MATT BACAK'S CHECKLIST

Checklist 2 - Leveraging Multi-Factor Authentication (MFA)

Project Name: _____ **Date:** _____

		Yes	No
	In addition to using usernames and passwords, it is advisable to add an extra authentication factor to improve your security. Multi-factor authentication or 2FA assures your business of an additional layer of security. Consider applying multi-factor authentication on your networks, banking sites, and emails for extra security in the event that your passwords are compromised. Multi-factor authentication uses several approaches to approve user access by authenticating the identity of the user through passwords, biometrics, trusted devices, and fingerprints. When selecting a multi-factor authentication solution, always ensure that the solution meets the needs and requirements of your organization. Select an option that is applicable to your local apps and devices, as well as your cloud-based environments. An effective multi-factor authentication solution should be able to meet your organization's current needs and also have the ability to anticipate future needs. This checklist provides guiding principles when selecting a multi-factor authentication solution for your organization.		
1	What are the business and technical needs of your organization/business?	☐	☐
2	Does your selected MFA cater to both your business and technical needs?	☐	☐

Notes

MATT BACAK'S CHECKLIST

Checklist 2 - Leveraging Multi-Factor Authentication (MFA)

3 Can the MFA anticipate future needs and changes of your business? ☐ ☐

4 Is your MFA solution highly available? ☐ ☐

5 Does the MFA solution allow storage of data in the user directory? ☐ ☐

6 Does the solution support a wide range of applications and interfaces? ☐ ☐

7 Is risk-based step-up authentication supported by the selected MFA? ☐ ☐

8 Does the MFA solution come with additional software costs for software tokens? ☐ ☐

9 Is the selected MFA flexible enough to maximize usability? ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 2 - Leveraging Multi-Factor Authentication (MFA)

10 Can the MFA anticipate objections? ☐ ☐

11 Does it come with options regarding software tokens? ☐ ☐

12 Does the MFA provider have technical innovation plans for the future? ☐ ☐

13 Does it provide a positive user experience (ease of use by workers and customers)? ☐ ☐

14 Does the MFA mitigate risks such as opt-outs? ☐ ☐

15 Does the MFA utilize passive user data like IP address, geolocation, and device identifiers? ☐ ☐

16 Have you established alternatives to phone-based MFA solutions? ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 2 - Leveraging Multi-Factor Authentication (MFA)

17 Does your business require a stand-alone MFA solution? ☐ ☐

18 Are greater identity and access management (IAM) capabilities required? ☐ ☐

19 Does the MFA have built-in and tightly integrated components utilizing single user and management interface? ☐ ☐

20 Does your selected MFA support the authenticator's digital identity and lifecycle requirements? ☐ ☐

21 Do your configurations support only approved authenticators? ☐ ☐

22 Are all your systems and software patched and up-to-date? ☐ ☐

23 Does the MFA solution offer a local installation and external hosting? ☐ ☐

Notes

MATT BACAK'S CHECKLIST

Checklist 2 - Leveraging Multi-Factor Authentication (MFA)

Notes:

•Avoid going overboard with your MFA type by not exceeding 2-3 factors in your MFA.
•Check that your selected MFA solution does not contain hidden costs.

Notes