan mitigasi risiko bertujuan memastikan bahwa penyelenggaraan QRIS berjalan sesuai dengan ketentuan yang ditetapkan oleh regulator, termasuk Peraturan Bank Indonesia terkait manajemen risiko sistem pembayaran elektronik. Kepatuhan regulasi menjadi bagian penting dalam menjaga integritas dan legalitas ekosistem pembayaran digital.

#### 2.1.5.5 Indikator Mitigasi Risiko

Indikator kemampuan mitigasi risiko QRIS dalam penelitian ini diadaptasi dari *NIST Cybersecurity Framework (CSF) 2.0* yang diterbitkan oleh *National Institute of Standards and Technology* pada tahun 2024. NIST CSF 2.0 merupakan kerangka keamanan siber yang diakui secara internasional dan dirancang secara fleksibel sehingga dapat diterapkan oleh berbagai jenis organisasi maupun individu, termasuk pelaku usaha kecil dan menengah, dalam mengelola dan memitigasi risiko keamanan digital secara sistematis (National Institute of Standards & Technology, 2024).

Adaptasi indikator dari NIST CSF 2.0 ke tingkat individu pengguna QRIS dilakukan dengan mempertimbangkan kemampuan nyata yang dapat diamati pada pelaku UKM *food and beverage* dalam aktivitas transaksi digital sehari-hari. Adapun indikator kemampuan mitigasi risiko QRIS yang digunakan dalam penelitian ini adalah sebagai berikut:

##### 1. **Detect (Kemampuan Deteksi),**

Kemampuan individu dalam mengidentifikasi dan mendeteksi secara mandiri adanya ancaman, aktivitas mencurigakan, atau indikasi penipuan yang terjadi dalam penggunaan sistem pembayaran QRIS. NIST CSF 2.0 mendefinisikan fungsi *Detect* sebagai kemampuan untuk menemukan dan menganalisis kondisi yang mengindikasikan terjadinya insiden keamanan siber secara tepat waktu, sehingga tindakan pencegahan dapat segera diambil sebelum kerugian yang lebih besar terjadi.

## 2. ***Protect* (Kemampuan Perlindungan)**

Kemampuan individu dalam menerapkan langkah-langkah perlindungan yang diperlukan untuk mencegah terjadinya insiden keamanan dalam penggunaan QRIS, seperti memastikan transaksi hanya dilakukan melalui jaringan dan perangkat yang aman serta menerapkan prosedur keamanan berlapis sebelum bertransaksi. NIST CSF 2.0 menjelaskan bahwa fungsi *Protect* bertujuan untuk memitigasi dampak dari potensi insiden keamanan siber melalui penerapan pengamanan proaktif yang mendukung keberlangsungan layanan kritis.

## 3. ***Respond* (Kemampuan Respons)**

Kemampuan individu dalam mengambil tindakan yang cepat dan tepat ketika menemukan indikasi penipuan atau insiden keamanan dalam transaksi QRIS, termasuk kemampuan dalam melaporkan kejadian tersebut kepada pihak berwenang secara mandiri. NIST CSF 2.0 mendefinisikan fungsi *Respond* sebagai kemampuan untuk mengembangkan dan mengimplementasikan tindakan yang sesuai terhadap insiden keamanan siber yang terdeteksi guna membatasi dampak yang ditimbulkan.

## 4. ***Recover* (Kemampuan Pemulihan)**

Kemampuan individu dalam memulihkan kondisi akun pembayaran dan meminimalkan kerugian setelah terjadinya insiden keamanan dalam penggunaan QRIS, termasuk kemampuan memblokir akses tidak sah dan mengembalikan aktivitas transaksi ke kondisi normal. NIST CSF 2.0 menjelaskan bahwa fungsi *Recover* mendukung pemulihan operasional

secara tepat waktu setelah terdampak insiden keamanan siber, serta memastikan peningkatan ketahanan sistem untuk mencegah terulangnya insiden serupa di masa mendatang.

## 2.1.6 Penelitian Terdahulu

**Tabel 2.1**  
**Penelitian Terdahulu**

| No | Peneliti                 | Judul Penelitian                                                                                                | Hasil Penelitian                                                                                                                                                                                                                                                                             | Referensi                                                                                                                                                                                                                                                                     |
|----|--------------------------|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Sahi et al. (2022)       | The Research Trend of Security and Privacy in Digital Payment                                                   | Persepsi keamanan dan privasi berpengaruh positif terhadap kepercayaan pengguna dalam menggunakan pembayaran digital, serta framework TAM dan UTAUT terbukti efektif dalam menjelaskan adopsi sistem pembayaran digital.                                                                     | Informatics (MDPI) Vol. 9(2):32 (2022)<br>Scopus Q2<br><a href="https://www.mdpi.com/2227-9709/9/2/32">https://www.mdpi.com/2227-9709/9/2/32</a>                                                                                                                              |
| 2  | Bada & Nurse (2023)      | A Quest for Research and Knowledge Gaps in Cybersecurity Awareness for SMEs                                     | <i>Cybersecurity awareness</i> berpengaruh positif sebagai komponen penting dalam meningkatkan pertahanan siber UMKM, serta peningkatan <i>awareness</i> turut mendorong peningkatan literasi keamanan dan alokasi sumber daya yang lebih besar untuk inisiatif keamanan siber.              | Computers & Security (Elsevier) Vol. Vol. 132 (2023)<br>Scopus Q1<br><a href="https://www.sciencedirect.com/science/article/pii/S157401372300059X">https://www.sciencedirect.com/science/article/pii/S157401372300059X</a>                                                    |
| 3  | Elrayah & Jamil (2023)   | Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour                               | Literasi digital berpengaruh positif terhadap perilaku keamanan siber; individu yang aktif memanfaatkan informasi digital lebih cenderung mengadopsi langkah perlindungan privasi. <i>Cybersecurity awareness</i> terbukti memoderasi hubungan antara literasi digital dan perilaku keamanan | International Journal of Cyber Criminology, Vol. 17 No. 1 (2023),<br>Scopus Q2<br><a href="https://cybercrimejournal.com/menu-script/index.php/cybercrimejournal/article/view/205">https://cybercrimejournal.com/menu-script/index.php/cybercrimejournal/article/view/205</a> |
| 4  | Anisah & Amaniyah (2024) | Pengaruh Literasi Keuangan, Risiko Transaksi, dan Kemudahan terhadap Minat Penggunaan QRIS pada UMKM di Sampang | Literasi digital, risiko transaksi, dan kemudahan penggunaan berpengaruh positif terhadap minat penggunaan QRIS pada UMKM, di mana semakin baik pemahaman teknologi, pengelolaan risiko, serta kemudahan sistem, semakin tinggi minat UMKM dalam menggunakan QRIS.                           | Journal of Accounting and Finance Management (JAFM) Vol. Vol. 5 No. 5 (2024)<br>SINTA 3<br><a href="https://dinastires.org/JAFM/article/view/1056">https://dinastires.org/JAFM/article/view/1056</a>                                                                          |

| No | Peneliti                        | Judul Penelitian                                                                                       | Hasil Penelitian                                                                                                                                                                                                                                                                                    | Referensi                                                                                                                                                                                                                                           |
|----|---------------------------------|--------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5  | Kristanty, D.N. (2024)          | Tren dan Tantangan Keamanan Bertransaksi dengan QRIS dalam Era Transformasi Sistem Pembayaran Digital  | Penerapan metode autentikasi yang kuat dan protokol enkripsi meningkatkan keamanan transaksi QRIS, serta edukasi dan peningkatan kesadaran pengguna berperan dalam mengurangi risiko penipuan dan phishing.                                                                                         | Syntax Admiration Vol. Vol. 5 No. 10 (2024) <i>SINTA 3</i><br><a href="https://jurnalsyntaxadmiration.com/index.php/jurnal/article/view/1538">https://jurnalsyntaxadmiration.com/index.php/jurnal/article/view/1538</a>                             |
| 6  | Varalakshmi et al. (2024)       | Modelling Cybersecurity Impacts on Digital Payment Adoption: A Game Theoretic Approach                 | <i>Cybersecurity awareness</i> dan pelatihan keamanan meningkatkan kepercayaan pengguna serta adopsi sistem pembayaran digital, sementara pemantauan transaksi secara <i>real-time</i> dan deteksi aktivitas mencurigakan berperan dalam mengurangi kejahatan siber dan memperkuat mitigasi risiko. | Digital Business (Elsevier) Vol. Vol. 4 (2024) <i>Scopus Q1</i><br><a href="https://www.sciencedirect.com/science/article/pii/S2949791424000411">https://www.sciencedirect.com/science/article/pii/S2949791424000411</a>                            |
| 7  | Thi Thuy et al. (2024)          | Digital Literacy, Online Security Behaviors and E-Payment Intention                                    | Literasi digital berpengaruh positif terhadap perilaku keamanan pengguna dalam bertransaksi, serta perilaku keamanan berperan sebagai mediator dalam meningkatkan niat penggunaan e-payment secara berkelanjutan.                                                                                   | Journal of Retailing and Consumer Services (Elsevier) Vol. Vol. 79 (2024) <i>Scopus Q1</i><br><a href="https://www.sciencedirect.com/science/article/pii/S2199853124000866">https://www.sciencedirect.com/science/article/pii/S2199853124000866</a> |
| 8  | Baottong et al. (2025)          | Mitigating QR-Phishing Risks in Indonesian Digital Payments through Security Behavior Intentions Scale | Perilaku keamanan pengguna yang diukur menggunakan <i>Security Behavior Intentions Scale</i> (SeBIS) berpengaruh signifikan terhadap mitigasi risiko <i>QR-phishing</i> .                                                                                                                           | JMPKN, Vol. 5 No. 1 (2025), <i>SINTA 6</i><br><a href="https://ojs.nitromks.ac.id/index.php/JMPKN/article/view/757">https://ojs.nitromks.ac.id/index.php/JMPKN/article/view/757</a>                                                                 |
| 9  | Oktiana M.S., Tarigan A. (2025) | Measurement of Security Awareness Level in the Implementation of QRIS                                  | Tingkat <i>cybersecurity awareness</i> pengguna QRIS berada pada kategori cukup baik dan menunjukkan bahwa sebagian besar pengguna telah memahami pentingnya aspek keamanan dalam bertransaksi, sehingga awareness berperan dalam meningkatkan kewaspadaan terhadap risiko penggunaan QRIS.         | JCoSITTE, Vol. 8 No. 1 (2025), <i>SINTA 4</i><br><a href="https://jurnal.umsu.ac.id/index.php/jcositte/article/view/26050">https://jurnal.umsu.ac.id/index.php/jcositte/article/view/26050</a>                                                      |
| 10 | Anggita et al. (2025)           | Mitigasi Ancaman Social Engineering bagi UMKM melalui Program Sosialisasi di Kota Pangkalpinang        | Program sosialisasi keamanan digital meningkatkan kesadaran dan pemahaman pelaku UMKM terhadap ancaman social engineering, sehingga mendukung upaya mitigasi risiko dan peningkatan keamanan dalam aktivitas digital.                                                                               | Jurnal Abdimas Ilmiah Citra Bakti, Vol. 6 No. 1 (2025), <i>SINTA 5</i><br><a href="https://jurnal.citrabakti.ac.id/index.php/jailcb/article/view/4556">https://jurnal.citrabakti.ac.id/index.php/jailcb/article/view/4556</a>                       |

## **2.2 Kerangka Pemikiran**

### **2.2.1 Pengaruh Literasi Digital terhadap *User Awareness***

Literasi digital memiliki peran penting dalam membentuk tingkat kesadaran pengguna (*user awareness*) terhadap risiko yang muncul dalam penggunaan teknologi digital. Individu dengan tingkat literasi digital yang tinggi cenderung mampu memahami informasi digital secara kritis, termasuk mengenali potensi ancaman seperti phishing, malware, dan kebocoran data. Hal ini menunjukkan bahwa literasi digital tidak hanya berkaitan dengan kemampuan teknis, tetapi juga mempengaruhi tingkat kewaspadaan pengguna dalam menjaga keamanan aktivitas digital (Suartana et al., 2022).

Selain itu, literasi digital juga berperan dalam meningkatkan pemahaman terhadap keamanan informasi serta risiko yang dihadapi dalam aktivitas digital. Penelitian menunjukkan bahwa rendahnya literasi digital menyebabkan rendahnya tingkat kesadaran terhadap keamanan siber, sehingga individu lebih rentan terhadap serangan digital. Sebaliknya, peningkatan literasi digital mampu meningkatkan *awareness* serta kesiapan dalam menghadapi ancaman siber (Ajhari et al., 2023).

### **2.2.2 Pengaruh Perilaku Keamanan terhadap *User Awareness***

Perilaku keamanan (*security hygiene practice*) berpengaruh positif terhadap *user awareness* dalam penggunaan teknologi digital. Praktik ini mencakup perilaku rutin pengguna seperti penggunaan *password* yang kuat, pembaruan sistem secara berkala, serta kewaspadaan terhadap aktivitas mencurigakan. Penelitian menunjukkan bahwa individu yang secara konsisten menerapkan praktik keamanan memiliki tingkat kesadaran yang lebih tinggi terhadap ancaman siber, karena

mereka lebih memahami potensi risiko dan cara pencegahannya (Parsons et al., 2017).

Selain itu, penerapan *security hygiene practices* juga meningkatkan kemampuan pengguna dalam mengenali dan merespons ancaman digital. Pengguna yang aktif melakukan praktik keamanan seperti autentikasi berlapis dan verifikasi informasi cenderung lebih peka terhadap serangan seperti phishing dan penipuan online. Hal ini menunjukkan bahwa semakin baik praktik keamanan yang diterapkan, maka semakin tinggi tingkat user awareness terhadap risiko digital (Ifinedo, 2012).

### **2.2.3 Pengaruh Literasi Digital terhadap Kemampuan Mitigasi Risiko**

#### **QRIS**

Elrayah & Jamil, (2023)Elrayah & Jamil, (2023) menunjukkan bahwa literasi digital berpengaruh positif terhadap perilaku keamanan siber pengguna, di mana individu yang aktif memanfaatkan informasi digital cenderung lebih mampu mengadopsi langkah-langkah perlindungan untuk menghadapi ancaman dalam transaksi digital. Temuan ini mengindikasikan bahwa literasi digital berperan dalam meningkatkan kemampuan individu dalam mengelola risiko yang muncul dalam penggunaan layanan pembayaran digital.

Sejalan dengan hal tersebut, (Nguyen et al., 2024) menunjukkan bahwa literasi digital berpengaruh positif terhadap perilaku keamanan pengguna dalam bertransaksi secara elektronik. Peningkatan literasi digital mendorong penerapan praktik keamanan yang lebih baik, yang pada akhirnya berkontribusi dalam meningkatkan kemampuan pengguna dalam mengurangi risiko serta mendorong

penggunaan layanan pembayaran digital secara lebih aman dan berkelanjutan. Berdasarkan kedua temuan tersebut, literasi digital memiliki hubungan positif terhadap kemampuan mitigasi risiko QRIS.

#### **2.2.4 Pengaruh Perilaku Keamanan Terhadap Kemampuan Mitigasi Risiko QRIS**

Singkeruang et al., (2025) menunjukkan bahwa perilaku keamanan pengguna yang diukur menggunakan *Security Behavior Intentions Scale (SeBIS)* berkaitan dengan upaya mitigasi ancaman *quishing* pada transaksi berbasis *QR Code*. Temuan ini menegaskan bahwa penerapan perilaku keamanan merupakan faktor penting dalam mendukung pengurangan risiko pada sistem pembayaran digital.

Sejalan dengan itu, (Baottong et al., 2025) menunjukkan bahwa *password management, software updates, dan device security practices* berpengaruh positif terhadap mitigasi risiko *quishing* pada transaksi digital berbasis *QR Code*. Hasil ini mengindikasikan bahwa semakin baik perilaku keamanan pengguna, semakin tinggi kemampuan pengguna dalam mendeteksi, merespons, dan mengurangi risiko serangan pada penggunaan QRIS. Berdasarkan temuan tersebut, perilaku keamanan memiliki hubungan positif terhadap kemampuan mitigasi risiko QRIS.

#### **2.2.5 Pengaruh User Awareness Terhadap kemampuan Mitigasi Risiko QRIS**

*User awareness* memiliki peran penting dalam mendukung kemampuan mitigasi risiko dalam penggunaan sistem pembayaran digital seperti QRIS. *User awareness* mencerminkan tingkat pemahaman dan kewaspadaan pengguna

terhadap berbagai ancaman siber, seperti *phishing*, penipuan, dan kebocoran data. Penelitian menunjukkan bahwa awareness berkontribusi dalam mengurangi risiko keamanan digital, di mana pengguna yang memiliki kesadaran tinggi cenderung lebih mampu mengenali ancaman serta mengantisipasi potensi risiko dalam aktivitas digital (AlHogail, 2023).

*User awareness* juga mendorong pengguna untuk menerapkan tindakan preventif sebagai bagian dari upaya mitigasi risiko. Pengguna yang memiliki tingkat kesadaran yang tinggi terhadap keamanan digital akan lebih aktif dalam menerapkan langkah-langkah proteksi, seperti verifikasi transaksi, penggunaan autentikasi berlapis, serta kehati-hatian dalam berbagi informasi. Hal ini menunjukkan bahwa peningkatan *awareness* tidak hanya meningkatkan pemahaman terhadap risiko, tetapi juga (Zwilling et al., 2022).

#### **2.2.6 Peran Mediasi *User Awareness* pada Pengaruh Literasi Digital terhadap Kemampuan Mitigasi Risiko QRIS**

(Elrayah & Jamil, 2023) Literasi digital tidak hanya berkaitan dengan kemampuan pengguna dalam memahami teknologi, tetapi juga mendorong terbentuknya *user awareness* yang lebih baik dalam menghadapi ancaman digital. (Elrayah & Jamil, 2023) menunjukkan bahwa literasi digital berpengaruh positif terhadap *cybersecurity behaviour*, dan pengaruh tersebut menjadi lebih kuat ketika pengguna memiliki tingkat *cybersecurity awareness* yang lebih tinggi. Temuan ini menunjukkan bahwa peningkatan literasi digital dapat memperkuat kesadaran pengguna terhadap risiko keamanan, yang selanjutnya mendukung kemampuan mereka dalam menghadapi ancaman pada transaksi digital.

Temuan tersebut sejalan dengan (Nguyen et al., 2024) yang menunjukkan bahwa *digital literacy* berpengaruh terhadap *online security behavior* dalam penggunaan *e-payment*. Hal ini mengindikasikan bahwa literasi digital mendorong terbentuknya awareness dan perilaku keamanan yang lebih baik, yang pada akhirnya memperkuat kemampuan pengguna dalam mengidentifikasi, merespons, dan mengurangi risiko pada penggunaan QRIS. Dengan demikian, *user awareness* berperan sebagai mediator positif pada pengaruh literasi digital terhadap kemampuan mitigasi risiko QRIS.

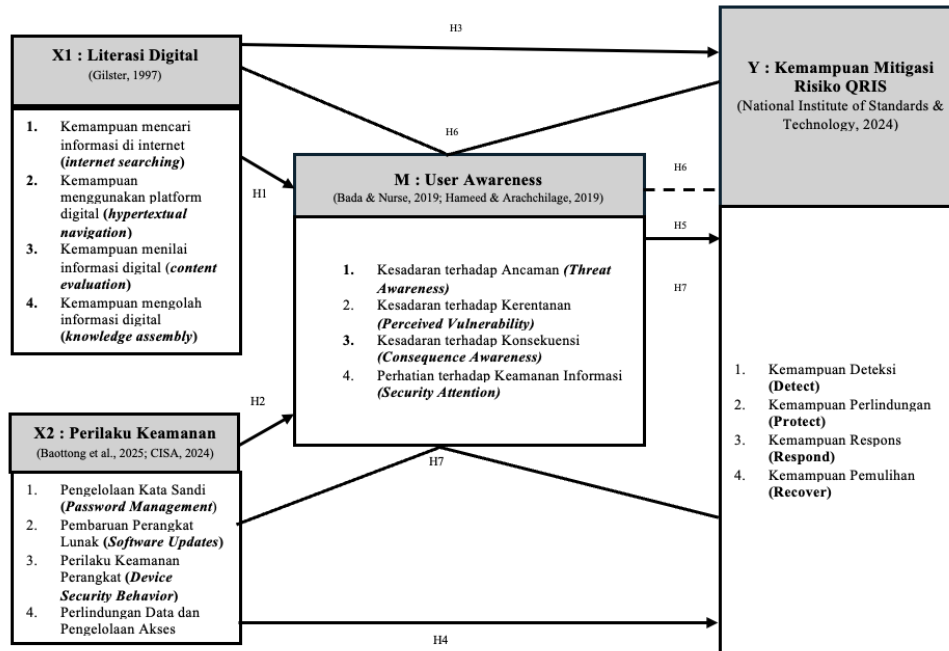
#### **2.2.7 Peran Mediasi User Awareness pada Pengaruh Perilaku Keamanan terhadap Kemampuan Mitigasi Risiko QRIS**

Perilaku keamanan tidak hanya berfungsi sebagai bentuk perlindungan langsung terhadap ancaman digital, tetapi juga mendorong meningkatnya user awareness dalam penggunaan sistem pembayaran berbasis *QR Code*. (Baottong et al., 2025) menunjukkan bahwa *password management*, *regular software updates*, dan *device security practices* berpengaruh positif terhadap mitigasi risiko *quishing*, dengan *user awareness* sebagai variabel mediasi yang memperkuat pengaruh perilaku pengguna terhadap mitigasi risiko. Temuan ini menunjukkan bahwa perilaku keamanan yang baik dapat meningkatkan kesadaran pengguna terhadap ancaman digital, yang selanjutnya memperkuat kemampuan mereka dalam mengurangi risiko pada transaksi QRIS.

Temuan tersebut diperkuat oleh (Puri et al., 2025) yang menunjukkan bahwa perilaku pencegahan merupakan faktor penting dalam mengurangi risiko *digital financial fraud* pada sistem pembayaran digital. Hal ini menegaskan bahwa ketika

perilaku keamanan mampu membentuk *awareness* yang lebih tinggi, pengguna akan lebih siap dalam mengenali ancaman, mengambil tindakan preventif, dan meminimalkan risiko transaksi digital. Dengan demikian, *user awareness* berperan sebagai mediator positif pada pengaruh perilaku keamanan terhadap kemampuan mitigasi risiko QRIS.

## 2.2.8 Paradigma Penelitian



Sumber : (Bada & Nurse, 2019; N. Baottong et al., 2025; CISA, 2024; Gilster, 1997; Hameed & Arachchilage, 2019; National Institute of Standards & Technology, 2024)

**Gambar 2.1 Paradigma Penelitian**

## 2.3 Hipotesis Penelitian

Berdasarkan kajian teori dan kerangka pemikiran diatas, maka hipotesis yang diajukan adalah sebagai berikut:

1. Hipotesis 1: Literasi digital berpengaruh positif terhadap *user awareness* pada pelaku UKM *food and beverage* pengguna QRIS.
2. Hipotesis 2: Perilaku keamanan berpengaruh positif terhadap *user awareness* pada pelaku UKM *food and beverage* pengguna QRIS.
3. Hipotesis 3: Literasi digital berpengaruh positif terhadap kemampuan mitigasi risiko QRIS pada pelaku UKM *food and beverage*.

4. Hipotesis 4: Perilaku keamanan berpengaruh positif terhadap kemampuan mitigasi risiko QRIS pada pelaku UKM *food and beverage*.
5. Hipotesis 5: *User awareness* berpengaruh positif terhadap kemampuan mitigasi risiko QRIS pada pelaku UKM *food and beverage*.
6. Hipotesis 6: *User awareness* memediasi pengaruh literasi digital terhadap kemampuan mitigasi risiko QRIS pada pelaku UKM *food and beverage*.
7. Hipotesis 7: *User awareness* memediasi pengaruh perilaku keamanan terhadap kemampuan mitigasi risiko QRIS pada pelaku UKM *food and beverage*.